Práctica de laboratorio 1.1.2 Repaso del modelo OSI - Descripción general



Duración estimada: 20 min.

Objetivos:

- Relacionar los dispositivos y la terminología con las diversas capas del modelo OSI
- Comparar las capas del modelo OSI con las del modelo TCP/IP
- Identificar las utilidades y los protocolos TCP/IP que operan en cada capa

Información básica:

Esta práctica de laboratorio sirve como repaso para reforzar la comprensión de las siete capas del modelo OSI y su relación con el modelo TCP/IP. El enfoque se centra en los términos y dispositivos que se adecuan al modelo OSI. Esta práctica de laboratorio se puede organizar como una entretenida actividad competitiva de conocimiento.

Herramientas / Preparación:

Se puede hacer una competencia entre grupos. Cuente los estudiantes y divídalos en grupos de 2 a 4 personas cada uno. Sin consultar apuntes o respuestas, vea con qué porcentaje de aciertos los miembros de su grupo pueden completar la tabla sobre OSI de la planilla de trabajo. El grupo que tenga la mayor cantidad de respuestas correctas (puntos) en la tabla al finalizar el período de tiempo especificado (por ej., 10 min.) será el ganador. Si algún otro grupo pone en duda un término o una respuesta de la tabla, pueden cuestionarlo/a y recibir los puntos si la comisión de revisión (compuesta por un miembro de cada grupo) está de acuerdo con este cuestionamiento.

Antes de iniciar esta práctica de laboratorio, es conveniente leer el capítulo 1 de la Guía del segundo año de la Academia de networking y los capítulos 1, 9 y 10 de la Guía del primer año.

También conviene repasar la Lección 1 en línea del Semestre 3. Se requieren los siguientes recursos:

- Estación de trabajo de PC con Windows instalado
- NIC instalada y cable de conexión Cat 5 con conexión a Internet
- Software navegador (Netscape Navigator 3.0 o versión más reciente o Internet Explorer 4.0 o versión más reciente) instalado
- Elementos de networking típicos como, por ejemplo, NIC Ethernet y Token Ring con distintos conectores (Coaxial, AUI, RJ-45)
- Hubs, switches y routers de ejemplo

Notas:

Paso 1 - El modelo OSI y las capas de pila de protocolo TCP/IP asociadas.

Tarea: Complete las siguientes tablas basándose en su conocimiento de los modelos OSI y TCP/IP.

Explicación: Su comprensión del modelo OSI y su relación con el modelo TCP/IP aumentará considerablemente su capacidad para incorporar y categorizar la información de networking a medida que la aprenda.

1. Dado el número de capa OSI, complete el cuadro que aparece a continuación. De ser posible, compita con los demás grupos y trate de pensar en la mayor cantidad de protocolos, estándares, utilidades, términos y dispositivos que le sea posible sin consultar sus notas. Nota: Las capas TCP/IP se relacionan con más de una de las capas OSI.

El modelo OSI y la pila de protocolo TCP/IP

Nº de OSI	Nombre de la capa OSI (y su función)	№ de TCP/ IP	Nombre de la capa TCP/IP	Protocolos, estándares y utilidades en cada capa TCP/IP	Dispositivos y términos asociados con esta capa
7					
6					
5					

4			
3			
2			
1			

Práctica de laboratorio 1.5.13.1 Repaso de la configuración de laboratorio del router- Descripción general

Duración estimada: 30 min.

Objetivos:

- Configurar el equipo de laboratorio de Cisco de acuerdo con el diagrama de topología del Semestre 2 que aparece anteriormente o analizar las conexiones físicas de una configuración de laboratorio existente.
 - Documentar el cableado y las conexiones entre los dispositivos.
- Preparar un diagrama de configuración del equipo de laboratorio.

Información básica:

Esta práctica de laboratorio sirve como repaso de la forma en que se configuran y se conectan los routers de laboratorio de Cisco para la topología del Semestre 2 (consulte el diagrama que aparece anteriormente). Este es un repaso de la topología de red del semestre 2. Usted examinará y documentará las conexiones físicas entre estos routers y los demás componentes de hardware de laboratorio, tales como, hubs, switches y estaciones de trabajo. Si no es posible comenzar con el equipo desconectado, documente una configuración de laboratorio existente. En esta práctica de laboratorio se utiliza la configuración estándar compuesta por 5 routers, 4 hubs, 1 switch y por lo menos 5 estaciones de trabajo además de todo el cableado y los adaptadores asociados.

De ser posible, es una buena idea trabajar en esta práctica de laboratorio y en la siguiente (1.5.13.2) de forma simultánea. La siguiente práctica de laboratorio le brinda la oportunidad de desarrollar un esquema de direccionamiento IP basado en múltiples direcciones de subred Clase B. Puede trabajar en grupos de 3 a 5 y, mientras un grupo realiza la configuración física del router de laboratorio, el otro grupo puede diseñar el esquema de direccionamiento Clase B en el pizarrón.

Herramientas / Preparación:

Antes de iniciar esta práctica de laboratorio, debe tener disponible el equipo necesario para la práctica de laboratorio estándar de 5 routers (routers, hubs, switch, etc.). Los routers y los hubs se deben desconectar y apilar. Se debe agrupar cada tipo de cableado (WAN, LAN, consola, alimentación). Si no es posible comenzar con el equipo desconectado, debe repasar los pasos de la práctica de laboratorio con el equipo ya conectado. Esto le permitirá reforzar su conocimiento acerca de las conexiones físicas y las interfaces de los dispositivos.

De ser posible, comience con los routers, switches, hubs y el cableado desconectados. Su grupo deberá conectarlos de acuerdo con el diagrama de topología que se suministra en la descripción general que aparece al comienzo de esta práctica de laboratorio y luego debe documentar los resultados. Esta práctica de laboratorio requiere que se conecten los routers según la topología estándar de laboratorio o lo más parecido posible, según del equipo del que disponga. La siguiente práctica de laboratorio 1.5.13.2 suministra instrucciones para la configuración de los routers y las estaciones de trabajo utilizando una dirección de red Clase B con subredes. Se trabaja en grupos de 3 o más personas. Antes de empezar esta práctica de laboratorio, puede resultarle útil repasar el capítulo 1 de la Guía del segundo año de la Academia de networking de Cisco y el capítulo 1 del Semestre 3 del currículum en línea.

Es necesario contar con los siguientes recursos:

- 5 estaciones de trabajo de PC (mín.) con el sistema operativo Windows e HyperTerminal instalados.
- 5 routers Cisco (modelo de la serie 1600 o de la serie 2500 con IOS 11.2 o versión posterior).
- 4 hubs Ethernet (10BASE-T con 4 a 8 puertos).
- Un switch Ethernet (Cisco Catalyst 1900 u otro similar).
- 5 cables de consola serial para conectar la estación de trabajo con el puerto de consola (con convertidores de RJ-45 a DB9).
- 3 conjuntos de cables seriales WAN V.35 (DTE macho/ DCE hembra) para conectarse de router a router.
- Cables Ethernet CAT5 de conexión directa para conectar los routers y estaciones de trabajo a hubs y switches.
- Transceivers AUI (DB15) a Ethernet RJ-45 (la cantidad depende de la cantidad de routers con puertos AUI) para convertir las interfaces del router AUI a 10BASE-T RJ-45.

Recursos de sitio Web:

Routing basics General information on routers 2500 series routers 1600 series routers Terms and acronyms IP routing protocol IOS command summary Cisco ConfigMaker information and download

Notas:

Paso 1 - Planificación preliminar de LAN/WAN para la práctica de laboratorio sobre routers.

Al configurar el equipo de laboratorio desde cero, es posible que deba prestar atención a las siguientes preguntas. Incluso en caso de estar iniciando la práctica con una configuración de laboratorio existente, debe repasar todos los pasos y contestar todas las preguntas para

familiarizarse con la conexión de los routers. Aunque es posible que en realidad no conecte el equipo, debe ubicar, examinar y documentar el cableado y las conexiones físicas entre los routers, hubs y estaciones de trabajo.

- ¿Dónde se deben ubicar los PC?
- ¿Dónde se deben ubicar los routers?
- ¿Dónde se deben ubicar el switch y los hubs?
- ¿Cómo se deben tender los cables Ethernet, seriales y de alimentación?
- ¿Cuántas tomas y cables de alimentación se necesitan?
- ¿Qué PC se conecta con qué router?
- ¿Qué PC se conecta a qué hub o switch?
- ¿Qué router se conecta a qué hub o switch?
- ¿Cómo se deben rotular los dispositivos y el cableado?

Paso 2 - Disposición del equipo de laboratorio.

La disposición de los routers y del equipo varía según el espacio y la configuración física del área de laboratorio. El objetivo es agrupar cada combinación de router/hub/estación de trabajo para que estén lo más cerca posible, ya que pueden representar LAN y ubicaciones geográficas separadas en el mundo real. Es más fácil ver las relaciones entre los equipos con esta disposición. El equipo se debe colocar de tal modo que todas las interfaces estén orientadas en la misma dirección y que se pueda acceder con facilidad al cableado y a las conexiones.

Paso 3 - Conexión del cableado serial WAN.

A continuación, debe conectar los cables seriales (DCE-DTE) entre los routers. En esta configuración de laboratorio, la interfaz serial 0 (S0) del router se conecta al cable DCE. DCE se refiere a las conexiones del Equipo de transmisión de datos (o Equipo de comunicación de datos) y representa el extremo de sincronización del enlace síncrono WAN. El cable DCE tiene un conector hembra V.35 (34 pins) de gran tamaño en uno de los extremos y un conector DB-60 en el otro extremo, que se conecta a la interfaz serial del router. La interfaz serial 1 (S1) se conecta al cable DTE (Equipo terminal de datos). El cable DTE tiene un conector macho V.35 de gran tamaño en uno de los extremo, que se conecta a la interfaz serial del router. Los cables también se rotulan como DCE o DTE.

1. Examine los cables y las conexiones de los routers y documente las conexiones en la tabla:

Nombre del router origen	Interfaz	Nombre del router destino	Interfaz

Paso 4 - Conexión del cableado Ethernet del router.

Para los routers que tienen una AUI (Interfaz de unidad de conexión) Ethernet 0 (E0) o puerto E1, se necesita un transceiver externo que convierta la AUI DB15 en un conector RJ-45 10BASE-T. Los routers de la serie 2500 generalmente tienen un puerto AUI. La serie 1600 tiene puertos AUI y RJ-45 y se puede utilizar el puerto RJ-45 sin que sea necesario colocar un transceiver externo. Todo el cableado Ethernet desde los routers hasta los hubs o switches debe ser de Categoría 5 (Cat 5) y debe estar tendido en forma de conexión directa (pin 1 a pin 1, pin2 a pin 2 etc.). Conecte el cableado Ethernet como se indica en el diagrama y luego rotule el cableado en cada extremo. Los hubs se deben numerar como Hub 1, Hub 2, etc.

2. Registre en la tabla cuáles son las interfaces Ethernet del router que están en uso y a qué hub (o switch) están conectados:

Nombre del router origen	Interfaz del router:	Hasta qué dispositivo Ethernet
Lab-A		
Lab-A		
Lab-B		
Lab-C		
Lab-D		
Lab-E		

Paso 5 - Conexión del cableado Ethernet de la estación de trabajo.

Coloque los PC en las ubicaciones planificadas y rotúlelos (ET-1, ET-2...) de izquierda a derecha, según el diagrama. Tienda los cables de conexión directa CAT 5 desde cada PC hacia donde se encuentran el switch y los hubs. Conecte el cableado Ethernet como se indica y luego rotule los cables en cada extremo según el dispositivo y la interfaz a los que se conectan. La siguiente tabla muestra las conexiones para las 10 estaciones de trabajo. Conecte por lo menos una estación de trabajo a cada hub o switch.

3. En la tabla que aparece a continuación, indique cuál es el dispositivo Ethernet al que se conecta cada estación de trabajo:

Desde la estación de trabajo	Hasta qué dispositivo Ethernet
ET-1	
ET-2	
ET-3	
ET-4	
ET-5	
ET-6	
ET-7	
ET-8	
ET-9	
ET-10	

Paso 6 - Conexión de las estaciones de trabajo de consola con los routers.

Conecte uno de los extremos de los cables rollover desde las estaciones de trabajo 4, 6, 8, 9 y 10 a la interfaz de consola de los routers Lab-A, B, C, D y E. Conecte uno de los extremos de cada uno de los cables rollover a un conector serial RJ-45 a DB-9. Conecte el conector serial a los puertos seriales de las 5 estaciones de trabajo. Rotúlelos en cada uno de los extremos.

4. ¿Qué tipo de cable es el cable de consola?

Paso 7 - Conectar los cables de alimentación a todos los dispositivos.

Enchufe y encienda todos los dispositivos. Verifique que todos estén activados observando las luces indicadoras.

¿Las luces de enlace que corresponden al switch, los hubs y las Tarjetas de interfaz de red (NIC) de las estaciones de trabajo están encendidas?

¿Las luces ubicadas en la parte trasera de los routers están encendidas?

5.

Paso 8 - Diseñar el diagrama de laboratorio utilizando ConfigMaker.

6. Utilice ConfigMaker para rediseñar el diagrama de laboratorio del router para que concuerde con la configuración física (routers, switches, hubs, estaciones de trabajo, etc). Este paso lo guiará a través del proceso de conectar todo el equipo de laboratorio y especificar todas las direcciones IP para todo el equipo y las interfaces. ConfigMaker también genera los archivos config reales que se pueden utilizar como referencia o para configurar el router. Asegúrese de rotular todo el equipo (por ej., Lab-A, Lab-B, etc.). En el Semestre 2 se incluye una Práctica de laboratorio de introducción a ConfigMaker y, si no está familiarizado con el producto, también puede ejecutar la demostración. Una vez que haya terminado el diagrama ConfigMaker, guarde una copia en su cuaderno o diario.

Nota: Si no tiene acceso a ConfigMaker, póngase en contacto con el instructor o descárguelo del sitio Web de Cisco que aparece en la lista de Recursos de sitio Web de la sección Descripción general de esta práctica de laboratorio.

Es posible utilizar el espacio que aparece a continuación para hacer un boceto de la configuración de laboratorio o para tomar apuntes.

7

Práctica de laboratorio 1.5.13.2 Repaso de las subredes del router-Descripción general

Duración estimada: 30 min.

Objetivos:

- Desarrollar un esquema de direccionamiento Clase B con subredes para la configuración de laboratorio de 5 routers
- Utilizar los comandos del IOS para configurar los routers en el esquema de subred de Clase B
- Asignar los números de red IP, las interfaces, direcciones IP y la información de la máscara de subred para las Redes de área local (LAN) y las Redes de área amplia que están en uso.
- Utilizar el icono del Panel de control / Red o la utilidad winipcfg.exe en cada estación de trabajo para verificar los valores de dirección IP, máscara de subred y gateway por defecto.
- Utilizar el comando Ping para probar las conexiones del router y de la estación de trabajo.

Información básica:

Esta es una práctica de laboratorio importante que permite demostrar su comprensión de la configuración de laboratorio de Cisco (consulte el diagrama que aparece anteriormente) y cómo se aplica la división en subredes a múltiples routers. Desarrollará un esquema de direccionamiento basado en una dirección de red Clase B y luego la dividirá en subredes para adaptarse a la red física actual, permitiendo su crecimiento futuro. Debe ser capaz de configurar los routers y las estaciones de trabajo sin consultar sus apuntes y utilizando solamente la función de ayuda del IOS.

La práctica de laboratorio 1.2 anterior brindó una oportunidad para configurar la configuración física de laboratorio. Se trabaja en grupos de 3 a 5, y, mientras un grupo configura la configuración física de laboratorio del router, el otro puede diseñar el esquema de direccionamiento Clase B y asignar la dirección IP a los dispositivos.

Herramientas / Preparación:

Antes de iniciar esta práctica de laboratorio, debe tener disponible el equipo estándar de 5 routers (routers, hubs, switch, cables, etc.). En esta práctica de laboratorio se da por sentado que se ha completado la práctica de laboratorio 1.2 anterior y que el equipo de la práctica de laboratorio (routers, hub, estaciones de trabajo, etc.) se encuentra reunido y conectado en la topología de laboratorio estándar. Se trabaja en grupos de 3 o más personas. Antes de empezar esta práctica de laboratorio, puede resultarle útil repasar el capítulo 1 de la Guía del segundo año de la Academia de networking de Cisco y el capítulo 1 del Semestre 3 del currículum en línea.

Es necesario contar con los siguientes recursos:

- (5) estaciones de trabajo de PC (mín.) con el sistema operativo Windows e HyperTerminal instalados.
- (5) routers Cisco (modelo de la serie 1600 o de la serie 2500 con IOS 11.2 o versión posterior).
- (4) hubs Ethernet (10BASE-T con 4 a 8 puertos).
- (1) switch Ethernet (Cisco Catalyst 1900 u otro similar).
- (5) cables de consola serial para conectar la estación de trabajo al puerto de consola (con convertidores de RJ-45 a DB9).

- (3) conjuntos de cables seriales WAN V.35 (DTE macho/ DCE hembra) para conectarse de router a router.
- Cables Ethernet CAT5 de conexión directa para conectar los routers y estaciones de trabajo a hubs y switches.
- Transceivers AUI (DB15) a Ethernet RJ-45 (la cantidad depende de la cantidad de routers con puertos AUI) para convertir las interfaces del router AUI a 10BASE-T RJ-45.

Recursos de sitio Web:

Routing basics General information on routers 2500 series routers 1600 series routers Terms and acronyms IP routing protocol IOS command summary

Notas:

Paso 1 - Verificar que todas las conexiones físicas sean las correctas.

Repase el diagrama estándar de la práctica de laboratorio del Semestre 2 en la sección descripción general de esta práctica de laboratorio o el diagrama que ha creado en la práctica de laboratorio anterior y verifique todos los dispositivos físicos, cables y conexiones. Verifique que los routers estén configurados correctamente desde el punto de vista físico.

Paso 2 - Desarrollar un esquema de direccionamiento Clase B.

Se le ha otorgado una dirección de red Clase B de 172.16.0.0. Esta en realidad es una dirección Internet privada para la red de 5 routers que sirve para las ocho redes que debe definir (5 LAN y 3 WAN). **Puede pedir prestados alrededor de ocho bits para la parte de la dirección que corresponde al host pero todavía debe dejar lugar a por lo menos 100 hosts por subred.** Conteste las siguientes preguntas acerca del diseño de la subred:

1. Escriba aquí la dirección clase B:

2. ¿Cuántos bits pidió prestados?

3. ¿Cuál es la máscara de subred?

4. ¿Cuántas subredes utilizables puede crear?

- 5. ¿Cuántos hosts puede tener cada subred?
- 6. Complete la tabla siguiente con información sobre las 10 primeras subredes (no utilice la subred cero al asignar subredes al diagrama de laboratorio)

Nº de subred	Dirección de subred	Dirección de broadcast de subred	Intervalo de direcciones de host
0 (no se utiliza)			
1			
2			
3			
4			
5			
6			
7			
8			
9			

Paso 3 - Configurar los routers.

A. Conéctese al primer router Lab-A.

Verifique que haya una buena conexión de consola desde la estación de trabajo hacia el router e inicie el programa HyperTerminal (Inicio/Programas/Accessorios/Comunicaciones). Escriba la contraseña cisco si se le indica que entre al modo usuario. El indicador debe ser Lab-A>

B. Entre al modo Exec privilegiado.

Introduzca el comando enable en el indicador del router. Introduzca la contraseña class si se solicita. El indicador ahora debe ser Lab-A#

C. Aplique el esquema de direccionamiento de subred IP a los routers

Decida cuál es la subred que utilizará con cada red y cuál es la dirección IP que aplicará a cada interfaz del router (E0, S0 etc.) y configure el router en consecuencia. Utilice el protocolo de enrutamiento RIP o IGRP. Utilice la planilla de trabajo que aparece a continuación para asignar información de interfaz a cada uno de los cinco routers basándose en las subredes definidas en la tabla anterior. Puede usar la utilidad setup configuration o introducir comandos directamente en el modo de configuración. Puede utilizar la opción help (ayuda) del IOS en cualquier momento. Trabaje en grupos y trate de no consultar sus apuntes. Se pueden encontrar ejemplos de comandos de configuración para el router Lab-A en el final de la sección que corresponde a las respuestas. Las respuestas varían.

7. Complete la tabla que aparece a continuación con la información de interfaz IP para cada uno de los cinco routers.

Configuración IP de router de subred Clase B de laboratorio de Cisco

Nombre del router	Lab-A	Lab-B	Lab-C	Lab-D	Lab-E
Número de modelo					
Dirección IP de la interfaz E0					
Máscara de subred de la interfaz E0					
Dirección IP de la interfaz E1					
Máscara de subred de la interfaz E1					
Dirección IP de la interfaz S0					
Máscara de subred de la interfaz S0					
Velocidad de reloj de la interfaz S0					
Dirección IP de la interfaz S1					
Máscara de subred de la interfaz S1					

Paso 4 - Configurar las estaciones de trabajo.

- A. Utilice la planilla de trabajo que aparece a continuación para asignar información de interfaz a cada estación de trabajo basándose en las subredes definidas anteriormente. Asegúrese de que las direcciones IP de las estaciones de trabajo y los gateways por defecto sean compatibles con la misma LAN en la que está ubicada la interfaz Ethernet del router. Las respuestas varían.
- 8. Complete la información de direccionamiento IP para las estaciones de trabajo. Numere las estaciones de trabajo del diagrama de izquierda a derecha, a partir de la LAN conectada a E1 en el router Lab-A.

Configuración de la dirección IP de la estación de trabajo (las respuestas pueden variar)

№ de estación de trabajo	Dirección IP de la estación de trabajo	Máscara de subred de la estación de trabajo	Dirección IP del gateway por defecto
1 (Lab-A, E1)			
2 (Lab-A, E1)			
3 (Lab-A, E0)			
4 (Lab-A, E0)			
5 (Lab-B, E0)			
6 (Lab-B, E0)			
7 (Lab-C, E0)			
8 (Lab-C, E0)			
9 (Lab-D, E0)			
10 (Lab-E, E0)			

Paso 5 - Probar la conectividad de laboratorio del router.

B. Haga ping desde un router a otro.

Comience con el router Lab-A y utilice la conexión de la estación de trabajo de consola a él. Inicie el programa HyperTerminal y haga ping a la interfaz S1 del router Lab-B. Esto permite verificar si el enlace WAN entre Lab-A y Lab-B es correcto. Haga ping a las interfaces seriales de los demás routers. Lab-A> ping xxx.xxx.xxx (interfaz S1 de Lab-B)

¿El ping que se realizó desde el router Lab-A a Lab-B tuvo éxito?

C. Haga ping desde una estación de trabajo a otra.

Comience con una estación de trabajo conectada al primer hub. Haga clic en el indicador Inicio/Programas/MS-DOS y haga ping a la interfaz S1 del router Lab-B. Esto permite verificar si la configuración IP de la estación de trabajo y el enlace WAN entre Lab-A y Lab-B son correctos. Haga ping a las interfaces seriales de los demás routers y las direcciones IP de las demás estaciones de trabajo para verificar si la red está configurada de forma adecuada.

C:\WINDOWS> ping xxx.xxx.xxx (interfaz S1 del lab-B)

10. ¿El ping que se realizó desde la Estación de trabajo 1 a Lab-B tuvo éxito?

Práctica de laboratorio 1.6.6.1 Actualización del IOS / TFTP- Descripción general

Duración estimada: 30 min.

Objetivos:

9.

- Mostrar información acerca del software Cisco IOS actual y la memoria del router.
- Repasar los requisitos de memoria y las opciones de actualización del software Cisco IOS 12.0
- Utilizar un servidor TFTP para realizar una copia de respaldo desde la Flash de una imagen IOS existente en un router
- Utilizar un servidor TFTP para actualizar un router a una nueva versión del software Cisco IOS

Información básica:

A medida que se publican nuevas versiones del software IOS de Cisco, se hace necesario actualizar periódicamente la imagen IOS existente con el objeto de brindar soporte para las funciones y mejoras recién introducidas. En esta práctica de laboratorio determinará la versión del IOS que se encuentran en ejecución en su server y se familiarizará con los requisitos para actualizarse a una nueva versión. Determinará la cantidad de memoria flash que el router tiene a su disposición, así como la cantidad de ésta que ocupa actualmente la imagen IOS y la cantidad que se encuentra disponible. Es preciso que haga una copia de respaldo del IOS actual antes de actualizarse a una versión más reciente. Además, es aconsejable conservar una copia de respaldo del archivo de imagen IOS para cada router. Se dará un repaso también del proceso de descargar una nueva imagen IOS de la Conexión Cisco en Línea (CCO). En esta práctica de laboratorio se explicará el método de actualización del IOS basado en el servidor TFTP. El objetivo principal de este laboratorio es el de actualizar su router a la versión 12.0 del IOS.

Herramientas / Preparación:

Antes de iniciar esta práctica de laboratorio necesita conectar una estación de trabajo PC con HyperTerminal a la interfaz de consola del router utilizando un cable rollover. Necesitará también una conexión Ethernet al router. El instructor o el asistente de laboratorio debe tener un PC con Windows 9x en el que se haya instalado un servidor TFTP y que cuente con la imagen más reciente de IOS 12.0 en el disco duro. Verifique que el router tenga acceso al servidor TFTP. El servidor TFTP de Cisco y las actualizaciones de IOS más recientes se pueden descargar desde los sitios Web a continuación. Aunque las instrucciones de esta práctica de laboratorio para descargar el software de imagen del firmware sólo pueden ser ejecutadas por una persona que tenga una cuenta de CCO, debe leerlas cuidadosamente para familiarizarse con el proceso.

Puede resultarle útil repasar el capítulo 16 de la Guía del primer año de la Academia de networking de Cisco y la lección 1 del Semestre 3 del currículum en línea antes de empezar esta práctica de laboratorio. Se puede trabajar en forma individual o en equipo.

Recursos requeridos:

- PC con monitor, teclado, ratón y cables de alimentación, etc.
- Sistema operativo Windows (Win 95, 98, NT o 2000) instalado en un PC
- Programa HyperTerminal configurado para acceder a la consola del router
- PC conectado al puerto de consola del router mediante un cable rollover
- PC conectado a un hub al que está conectado el router o a un cable crossover directamente al router
- PC instalado en una red que ejecuta un daemon (servidor) TFTP y que el router pueda enviar y recibir.

Recursos de sitio Web:

Routing basics General information on routers 2500 series routers 1600 series routers Terms and acronyms IP routing protocol IOS command summary Cisco ConfigMaker information and download Cisco TFTP Server (Win 9x version) TFTP Command Syntax Cisco IOS images

Notas:

Paso 1- Conectarse al router.

Conéctese al router con la conexión de consola. Introduzca la contraseña cisco si se solicita. Ingrese en el modo privilegiado con el comando enable. Introduzca la contraseña class.

Paso 2 - Verificar la versión de IOS actual.

Utilice el comando show version para verificar la versión de IOS

1. ¿Qué versión de IOS se está ejecutando actualmente?

Paso 3 - Verificar el archivo de imagen de IOS y la memoria flash.

Utilice el comando **show flash** para obtener información acerca de la memoria Flash y la imagen IOS.

2. Documente la siguiente información del comando show flash.

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

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

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

Paso 4 - Revisar los requisitos de memoria de la imagen de IOS.

Las opciones para actualizar el IOS del router varían según el número de modelo del router, la versión de IOS que se ejecuta actualmente, la cantidad de memoria Flash y la cantidad de memoria DRAM que tiene el router. La siguiente tabla muestra diversas actualizaciones de imágenes IOS disponibles y sus requisitos de memoria. (Nota: Todas las imágenes que se muestran aquí se ejecutan desde la memoria Flash)

Serie de los routers Cisco	Versión del IOS / Conjunto de funciones	*Nombre de la imagen	Tamaño de la imagen	Memoria Flash requerida	Memoria DRAM requerida
1600	11.2(21) - **IP/IPX	C1600-ny-l.112- 21.P.bin	3.729kB	4MB	2MB
1600	12.0(10) - **IP/IPX	C1600-ny-l.120- 10.bin	5.031kB	6MB	4MB
2500	11.2(21) - **IP/IPX/AT/DEC	C2500-d-l.112-21.bin	5.292kB	8MB	4MB
2500	12.0(10)**IP/IPX/AT/DEC	C2500-d-l.120-10.bin	6.730kB	8MB	6MB

Notas: * El último carácter de la parte correspondiente a las funciones del nombre de imagen IOS (por ej., C1600-ny-l) es una letra L minúscula, no un número 1. ** Conjuntos de funciones: IP = protocolo TCP/IP, IPX = protocolo Novell IPX, AT = protocolo AppleTalk, DEC = protocolo DecNet.

Todas las imágenes que se muestran aquí se ejecutan desde la memoria Flash

Paso 5 - Revisar las opciones para obtener el archivo de imagen del IOS.

Puede obtener una imagen del IOS adquiriendo un paquete de Software Cisco IOS (SFP) o descargando el IOS desde el sitio Web de Cisco. También puede utilizar una copia de respaldo de otro router si tiene una versión más reciente. Todas las opciones deben cumplir con el acuerdo de licencia del software Cisco IOS.

A. Paquete de funciones de software (SFP)

El SFP generalmente viene en un paquete para una serie específica de routers como, por ejemplo, la serie 2500, e incluye instrucciones, notas de versión y un CD con varias versiones del IOS, el servidor TFTP de Cisco para Win 9x y el Cargador de software del router (RSL). RSL es una utilidad de aplicación de software Windows 9x que ayuda a cargar nuevas imágenes del IOS y se describe más adelante en esta práctica de laboratorio. Los SFP se pueden pedir a Cisco o a un distribuidor autorizado. Si no tiene un SFP con RSL debe descargar la imagen del IOS del sitio Web de Cisco y utilizar el método TFTP. El método RSL para actualizar el IOS del router se describe en la siguiente práctica de laboratorio, utilizando el paquete de software

B. Sitio Web de Cisco

Las versiones más recientes del IOS se pueden descargar del sitio Web de Cisco (www.cisco.com) y puede elegir entre varios conjuntos de funciones para las distintas series de routers (1600, 2500 etc.). También hay mucha información disponible acerca de las versiones de IOS, los conjuntos de funciones, las capacidades y los requisitos. Una vez que ha descargado la imagen la puede utilizar para actualizar el router utilizando TFTP. En esta práctica de laboratorio se describe el procedimiento TFTP. Es necesario tener un acuerdo de servicio SmartNet de Cisco y una cuenta de conexión de Cisco Connection Online (CCO) para poder descargar archivos del IOS.

C. Copia de respaldo de IOS desde otro router

Si tiene un router de la misma serie y número de modelo con un IOS más reciente, a veces puede copiar el IOS existente desde la memoria flash de ese router en un servidor TFTP. Luego puede cargar esta imagen en el nuevo router desde el servidor TFTP. En esta práctica de laboratorio se describe el procedimiento TFTP.

Paso 6 - Descargar el archivo de imagen del IOS.

A. Conéctese al sitio Web www.cisco.com.

Inicie el navegador, vaya al sitio Web <u>www.cisco.com</u> y conéctese. Debe tener una cuenta CCO. Si no se conecta con una cuenta CCO, no obtendrá permiso para realizar la descarga. Todas las academias de Cisco deben tener un acuerdo de servicio SmartNet para el equipo de laboratorio del router. Si cuenta con un acuerdo SmartNet, usted o el representante de la academia (el instructor o el contacto principal) también debe tener una cuenta de conexión CCO.

B. Navegue hasta la ubicación de descarga

Haga clic en Software Center (Centro de software) bajo Service and Support (Servicios y asistencia). En Software Center haga clic en IOS Upgrade Planner (Planificador de actualización de IOS) y luego haga clic en IOS 12.0. Nota: También puede descargar la versión 11.2 para practicar la actualización de una versión anterior de IOS.

C. Seleccione la plataforma y versión

Seleccione la plataforma (serie del router) para el IOS que desea descargar (por ej., 1601-1604 ó 2501-2525). Luego seleccione la **Major Release Update (Actualización de versión principal) (por ej., IOS 12.0 versión 10 ó 12.0.10) más reciente**. Se emiten nuevas versiones con regularidad y por lo general debe utilizar la versión principal más reciente disponible. En lo posible, trate de evitar la utilización de versiones anteriores que terminen con la letra T (por ej., 12.0.5T).

D. Seleccione las funciones del software

Seleccione el conjunto de funciones del software (Software Feature) que desee. Nota: cuantas más funciones tenga, más memoria ocupará esa versión del IOS. Seleccione el conjunto de funciones IP/IPX. La siguiente pantalla confirma la Plataforma, la versión de IOS, la Versión y el conjunto de funciones que ha elegido. También le permite saber cuál es la cantidad mínima de memoria Flash y de memoria DRAM que requiere esta versión. Verifique si el router que desea actualizar tiene suficiente memoria disponible para soportar esta versión. (Nota: La mayoría de los routers de la serie 1600 tienen solamente 6MB de memoria flash y 4MB de RAM,

mientras que la mayoría de los routers de la serie 2500 tienen 8MB de memoria flash y 8MB de RAM.) Se visualiza la siguiente información:

1601-1604 12.0.10 IP/IPX Minimum Recommended Memory to download image - 6 MB Flash and 4 MB RAM (memoria mínima recomendada para descargar imagen - 6 MB Flash y 4 MB RAM)

Haga clic en el botón: "I have read the above requirements and agree with them" (He leído los requisitos anteriores y los acepto)

E. Iniciar la descarga de la imagen de IOS Confirme la información de imagen de IOS que aparece en pantalla (consulte la información que aparece a continuación) y haga clic en File Name (Nombre de archivo) para iniciar la descarga. Lea el Acuerdo de Licencia de Software y luego haga clic en YES (SI) si lo acepta. Seleccione el sitio de descarga HTTP (o FTP). Haga clic en el botón "Save to Disk" (guardar en el disco duro) y luego seleccione el directorio local donde desea descargar el archivo de imagen del IOS.

Descarga de Software				
Nombre de archivo	Descripción	Tamaño en 'Bytes'	Fecha de publicación	Más información
C1600-ny-l.112- 10.bin	IP/IPX	5151224	03/27/2000 05:46:22	?

Una vez que se ha completado la descarga, puede cargar la imagen del IOS en el router utilizando TFTP.

Paso 7 - Verificar la conexión entre el router y el servidor TFTP.

Desde el router que va a actualizar, introduzca ping xxx.xxx.xxx (la dirección IP de la estación de trabajo que ejecuta el servidor TFTP).

3. ¿Cuál fue el resultado del comando ping?

Paso 8 - Verificar la ubicación del archivo del servidor TFTP.

Verifique la ubicación del directorio raíz del servidor TFTP dado que esta es la ubicación donde se guardará la copia de respaldo del archivo de imagen del IOS existente y del nuevo archivo de imagen del IOS. Asegúrese de copiar la nueva imagen IOS que se ha descargado en este directorio del PC antes de iniciar la actualización del IOS. Haga clic en View/Options (Ver/Opciones) y anote la ubicación o examine y cambie la ubicación por otro directorio.

4. ¿Cuál es la ubicación por defecto del directorio raíz del servidor TFTP?

Paso 9 - Hacer una copia de respaldo de la imagen del software Cisco IOS existente.

Introduzca copy flash tftp en el indicador del router El router le solicita la dirección IP o el nombre de host del host tftp. Introduzca la dirección IP del servidor tftp.

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

6. ¿Cuál es el archivo que se escribe en el servidor TFTP?

7. ¿Cuál fue la respuesta del router al copiar el archivo?

Paso 10 - Verificar la copia de respaldo del archivo del IOS que se copió en el servidor TFTP.

Verifique el servidor TFTP utilizando el explorador de Windows, el comando DIR o el comando ls UNIX para el archivo que acaba de escribir.

8. ¿Cuál es el tamaño en bytes del archivo que se escribió?

Paso 11 - Cargar la nueva imagen del IOS que se descargó desde el servidor TFTP..

Teclee copy tftp flash en el prompt del router. El router le pide la dirección IP o el nombre de host del host tftp. Introduzca la dirección IP del servidor tftp. Introduzca el nombre de la nueva imagen del IOS que se descargó anteriormente si se le solicita. También se le indicará que borre la flash antes de comenzar. Este proceso copiará el nuevo software Cisco IOS desde un host tftp a la flash del router.

9. Anote algunos de los indicadores y las respuestas que aparecieron en la pantalla del router. Nota: Puede utilizar HyperTerminal o la opción copiar / pegar de Windows para capturar el proceso de copia a medida que se realiza.

Paso 12 - Verificar la versión de IOS luego de la actualización.

Utilice el comando show version para verificar la versión de IOS

10. ¿Qué versión de IOS se está ejecutando después de la actualización?

Paso 13 - Verificar el archivo de imagen del IOS y la memoria flash después de la actualización.

Utilice el comando **show flash** para obtener información acerca de la memoria Flash y la imagen IOS.

11. Documente la siguiente información desde el comando **show flash** luego de la actualización del IOS.

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

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

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

Práctica de laboratorio 1.6.6.2 Actualización de la memoria del router - Descripción general

Duración estimada: 30 min.

Objetivos:

- Mostrar información acerca del software Cisco IOS actual y la memoria del router
- Repasar los pasos para la actualización de la memoria DRAM del router
- Repasar los pasos para la actualización de la memoria Flash del router

Información básica:

En esta práctica de laboratorio, determinará cuál es la versión y el IOS que el router ejecuta en la actualidad y se familiarizará con los requisitos necesarios para realizar la actualización a una versión más reciente. Verifique cuánta memoria flash tiene el router, cuánta de esa memoria utiliza en la actualidad la imagen IOS (código de sistema) y cuánta de esa memoria está disponible. También verificará la cantidad de DRAM (Memoria dinámica de acceso aleatorio).

Con los routers Cisco 1600 y 2500 y la mayoría de las imágenes de IOS, el IOS generalmente se ejecuta desde la memoria flash. Si determina que no hay suficiente memoria flash para realizar la actualización a una versión de IOS más grande y reciente, es necesario ejecutar una actualización de la memoria flash. Es posible que también deba actualizar el SIMM de DRAM si está actualizando el conjunto de funciones o la versión del software Cisco IOS si el router tiene tablas de enrutamiento grandes u otras funciones que usan mucha memoria, tales como spoofing o traducciones de protocolos. Si un router de la serie 2500 NO tiene 8MB de Flash Y 4MB de RAM, es necesario obtener e instalar módulos de memoria adicional. En esta práctica de laboratorio se describe el procedimiento para actualizar los SIMM (módulos de memoria en línea simples) de la DRAM y la flash para un router Cisco 2500.

Herramientas / Preparación:

Antes de iniciar esta práctica de laboratorio necesita conectar una estación de trabajo PC con HyperTerminal a la interfaz de consola del router utilizando un cable rollover. También necesita una conexión Ethernet al router. También debe haber un servidor TFTP disponible para realizar una copia de respaldo del IOS antes de reemplazar los SIMM de la flash. Aunque es posible que las instrucciones en esta práctica de laboratorio para actualizar la memoria flash del router no sean necesarias para la configuración de laboratorio, debe repasarlas para familiarizarse con el proceso.

Puede resultarle útil repasar el capítulo 16 de la Guía del primer año de la Academia de networking de Cisco y la lección 1 del Semestre 3 del currículum en línea antes de empezar esta práctica de laboratorio. Se debe trabajar en grupos. Observe que las instrucciones detalladas se pueden encontrar en el sitio Web que aparece a continuación. Se puede descargar un archivo PDF.

Recursos requeridos:

- PC con monitor, teclado, ratón y cables de alimentación, etc.
- Sistema operativo Windows (Win 95, 98, NT o 2000) instalado en un PC
- Programa HyperTerminal configurado para acceder a la consola del router
- PC conectado al puerto de consola del router mediante un cable rollover
- PC conectado a un hub al que está conectado el router o a un cable crossover directamente al router
- PC instalado en una red a la que el router pueda enviar y recibir, que ejecute un daemon (servidor) TFTP.
- Destornillador de hoja plana de tamaño mediano (1/4 de pulgada (0,625 cm))
- Correa para muñeca para evitar ESD (descargas electrostáticas)
- El SIMM de DRAM requerido para la actualización planificada
- Los SIMM de código de sistema

Recursos de sitio Web:

Routing basics General information on routers 2500 series routers 1600 series routers Terms and acronyms IP routing protocol IOS command summary Cisco TFTP Server (Win 9x version) TFTP Command Syntax Maintaining and upgrading the 2500 router

Notas:

•

Paso 1- Conectarse al router.

Conectarse al router mediante la conexión de consola. Introducir la contraseña **cisco** si se solicita. Entrar en el modo privilegiado con el comando **enable**. Introduzca la contraseña **class**.

Paso 2 - Verificar la versión actual del IOS y la cantidad de DRAM.

Utilice el comando show version para verificar la versión de IOS y la cantidad de DRAM.

1. ¿Qué versión de IOS se está ejecutando actualmente?

2. ¿Cuánta DRAM hay instalada?

Paso 3 - Verificar el archivo de imagen IOS y la memoria flash.

Utilice el comando **show flash** para obtener información acerca de la memoria Flash y la imagen IOS.

3. Documente la siguiente información desde el comando show flash.

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

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

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

Paso 4 - Revisar los requisitos de memoria de la imagen IOS.

Las opciones para actualizar el IOS del router varían según el número de modelo del router, la versión de IOS que se ejecuta actualmente, la cantidad de memoria Flash y la cantidad de memoria DRAM que tiene el router. La siguiente tabla muestra diversas actualizaciones de imágenes IOS disponibles y sus requisitos de memoria.

Serie de los Versión del IOS /	*Nombre de la Tamaño de	Memoria	Memoria DRAM
--------------------------------	-------------------------	---------	--------------

routers Cisco	Conjunto de funciones	imagen	la imagen	Flash requerida	requerida
1600	1.2(21) - **IP/IPX	C1600-ny- I.112-21.P.bin	3.729kB	4MB	2MB
1600	12.0(10) - **IP/IPX	C1600-ny- I.120-10.bin	5.031kB	6MB	4MB
2500	11.2(21) - **IP/IPX/AT/DEC	C2500-d-l.112- 21.bin	5.292kB	8MB	4MB
2500	12.0(10) **IP/IPX/AT/DEC	C2500-d-l.120- 10.bin	6.730kB	8MB	6MB

Notas: * El último carácter de la parte correspondiente a las funciones del nombre de imagen IOS (por ej., C1600-ny-l) es una letra L minúscula, no un número 1. ** Conjuntos de funciones: IP = protocolo TCP/IP, IPX = protocolo Novell IPX, AT = protocolo AppleTalk, DEC = protocolo DecNet. Todas las imágenes que se muestran aquí se ejecutan desde la memoria Flash

Sección 2 - Disposición de las tarjetas de sistema del router para la serie Cisco 2500

Tarjeta de sistema del modelo Cisco 2501, 2501, 2502, 2503 y 2504 (SIMM colocados)



Tarjeta de sistema del modelo Cisco 2514 (SIMM eliminados)



Sección 3 - Actualización del SIMM de DRAM

Esta sección describe cómo actualizar el SIMM de DRAM en la tarjeta de sistema. Ejecute los siguientes pasos para instalar los SIMM de DRAM.

Paso 1- DESCONECTAR el router.

Paso 2 - Colocarse una correa para muñeca para evitar descargas electrostáticas.

Paso 3 - Abrir la tapa

Siga las instrucciones de la sección "Apertura del chasis" del documento de Web.

Paso 4 - Retirar el SIMM de DRAM existente

Tire de los conectores hacia afuera para desconectarlos, como se indica más adelante. Asegúrese de no romper las abrazaderas del conector del SIMM.

Paso 5 - Instalar el nuevo SIMM

Coloque el nuevo SIMM de modo que la muesca de polarización quede ubicada a la izquierda de la toma del SIMM. (ver la figura que aparece a continuación)



Paso 6 - Insertar el nuevo SIMM de DRAM

Deslice el extremo con las patas de metal en la toma del conector del SIMM aproximadamente en un ángulo de 45 grados con respecto a la tarjeta de sistema. Oscile con cuidado el SIMM para colocarlo nuevamente en su lugar hasta que la traba de cualquiera de los lados se ubique en la posición correcta. Realice esta operación con cuidado porque el conector se puede romper.

Paso 7 -Volver a colocar la tapa del router.

Sección 4 - Actualización de la SIMM de la flash de código de sistema

Paso 1- DESCONECTAR el router.

Paso 2 - Colocarse una correa para muñeca para evitar descargas electrostáticas.

Paso 3- Abrir la tapa

Siga las instrucciones de la sección "Apertura del chasis" del documento de Web.

Paso 5 - Preparación para la instalación del SIMM de código de sistema

Hay dos tomas SIMM (memoria Flash) de código de sistema en la tarjeta de sistema. Si desea instalar los SIMM de código de sistema en ambas tomas, los SIMM deben tener el mismo tamaño. Por ejemplo, si ya hay un SIMM de código de sistema de 4 MB instalado en el router, el nuevo SIMM también debe tener 4 MB: Esta actualización le suministra un total de 8 MB.

Precaución: El código de sistema se guarda en los SIMM de la memoria Flash, pero los nuevos SIMM de código de sistema salen de fábrica sin software preinstalado. Antes de continuar con este procedimiento, utilice el comando <u>copy flash tftp</u> para realizar una copia de respaldo del código de sistema en un servidor TFTP. El proceso de copia de respaldo / restauración del servidor TFTP se describe en una práctica de laboratorio anterior.

Paso 6 - Cambiar los SIMM de la Flash.

Si está reemplazando un SIMM de 4 MB por un SIMM de 8 MB, ese SIMM de 8 MB se debe colocar en la toma 0 del SIMM. Si está agregando SIMM y se debe ubicar uno al lado del otro en la tarjeta de sistema, los SIMM deben tener el mismo tamaño, por ej., dos SIMM de 4 MB, y NO un SIMM de 4 MB y uno de 8 MB juntos.

Ubique las tomas de SIMM, rotuladas CODE 0 y CODE 1 en la tarjeta de sistema. De ser necesario, retire el SIMM de código de sistema existente empujando hacia afuera las abrazaderas del conector para destrabarlas. Si está instalando los SIMM de código de sistema en ambas tomas (CODE0 y CODE1), los SIMM deben tener el mismo tamaño. En primer lugar, coloque el SIMM en la toma rotulada CODE0; luego coloque el SIMM en la toma CODE1.

Paso 7- Reconfigurar la partición flash (de ser necesario).

Una vez que ha agregado el SIMM de la Flash, si el comando **show flash** del router indica que la memoria Flash tiene dos particiones, es necesario reconfigurar esa partición desde el router. El proceso de repartición del router implica borrar la memoria Flash, de modo que primero debe rearrancar el router para que se ejecute en modo ROM.

A. Reconfigure el router para arrancar desde la ROM. Cambie el config-register a 0x2101 y vuelva a cargarlo, utilizando los siguientes comandos:

```
Router#configure terminal
Introduzca los comandos de configuración, de a uno por línea. Finalice
con CNTL/Z Router(config)#config-register 0x2101
Router(config)#exit
Router#reload
```

Nota: Esto hará que el router se inicie en modo de arranque y que la Flash esté inactiva. No se puede cambiar la partición cuando el router se ejecuta bajo un IOS completo desde la Flash. Aparece un indicador del router distinto, pero las contraseñas de habilitación y la mayoría de los comandos son los mismos.

Router(boot)>enable Contraseña: Router(boot)#

B. Borre la Flash, incluyendo ambas particiones. Precaución: Es necesario que haga una copia de respaldo de la imagen IOS que ya está guardada en el servidor tftp ya que esto borrará todos los archivos de la Flash - ¡y la Flash es el lugar donde un 2500 guarda el IOS por defecto!

Router(boot)#erase flash

El router le indica que debe borrar ambas particiones (debe confirmar la sobreescritura y la eliminación de la flash).

C. Reparticionar la Flash

Ahora debe reparticionar la flash en una partición con un tamaño de 8 MB (si tiene dos SIMM de 4 MB instalados).

Router(boot)#configure t Router(boot)(config)#partition flash 1 8

D. Copie la imagen IOS que tiene guardada nuevamente en la flash

Utilice el comando copy tftp flash para recuperar la copia de respaldo de la imagen IOS en la memoria flash. El procedimiento de copia de respaldo / restauración del servidor TFTP se describe en una práctica de laboratorio anterior.

E. Cambie el config-register para arrancar desde la Flash

Cambie el config register para que el router examine la NVRAM buscando los comandos del sistema de arranque ("config-register 0x2102") que cargará la imagen IOS desde la flash. Salga y vuelva a arrancar; ahora el router debe indicar "8192k bytes of processor board System flash

Router(boot)(config)#config-register 0x2102
Router(boot)(config)#exit
Router(boot)#reload

Actividad de laboratorio interactiva (Flash, 604 kB)

En esta actividad de laboratorio con el router, se le presentará la oportunidad de realizar una configuración paso a paso del Router A (lab_A) en la topología del laboratorio. Trate de completar el laboratorio sin recurrir a sus apuntes o a su diario. Sin embargo, si no sabe cómo realizar un paso y si ha utilizado el currículum, sus notas y su diario para tratar de entenderlo, puede utilizar el botón "Ejecutar demo", que muestra la secuencia de configuración en letras rojas. Recuerde que esta secuencia de pasos de configuración es tan sólo una de muchas secuencias posibles.

¿Cuál es la diferencia entre esta actividad y un verdadero router?

Siga los pasos con EXACTITUD y en el mismo orden con que se le presenten. Con un router de verdad, y en una actividad que realizará más adelante, puede introducir los comandos con muchas secuencias diferentes, todas ellas correctas. En esta actividad, le "guiamos" un poco más.

No se proporciona ayuda contextual "?"

Recuerde que no basta con configurar la dirección ip en una interfaz; también debe emitir un comando "no shutdown".

Debe usar exit; CONTROL-Z no funciona

En este laboratorio debe utilizar el comando IOS COMPLETO, no las abreviaturas que seguramente utilizará una vez que haya aprendido el conjunto básico de comandos IOS. Por ejemplo, para entrar en el modo de configuración global debe escribir "configure terminal"; sin embargo, una vez que haya ganado experiencia con los routers, podrá usar la abreviatura "config t".

Después de escribir un comando, presione ENTER. Se le permitirá continuar con el siguiente paso o se le presentará un mensaje de error, el cual puede servir de ayuda para que corrija el error. Si esto no da resultado, puede recurrir a "Ejecutar demo".

Cuando se le pida que configure el puerto de consola, la secuencia que debe usar es "line console 0", seguido de "login", seguido de "password cisco." Si se le pide que configure telnet, la secuencia de comandos es "line vty 0 4", seguido de "login", seguido de "password cisco."

Actividad de laboratorio interactiva (Flash, 412 kB)

En esta actividad de laboratorio en línea, configurará el router Lab-A basándose en la topología estándar del Semestre 2. Debe realizar esta configuración independientemente desde la línea de comando, sin recurrir notas o apuntes, sólo la topología de la red. Puede utilizar la función de ayuda de router (?), pero tenga en cuenta que se encuentra disponible sólo un conjunto limitado de comandos IOS. El objetivo es de configurar el router correctamente y tan rápido como sea posible. Esta actividad sirve como práctica para el verdadero laboratorio de router, la cual puede realizar mientras otros alumnos ocupan los routers. Acuérdese que una actividad de esta clase no sustituye al uso de los verdaderos routers.

Se debe tener en cuenta lo siguiente: Primero, si bien los comandos pueden introducirse en una amplia variedad de secuencias, ciertos comandos IOS siempre deben preceder a otros. Por ejemplo, se debe escribir config t antes de que se puedan introducir los comandos de configuración, y se debe escribir exit (CTRL-Z no funciona en esta actividad) para regresar a un modo diferente. La única manera de modificar un renglón antes de presionar ENTER consiste en usar la tecla de retroceso (no funcionan las demás opciones de edición normales de IOS). Por último, si bien se han aceptado unas pocas abreviaturas comunes, la mayoría de los comandos IOS deben escribirse en su totalidad.

¡Buena suerte!

Práctica de laboratorio 2.3.7 Características del switch - Descripción general



Duración estimada: 30 min.

Objetivos:

- Determinar el número de modelo de un switch Ethernet y cuáles son sus interfaces físicas (puertos).
- Identificar los cables, conexiones y dispositivos que se pueden conectar al switch
- Verificar y/o modificar los parámetros de configuración de HyperTerminal
- Conectarse al switch como su consola utilizando el PC e HyperTerminal.

Información básica:

En esta práctica de laboratorio examinará un Switch Ethernet para reunir información acerca de sus características físicas y empezar a apreciar la función de los switches en una red. Usted determinará el número de modelo y características de un switch específico incluyendo cuáles son las interfaces existentes y cuáles son el cableado y los dispositivos con los que están conectadas.

Un switch es un dispositivo de red de Capa 2 (enlace de datos) que actúa como el punto de concentración para la conexión de estaciones de trabajo, servidores, routers, hubs y otros switches. Un "hub" es un tipo antiguo de dispositivo de concentración que proporciona varios puertos, similar al switch salvo que con el hub, todas las estaciones de trabajo comparten el ancho de banda (10Mbps con Ethernet estándar) y se producen colisiones. Los hubs operan en half duplex (sólo pueden enviar o recibir) ya que deben ser capaces de detectar colisiones. Un switch proporciona una conexión dedicada punto a punto (circuito virtual) entre dos dispositivos de networking (tal como, estaciones de trabajo, servidores y routers) de manera que no hay colisiones. Como no tienen que detectar colisiones, pueden operar en modo full-duplex (envío y recepción simultáneos), que duplica efectivamente el rendimiento Los switches Ethernet están disponibles en varias velocidades incluyendo 10Mbps (Ethernet estándar), 100Mbps (Fast Ethernet) y 1000Mbps (Gigabit Ethernet).

A veces, se hace referencia a los switches como puentes multipuerto y representan la tecnología más avanzada para las redes actuales de área local (LAN) con cableado en estrella de Ethernet. Al igual que los routers, los switches son PC dedicados que contienen a CPU, RAM y un sistema operativo (IOS). Como ocurre con los routers, un switch se puede manejar conectándose al puerto de consola para permitirle ver y realizar cambios a la configuración. Muchos de los switches más modernos poseen un servidor web (HTTP) incorporado y también se pueden manejar a través de su dirección IP utilizando un PC y una interfaz de navegador como Netscape o Internet Explorer. La capacidad para comprender y configurar switches es esencial para el soporte de la red.

Herramientas / Preparación:

Un switch debe estar disponible con una estación de trabajo de PC conectada como consola con HyperTerminal instalado y debidamente configurado para acceder al switch. El switch debe estar colocado de forma tal que todos los lados estén visibles, de modo que se puedan inspeccionar todas las conexiones físicas y cables. Como es posible que sólo haya un switch disponible, el instructor debe como mínimo hacer una demostración con esta práctica de laboratorio; los estudiantes deben trabajar en grupos más grandes para poder trabajar en la práctica. Mientras un equipo está trabajando con el switch, los demás pueden realizar una investigación sobre switches en el sitio Web de Cisco, en los URL que aparecen a continuación. Antes de comenzar con esta práctica de laboratorio, puede resultarle útil repasar el capítulo 2 (Conmutación LAN) de la Guía del segundo año de la Academia de networking de Cisco. También conviene repasar la Lección 2 en línea del Semestre 3. Se requieren los siguientes recursos:

- PC Windows c/ HyperTerminal instalado
- Switch Cisco (modelo 19xx o 28xx) con manuales
- Cable de consola (Rollover)
- Cable CAT5 de la estación de trabajo al switch

Recursos de sitio Web:

- LAN Switching basics
- General information on all Cisco products (Ir al capítulo 22 Switches)
- <u>1900 / 2820 series Ethernet switches</u>
- 2900 series Fast Ethernet switches
- <u>3500 series Gigabit Ethernet switches</u>

Cisco switch clustering technology

Notas:

Paso 1 - Examinar el switch LAN adelante y atrás.

Responda a las siguientes preguntas. (Nota: Las respuestas varían según el modelo del switch). Es posible que desee consultar la Guía de instalación y configuración del switch con el cual está trabajando.

1. ¿Cuál es el número de modelo del switch?

2. ¿Cuál es el número de serie del sistema del switch?

3. ¿Puede ver algún puerto de consola? (S/N)

¿A cuál de los puertos de la terminal de consola (estación de trabajo de PC) está conectado?

4. ¿Qué tipo de cable es el cable de consola (roll-over, de conexión cruzada o de conexión directa)?

5. ¿Puede ver algún puerto AUI? (S/N)

¿Qué significa AUI y para qué se puede usar este puerto?

6. ¿Qué tipo de cable o adaptador se puede usar con el puerto AUI?

7. ¿Existe un conmutador de ENCENDIDO/APAGADO de la energía eléctrica? (S/N)

¿Cómo se hace para encender el switch?

8. ¿Cuál es la cantidad total de puertos en la parte delantera del switch para la conexión de estaciones de trabajo, servidores, routers, hubs u otros switches?

9. ¿Cuántos puertos Ethernet 10Mbps hay?

10. ¿Son puertos cruzados?

¿Cómo lo puede comprobar?

11. ¿Qué tipo(s) de conector(es) se utilizan?

12. ¿Cuántos puertos Fast Ethernet 100Mbps hay?

13. ¿Son puertos cruzados?

¿Cómo lo puede comprobar?

14. ¿Qué tipo(s) de conector(es) se utilizan?

15. ¿Qué tipo de luces indicadoras (LEDs) se encuentran en la parte delantera del switch?

16. ¿Qué botón se encuentra en la parte delantera del switch?

¿Para qué se usa?

Paso 2 - Revisión de las respuestas en relación al Paso 1 y registro de la información de interfaz.

Use la siguiente tabla para enumerar y resumir las características de todas las interfaces (o conectores de puerto) en el switch. Si no existe ningún cable conectado al puerto, identifique el tipo / conector de cable que se utilizaría comúnmente.

Interfaz del switch / Identificador de puerto	Tipo de cable/ Conector	Dispositivo y puerto a los que está conectado el cable

Paso 3 - Revisión de la configuración del programa HyperTerminal de la estación de trabajo.

1. Haga clic en Inicio/Programas/Accesorios/Comunicaciones y luego en HyperTerminal. Haga clic con el botón derecho del mouse en el icono que se ha definido para el acceso por consola al switch y luego haga clic en Propiedades. El nombre del icono puede ser cisco.ht o algún nombre similar. Si no existe ningún icono, puede crearlo utilizando los valores que aparecen en las respuestas de la planilla de trabajo. En la pantalla Properties, haga clic en la ficha Phone Number (Número de teléfono) y luego haga clic en el botón Configure (Configurar). Complete la siguiente tabla con la información que se suministra.

Opción de configuración	Parámetro(s) actual(es)
Puerto COM	
Bits por segundo	
Bits de datos	
Paridad	
Bits de parada	
Control de flujo	

Práctica de laboratorio 2.3.10.1: Consola de administración de switch - Descripción general

Duración estimada: 60 min.

Objetivos:

- Explorar los menús de la Interfaz del usuario de la consola de administración del
- switch.
 - Determinar el número de modelo del switch y la dirección MAC

- Documentar las opciones primarias del menú de interfaz del usuario
- Utilizar los menús de la Consola de administración para ver y configurar los valores de dirección IP del switch.
 - Documentar las opciones del menú de configuración de la dirección IP.
 - Verificar los valores de red de las estaciones de trabajo para comprobar la compatibilidad con los valores de los switches y routers

Información básica:

Esta práctica de laboratorio ayudará a desarrollar una comprensión básica de la administración del switch Ethernet y lo ayudará a prepararse para las lecciones de conmutación más avanzadas como las VLAN. Trabajará con los menús de Interfaz del usuario de la consola de administración del switch para configurar algunas opciones de conmutación básicas. La administración del switch se puede realizar a través de una interfaz administrada con menús como la Consola de administración o a través de una interfaz de línea de comando (CLI) como con la mayoría de los routers.

En esta práctica de laboratorio, se conectará a través de la consola con el switch y podrá ver las opciones de menú disponibles con el menú de interfaz del usuario a fin de familiarizarse con los distintos tipos de configuraciones y acciones que se pueden realizar al configurar el switch. También deberá establecer la dirección IP del switch utilizando la Consola de administración y usar la función Panel de control/Redes de la estación de trabajo para verificar que la configuración de dirección IP sea compatible con la dirección IP del switch. Es fundamental familiarizarse con los switches y su administración para lograr un soporte exitoso de las redes Ethernet actuales.

Herramientas / Preparación:

Antes de comenzar con la práctica de laboratorio, el profesor o asistente de laboratorio debe preparar un switch con los valores VLAN por defecto. Se debe colocar también a disposición de los estudiantes una estación de trabajo con HyperTerminal para realizar la conexión de consola al switch y una conexión Ethernet para hacer Telnet al switch. Como es posible que sólo haya un switch disponible, el instructor debe como mínimo hacer una demostración con esta práctica de laboratorio; los estudiantes deben trabajar en grupos más grandes para poder trabajar en la práctica. Mientras un equipo está trabajando con el switch, los demás pueden realizar una investigación sobre switches en el sitio Web de Cisco, en los URL que aparecen a continuación. Antes de iniciar esta práctica de laboratorio, le aconsejamos que lea el capítulo 2 sobre conmutación LAN en la Guía del segundo año de la Academia de networking. También debe repasar la Lección en línea 2 del Semestre 3. A continuación, presentamos una lista del equipo requerido.

- PC Windows c/ HyperTerminal instalado (configurado para conexión de consola al switch)
- Switch Cisco (modelo 19xx, 28xx, 29xx)
- Cable de consola (roll-over)
- Cable Ethernet CAT 5 desde la estación de trabajo a un puerto Ethernet de switch

Recursos de sitio Web:

- LAN Switching basics
- General information on all Cisco products (Ir al capítulo 22 Switches)
- 1900 / 2820 series Ethernet switches
- 2900 series Fast Ethernet switches
- <u>3500 series Gigabit Ethernet switches</u>
- Cisco switch clustering technology

Notas:

Paso 1- Conectar la estación de trabajo al puerto de consola del switch y active el switch

Espere unos pocos minutos para que el switch arranque y aparecerá un menú de opciones conocido como la "Consola de administración" (versión 1900). Este ejercicio lo ayudará a familiarizarse con las distintas opciones de menú disponibles.

1. ¿Cuál es el número de modelo del switch?

2. ¿Cuál es la dirección Ethernet (dirección MAC de Capa 2) del switch?

3. Complete la siguiente tabla con las opciones del Menú principal disponibles. (Las respuestas varían según el modelo del switch y el firmware)

Opción de menú	Descripción de las opciones del menú	Opciones de submenú (enumerar dos o más)

Opciones del menú disponibles desde un switch Ethernet Cisco Catalyst 1924 (10 Mbps)

Paso 2- Utilizar la Consola de administración para configurar el acceso IP.

La dirección IP del switch se puede utilizar para hacer Ping o Telnet al switch. No se requiere asignar una dirección IP a un switch pero se recomienda para la administración de un switch remoto. En algunos switches más modernos la dirección IP se puede utilizar para acceder al switch utilizando la interfaz de administración del navegador basado en Web. Cuando se administra un switch, el "dominio de administración" es siempre VLAN 1. Todos los puertos se asignan a VLAN 1 por defecto.

4. Seleccione la configuración IP en los menús. Utilizando la tabla que aparece a continuación, enumere las primeras 5 "Configuraciones" en el menú de configuración IP y sus valores. ¿Cuál es la primera "Acción" disponible?

Configuración	Configuración / Descripción de acción	Valor de configuración
I	Dirección IP	
S	Máscara de subred	
D	Gateway por defecto	
V	VLAN de administración	
М	Dirección IP del servidor DNS 1	
Р	Ping	

Opciones del menú disponibles desde un switch Ethernet Cisco Catalyst 1912 (10 Mbps)

5. Asigne una dirección IP y máscara de subred al switch Asegúrese de usar una dirección IP y máscara de subred que sean compatibles con la red o subred en la que se encuentra actualmente el switch. Si el switch se conecta al Router Lab-A, Interfaz E1 (205.7.5.1) como se ve en el diagrama de configuración estándar de laboratorio, entonces asigne una dirección IP compatible y máscara de subred al switch.

Dirección IP:

Máscara de subred:

6. Verifique que todos los puertos se asignen a VLAN 1. Enumere los puertos actualmente asignados a VLAN 1 por defecto:

7. Configure una estación de trabajo con una configuración de red TCP/IP que sea compatible con la dirección IP del switch y la dirección (E1) de la interfaz del router. Asegúrese de establecer la dirección IP de la estación de trabajo, la máscara de subred y el gateway por defecto (interfaz del router cercano).

Dirección IP:

Máscara de subred:

Gateway por defecto:

Práctica de laboratorio 2.3.10.2: Opciones de puerto de switch - Descripción general

Duración estimada: 20 min.

Objetivos:

- Trabajar con los menús de Interfaz del usuario para consola de administración a fin de determinar el número de modelo del switch, la dirección MAC y la revisión de firmware
- Utilizar el menú de configuración del sistema para configurar la operación Libre de fragmentos
- Utilizar el menú de configuración de puerto para habilitar la operación full-duplex
- Utilice el menú de configuración de puerto para habilitar la operación Puerto rápido

Información básica:

En esta práctica de laboratorio trabajará con los menús de interfaz de la Consola de administración a fin de configurar un switch para operar en el modo de conmutación libre de fragmentos. También deberá configurar un puerto para permitir una operación FULL DUPLEX y de Puerto rápido. La mayoría de los switches se pueden configurar con estas opciones.

Operación libre de fragmentos

Los switches tienen 3 modos de operación; 1) Método de corte o rápido, 2) Almacenamiento y envío y 3) Libre de fragmentos. En el modo de conmutación rápida, el switch sólo lee la dirección MAC destino del encabezado de la trama y luego envía inmediatamente la trama. Este modo es el más rápido paro también puede enviar fragmentos de colisión menores de 64 bytes (un runt). Almacenamiento y envío espera hasta recibir la trama completa (hasta 1.518 bytes) antes de enviar la trama. Es el modo de conmutación más lento pero el que produce menos errores. El modo libre de fragmentos reduce el retardo ya que toma la decisión de envío luego de recibir los primeros 64 bytes. Esto significa que no se enviará ningún "runt", que es el tipo más común de trama defectuosa de Ethernet. El modo libre de fragmentos es la mejor opción para obtener un equilibrio entre la velocidad y la posibilidad de errores. Los switches de Cisco se pueden configurar para que operen en modo Almacenamiento y envío, Libre de fragmentos o Conmutación rápida, según el modelo.

Operación con full duplex

Cuando se habilita la opción full duplex en un puerto, éste puede duplicar el ancho de banda permitiéndole transmitir y recibir simultáneamente. Esto significa que un puerto Ethernet de 10Mbps puede operar a 20Mbps, siempre y cuando la interfaz del dispositivo conectado (interfaz de NIC o de router) también pueda soportar la operación full duplex. Como un switch proporciona un circuito virtual sin colisiones para el dispositivo, se trata de un ancho de banda dedicado para el dispositivo. Un puerto Fast Ethernet de 100Mbps puede operar a un ancho de banda dedicado de 200Mbps. Se debe establecer la operación con full duplex para cada puerto.

Operación de Puerto rápido

Cuando un puerto de switch se activa, normalmente pasa por los estados normales de Bloquear, Escuchar, Aprender y Enviar de Spanning-Tree de 802.1d Este proceso puede tardar hasta unos 45 segundos. Cuando se habilita el modo de puerto rápido (spanning-tree), el Protocolo Spanning-Tree (STP) puede pasar el estado del puerto de Bloquear a Enviar sin pasar por los estados intermedios de Escuchar y Aprender. Esto puede resultar ventajoso, especialmente en los entornos Novell Network IPX donde las peticiones del cliente pueden a veces expirar debido al tiempo que tarda el puerto de un switch en responder.

Herramientas / Preparación:

Antes de comenzar con la práctica de laboratorio, el profesor o asistente de laboratorio debe preparar un switch con los valores VLAN por defecto. Se debe colocar también a disposición una estación de trabajo con HyperTerminal para realizar la conexión de consola al switch y una conexión Ethernet para hacer Telnet al switch. Como es posible que sólo haya un switch disponible, el instructor debe como mínimo hacer una demostración con esta práctica de laboratorio; los estudiantes deben trabajar en grupos más grandes para poder trabajar en la práctica. Mientras un equipo está trabajando con el switch, los demás pueden realizar una investigación sobre switches en el sitio Web de Cisco, en los URL que aparecen a continuación. Antes de comenzar con esta práctica de laboratorio, puede resultarle útil repasar el capítulo 2 (Conmutación LAN) de la Guía del segundo año de la Academia de networking de Cisco. También conviene repasar la Lección 2 en línea del Semestre 3. Se requieren los siguientes recursos:

- PC Windows c/ HyperTerminal instalado (configurado para conexión de consola al switch)
- Switch Cisco (modelo 19xx o 28xx)
- Cable de consola (roll-over)
- Cable Ethernet CAT 5 de conexión directa desde la estación de trabajo a un puerto Ethernet de switch

Recursos de sitio Web:

- LAN Switching basics
- <u>General information on all Cisco products</u> (Ir al capítulo 22 Switches)
- 1900 / 2820 series Ethernet switches
- 2900 series Fast Ethernet switches
- <u>3500 series Gigabit Ethernet switches</u>
- Cisco switch clustering technology

Paso 1- Conectar la estación de trabajo al puerto de consola del switch y activar el switch

Espere unos pocos minutos para que el switch arranque y aparecerá un menú de opciones conocido como la "Consola de administración" (versión 1900).

1. ¿Cuál es el número de modelo del switch?

2. ¿Cuál es la dirección Ethernet (dirección MAC de Capa 2) del switch?

3. ¿Cuál es la revisión y tipo de firmware del switch?

Paso 2 - Configurar el switch para una operación libre de fragmentos

Seleccione la opción **[S] System** del menú principal y vea las opciones del menú dentro de **Settings**

4. ¿Cuál es el modo actual del switch?

5. ¿Qué opción del menú le permitirá cambiar el modo?

6. ¿Qué opciones hay disponibles?

Paso 3 - Configurar un puerto para operación full duplex.

7. Enumere los puertos disponibles para su selección: Identifique el puerto:

8. ¿Se encuentra habilitado full duplex? ¿Qué opción se utiliza para habilitarlo?

Paso 4 - Configurar un puerto para el modo Puerto rápido.

Desde el menú de configuración de puerto, seleccione la opción de configuración de Puerto rápido (Port Fast).

9. ¿Qué opción selecciona Port fast?

Paso 5 - Verificar la configuración IP del switch.

Desde la opción [N] Administración de red del menú principal, seleccione [I] para la configuración IP.

10. ¿El switch tiene una dirección IP? De ser así, ¿cuál es?

Práctica de laboratorio 2.4.2 Navegador de config. del switch - Descripción general

Duración estimada: 30 min.
Objetivos:

- Utilizar los menús de la Consola de administración para ver y ajustar la configuración de la dirección IP del switch.
- Verificar los valores de red de las estaciones de trabajo para verificar la compatibilidad con valores de los switches y routers
- Probar el cableado y la conectividad IP desde la estación de trabajo al switch utilizando los comandos Ping y Telnet.
- Utilizar una estación de trabajo con software navegador para conectarse con el switch y verificar el estado del puerto.

Información básica:

Esta práctica de laboratorio le ofrecerá la oportunidad de configurar un switch para el acceso IP y HTTP (Protocolo de transferencia de hipertexto). Al asignar una dirección IP al switch se le podrá hacer ping y Telnet. También podrá usar su navegador de estación de trabajo (Netscape o Internet Explorer) para conectarse al switch y verificar la configuración del switch y las estadísticas de puerto. El navegador proporciona una interfaz gráfica que muestra una vista frontal del switch y permite que seleccione cualquier puerto para verificar sus estadísticas y características. Muchos switches más modernos poseen un software de servidor web HTTP incorporado para soportar la administración de switch basada en navegador. Con la tecnología de agrupación de switches de Cisco, puede manejar hasta 16 switches con una sola dirección IP. Es muy importante asignar una contraseña al switch si va a asignar una dirección IP.

Herramientas / Preparación:

Antes de comenzar con la práctica de laboratorio, el profesor o asistente de laboratorio debe preparar un switch con los valores VLAN por defecto. Se debe colocar también a disposición de los estudiantes una estación de trabajo con HyperTerminal para realizar la conexión de consola al switch y una conexión Ethernet para hacer Telnet al switch y para usar el navegador. Como es posible que sólo haya un switch disponible, el instructor debe como mínimo hacer una demostración con esta práctica de laboratorio; los estudiantes deben trabajar en grupos más grandes para poder trabajar en la práctica. Mientras un equipo está trabajando con el switch, los demás pueden realizar una investigación sobre switches en el sitio Web de Cisco, en los URL que aparecen a continuación. Antes de comenzar con esta práctica de laboratorio, puede resultarle útil repasar el capítulo 2 de la Guía del segundo año de la Academia de networking de Cisco, sobre conmutación LAN. También debe repasar la lección 2 en línea del semestre 3. A continuación, presentamos una lista del equipo requerido.

- PC Windows c/ HyperTerminal instalado (configurado para conexión de consola al switch)
- Switch Cisco (modelo 19xx o 28xx)
- Cable de consola (roll-over)
- Cable Ethernet CAT 5 desde la estación de trabajo a un puerto Ethernet de switch

Recursos de sitio Web:

- LAN Switching basics
- General information on all Cisco products (Ir al capítulo 22 Switches)
- 1900 / 2820 series Ethernet switches
- 2900 series Fast Ethernet switches
- <u>3500 series Gigabit Ethernet switches</u>
- <u>Cisco switch clustering technology</u>

Notas:

Paso 1- Conectar la estación de trabajo al puerto de consola del switch y active el switch

Según el switch necesitará un cable rollover RJ45 con un adaptador DB9 (en el extremo del PC) o un cable de módem DB9 a DB9 nulo (eliminador de módem). Espere unos pocos minutos para que el switch arranque y aparecerá un menú de opciones conocido como la "Consola de administración".

1. ¿Cuál es el número de modelo del switch?

2. ¿Cuál es la dirección Ethernet (dirección MAC de Capa 2) del switch?

Paso 2- Utilizar la Consola de administración para configurar el acceso IP al switch.

La dirección IP del switch se puede utilizar para hacer Ping o Telnet al switch, y para navegar a él. No se requiere asignar una dirección IP a un switch pero se recomienda para la administración de un switch. Cuando se administra un switch, el "Dominio de administración" es siempre VLAN 1. Todos los puertos son asignados a VLAN 1 por defecto.

3. Seleccione [N] Administración de red y luego [I] Configuración IP desde los menús. Asigne una dirección IP y una máscara de subred al switch. Asegúrese de usar una dirección IP y máscara de subred que sean compatibles con la red o subred en la que se encuentra actualmente el switch. Si el switch se conecta al Router Lab-A, Interfaz E1 (205.7.5.1) como se ve en el diagrama de configuración estándar de laboratorio, entonces asigne una dirección IP compatible y máscara de subred al switch.

Dirección IP: _____

Máscara de subred:

4. Seleccione [V] LAN virtual en el menú y verifique que todos los puertos se asignen a VLAN 1. Enumere los puertos que se asignan actualmente a VLAN 1 por defecto:

Paso 3- Utilizar la Consola de administración para configurar el acceso HTTP.

5. Seleccione el menú [N] Administración de red y verifique que el switch acepte las peticiones HTTP. ¿Qué opción se utiliza para configurar el switch para que sea un servidor HTTP?

(Nota: Esta opción puede no estar disponible para todos los switches)

Paso 4 - Configurar las estaciones de trabajo para obtener el acceso Ethernet al switch.

Configure la estación de trabajo con valores de red TCP/IP que sean compatibles con la dirección IP del switch y la dirección (E1) de la interfaz del router. Asegúrese de establecer la dirección IP de la estación de trabajo, la máscara de subred y el gateway por defecto (interfaz del router cercano).

6. Escriba aquí la información relativa a la dirección IP de la estación de trabajo:

Dirección IP:

Máscara de subred:

Gateway por defecto:

Paso 5 - Hacer ping a la dirección IP del switch.

Conecte el cable Ethernet de la estación de trabajo (de conexión directa) al puerto 1 del switch y utilice el comando ping del indicador de DOS de la estación de trabajo para probar la conectividad y la configuración IP entre las estaciones de trabajo y el switch.

C:\WINDOWS> ping 205.7.5.4

7. ¿El comando ping tuvo éxito?

Paso 6 - Hacer Telnet a la dirección IP del switch.

Haga Telnet al switch desde el indicador de DOS de la estación de trabajo para probar la conectividad de capa superior y la configuración IP entre la estación de trabajo y el switch. Deberá ver el mismo menú que cuando se conecta a través de la consola.

C:\WINDOWS> telnet 205.7.5.4

8. ¿Telnet fue exitoso?

Paso 7 - Utilizar el navegador para acceder al switch.

Inicie el software del navegador (Netscape o Internet Explorer). Escriba la dirección IP que acaba de asignar al switch en el área destinada a la dirección del navegador donde normalmente escribiría el URL de un sitio web. El servidor HTTP del switch deberá mostrar la Interfaz de usuario gráfica de administración de switch (GUI). Recuerde que puede utilizar los botones adelante y atrás en el navegador. El GUI del navegador es algo limitado en cuanto a configuración.

9. ¿Apareció la interfaz del navegador del Administrador de switch?

Paso 8 - Realizar algunos cambios de configuración en el switch mediante la interfaz del navegador.

10.Introduzca un nombre para el switch:

11. Introduzca una contraseña para el switch y confírmela.

12. ¿De qué color será el puerto en caso de que el enlace sea defectuoso o que el puerto esté desactivado?

13. Seleccione el puerto donde se encuentra conectada su estación de trabajo (puerto 1) y haga clic sobre éste con el ratón. Desplácese por la tabla de puertos hasta llegar al puerto 0/1. ¿Cuál es el modo dúplex actual real?

Cambie el modo de half duplex a full duplex. (Es posible que la NIC de su estación de trabajo no soporte la operación full duplex).

14. Verifique las estadísticas de puerto para las tramas recibidas y transmitidas haciendo clic en el botón **"Stats**". Introduzca la cantidad de paquetes, a continuación:

Tramas correctas recibidas:

Paquetes transmitidos:

Práctica de laboratorio 3.3.4.1 Creación de VLAN - Descripción general



Duración estimada: 45 min.

Objetivos:

Esta práctica de laboratorio sirve para practicar las siguientes tareas:

- Conectarse a través de la consola al switch para determinar la versión de firmware
- Verificar la dirección IP y la máscara de subred para el switch
- Usar la consola de administración para verificar las opciones del menú relacionadas con las VLAN
- Verificar los valores de red de las estaciones de trabajo para verificar la compatibilidad con valores de los switches y routers
 - Crear una nueva VLAN, nombrarla y desplazar puertos miembro a ella.
- Probar la funcionalidad de las VLAN desplazando una estación de trabajo de una VLAN a otra

Información básica:

En esta práctica de laboratorio se trabaja con redes de área local virtuales de Ethernet (VLAN). Las VLAN se pueden usar para separar grupos de usuarios según la función en lugar de la ubicación física. Normalmente todos los puertos en un switch están en la misma VLAN 1 por defecto. Un administrador de red puede crear VLAN adicionales y desplazar algunos puertos a los de las VLAN para crear grupos aislados de usuarios sin importar dónde se ubican físicamente. Esto crea dominios de broadcast más pequeños que ayudan a reducir y localizar el tráfico de red. Si un switch con 24 puertos se divide en 2 VLAN de 12 puertos cada uno, los usuarios de una VLAN no podrán acceder a los recursos (como servidores o impresoras) en la otra VLAN. Las VLAN también se pueden crear usando puertos desde múltiples switches que se unen en un enlace troncal en un backbone. Para que dos VLAN se comuniquen deben estar conectadas a un router. La seguridad se puede controlar mediante las listas de control de acceso (ACL), que se tratarán en una práctica de laboratorio futura.

Accederá mediante la consola al switch y usará los menús de interfaz del usuario de consola de administración para ver las opciones disponibles para administrar las VLAN y verificará la configuración actual de la VLAN. También hará Telnet para acceder al switch y verificará algunos valores. También trasladará la conexión de una VLAN a otra para determinar los alcances del "Dominio de administración". Al administrar un switch, el dominio de administración siempre es VLAN 1. La estación de trabajo del administrador de red debe tener acceso a un puerto en el dominio de administración VLAN 1. Todos los puertos son asignados a VLAN 1 por defecto. Esta práctica de laboratorio también ayudará a demostrar cómo las VLAN se pueden usar para separar el tráfico y reducir los dominios de broadcast.

Herramientas / Preparación:

Antes de comenzar con la práctica de laboratorio, el profesor o asistente de laboratorio debe preparar un switch con los valores VLAN por defecto. Se debe colocar también a disposición una estación de trabajo con HyperTerminal para realizar la conexión de consola al switch y una conexión Ethernet para hacer Telnet al switch. Como es posible que sólo haya un switch disponible, el instructor debe como mínimo hacer una demostración con esta práctica de laboratorio; los estudiantes deben trabajar en grupos más grandes para poder trabajar en la práctica. Mientras un equipo está trabajando con el switch, los demás pueden realizar una investigación sobre switches en el sitio Web de Cisco, en los URL que aparecen a continuación. Antes de comenzar con esta práctica de laboratorio, puede resultarle útil repasar el capítulo 3 (VLAN) de la Guía del segundo año de la Academia de networking de Cisco. También debe repasar la lección 3 del Semestre 3 en línea. A continuación se suministra la lista de equipo requerido.

- Dos estaciones de PC Windows con HyperTerminal instalado (configurado para la conexión de consola al switch y direcciones IP compatibles)
- Switch Cisco (modelo 19xx o 28xx)
- Cable de consola (roll-over) y adaptador DB-9/RJ45 o cable de módem nulo DB-9
 - Cable Ethernet CAT 5 desde cada estación de trabajo a un puerto Ethernet de switch

Recursos de sitio Web:

LAN Switching basics General information on all Cisco products - (Ir al capítulo 22 - Switches) 1900 / 2820 series Ethernet switches 2900 series Fast Ethernet switches 3500 series Gigabit Ethernet switches Virtual LAN for 1900/2820 Switches

Notas:

Paso 1 - Acceda al switch LAN a través de la consola.

Acceda al switch a través de la consola, conectando el puerto serial de la estación de trabajo al puerto de consola del switch con el cable rollover y responda a las siguientes preguntas. Use el

switch conectado al router Lab-A u otro (Nota: Las respuestas varían según el número de modelo del switch)

1. ¿Cuál es el número de modelo del switch?

2. ¿Este switch tiene software de edición estándar o para empresas?

3. ¿Cuál es la versión de firmware del switch?

4. ¿Cuál es la opción en el menú del switch que se usa para crear o modificar las VLAN?

Paso 2 - Verificar la dirección IP del router, el switch y las estaciones de trabajo conectadas.

5. Verifique la dirección IP y máscara de subred del router, switch y estaciones de trabajo para comprobar que sean compatibles y se encuentren en la misma red. Si el switch se conecta al Router Lab-A, Interfaz E1 como se ve en el diagrama de configuración estándar de laboratorio, entonces asigne las direcciones IP, máscaras de subred y gateways por defecto según resulte apropiado. Registre sus valores a continuación:

IP del router:	Máscara de subred:	_
IP del switch:	Máscara de subred:	_
IP de la Est. de trabajo 1:	Máscara de subred:	Gateway por defecto:
IP de la Est. de trabajo 2:	Máscara de subred:	Gateway por defecto:

Paso 3 - Entrar al modo de configuración de VLAN.

6. ¿Cuál es la cantidad máxima de VLAN que se pueden crear?

7. Seleccione la opción [L] List VLAN (Enumerar VLAN) en el submenú e introduzca la palabra ALL (Todas). ¿Cuántas VLAN aparecen actualmente?

8. Enumere las opciones en el menú y submenús de configuración de VLAN en la tabla siguiente:

Opción de menú	Descripción de la opción de menú de VLAN	Opciones de submenú (enumerar dos o más)

Opciones de menú de VLAN de un Switch Ethernet Cisco Catalyst 1912 (10Mbps)

Paso 4 - Configurar las VLAN con las opciones de menú VLAN.

NOTA: Los siguientes pasos se realizaron en un switch Catalyst 1912 WS-C1912C-EN (12 puertos) con firmware de edición de empresa, versión V8.01.02. Las respuestas varían.

9. Verifique la configuración de la VLAN por defecto, seleccionando la opción [M] Modify VLAN (Modificar VLAN) y seleccione VLAN 1. ¿Cuáles son los puertos miembro actuales en VLAN 1?

10. Cree una nueva VLAN Ethernet y póngale un nombre. Póngale un nombre (por ej.,: su apellido y un número: reyes1). ¿Qué nombre le puso?

11. ¿Cuál es el número de VLAN para su nueva VLAN?

12. Enumere los pasos requeridos para crear y nombrar la nueva VLAN:

13. Asigne los puertos del 7 al 12 y el puerto B a la nueva VLAN: Enumere los pasos que se requieren para hacer esto:

14. Verifique VLAN 1 nuevamente. ¿Qué cambios puede ver?

Salga al menú principal, y luego a la consola de administración

Paso 5 - Probar la funcionalidad de las 2 VLAN.

Para ver la VLAN en acción, configure dos estaciones de trabajo y verifique que las direcciones IP se encuentren en la misma subred (ver Paso 2). Reinicie los computadores según sea necesario.

Desde la Estación de trabajo 1, conecte el cable Ethernet desde la tarjeta NIC a un puerto desde 1-6 en el switch. Desde la Estación de trabajo 2, conecte el cable Ethernet desde la tarjeta NIC a un puerto desde 1-6 en el switch.

15. Emita un ping a cada estación de trabajo. ¿El ping fue exitoso?

16. Ahora tome el puerto Ethernet de la Estación de trabajo 2 del switch y conéctelo a uno de los puertos en VLAN 2 (puertos 7-12). Haga ping nuevamente a cada estación de trabajo. ¿El ping fue exitoso?

Práctica de laboratorio 3.3.4.2 VLAN de administración de switch - Descripción general

Duración estimada: 45 min.

Objetivos:

Esta práctica de laboratorio sirve para practicar las siguientes tareas:

- Acceder a través de la consola al switch y verificar las características del switch y sus parámetros de configuración.
 - Ver/configurar la dirección IP y la máscara de subred para el switch
- Verificar los valores de red de las estaciones de trabajo para comprobar la
- compatibilidad con valores de los switches y routers
- Usar la consola de administración para verificar y cambiar la configuración de la VLAN
 para el switch
- Hacer Telnet al switch, basándose en la ubicación del puerto y VLAN
- Trabajar con el dominio de administración del switch

Información básica:

En esta práctica de laboratorio trabajará con las redes de área local virtuales (VLAN). Accederá a través de la consola al switch y visualizará las opciones de menú disponibles para administrar las VLAN y verificará la configuración actual de la VLAN. También hará Telnet para acceder al switch y verificará algunos valores. También trasladará la conexión de una VLAN a otra para determinar los alcances del "Dominio de administración". Al administrar un switch, el dominio de administración siempre es VLAN 1. La estación de trabajo del administrador de red debe tener acceso a un puerto en el dominio de administración VLAN 1. Todos los puertos son asignados a VLAN 1 por defecto.

Herramientas / Preparación:

Antes de comenzar con la práctica de laboratorio, el profesor o asistente de laboratorio debe preparar un switch con los valores VLAN por defecto. Se debe colocar también a disposición una estación de trabajo con HyperTerminal para realizar la conexión de consola al switch y una conexión Ethernet para hacer Telnet al switch. Como es posible que sólo haya un switch disponible, el instructor debe como mínimo hacer una demostración con esta práctica de laboratorio; los estudiantes deben trabajar en grupos más grandes para poder trabajar en la práctica. Mientras un equipo está trabajando con el switch, los demás pueden realizar una investigación sobre switches en el sitio Web de Cisco, en los URL que aparecen a continuación. Antes de comenzar con esta práctica de laboratorio, puede resultarle útil repasar el capítulo 3 (VLAN) de la Guía del segundo año de la Academia de networking de Cisco. También debe repasar la Lección 3 del Semestre 3 en línea. A continuación se suministra la lista de equipo requerido.

- Dos estaciones de PC Windows con HyperTerminal instalado (configurado para la conexión de consola al switch)
- Switch Cisco (modelo 19xx o 28xx)
- Cable de consola (roll-over) y adaptador DB-9/RJ45 o cable de módem nulo DB-9
- Cable Ethernet CAT 5 desde la estación de trabajo a un puerto Ethernet de switch

Recursos de sitio Web:

LAN Switching basics General information on all Cisco products - (Ir al capítulo 22 - Switches) 1900 / 2820 series Ethernet switches 2900 series Fast Ethernet switches 3500 series Gigabit Ethernet switches Cisco switch clustering technology Virtual LAN for 1900/2820 Switches

Notas:

Paso 1 - Acceder al switch LAN a través de la consola.

Acceda al switch a través de la consola, conectando el puerto serial de la estación de trabajo al puerto de consola del switch con el cable rollover y responda las siguientes preguntas. Use el switch conectado al router Lab-A u otro (Nota: Las respuestas varían según el número de modelo del switch)

1. ¿Cuál es el número de modelo del switch?

2. ¿Este switch tiene software de edición estándar o para empresas?

3. ¿Cuál es la versión de firmware del switch?

4. ¿Qué opción del menú se usa para configurar la dirección IP del switch?

5. ¿Cuál es la opción en el menú del switch que se usa para crear o modificar VLAN?

Paso 2. Asignar una dirección IP para el switch.

6. Asigne una dirección IP y máscara de subred al switch Asegúrese de usar una dirección IP y máscara de subred que sean compatibles con la red o subred en la que se encuentra actualmente el switch. Si el switch se conecta al Router Lab-A, Interfaz E1 como se ve en el diagrama de configuración estándar de laboratorio, entonces asigne una dirección IP compatible y máscara de subred al switch.

Dirección IP: _____ Máscara de subred: _____

Paso 3. Verificar las opciones de configuración VLAN.

7. Seleccione la opción VLAN en el menú. ¿Cuántas VLAN se pueden configurar con este switch?

8. Verifique que todos los puertos se asignen a VLAN 1. Enumere los puertos actualmente asignados a VLAN1.

9. Enumere las primeras tres "Acciones" disponibles en el submenú de VLAN. ¿Qué opción de menú se usa para desplazar un puerto a una VLAN distinta?

Opción de menú	Descripción de la opción de menú VLAN	Opciones de submenú (enumerar dos o más)

Paso 4. Conectar una estación de trabajo y hacer Telnet al switch.

Conecte la estación de trabajo al switch con un cable Ethernet CAT5 de conexión directa, usando el puerto 12 en el switch. Verifique que la estación de trabajo tenga dirección IP, máscara de subred y valores de gateway por defecto que sean compatibles con el switch y el router. Haga Telnet al switch desde el indicador de DOS de la estación de trabajo.

10. ¿Qué comando usó?

11. ¿Pudo hacer Telnet al switch?

12. Mueva el puerto 12 a VLAN 2. ¿Qué pasó con la sesión de Telnet?

13. Con la estación de trabajo conectada al puerto 12 en VLAN 2 ¿todavía puede administrar el switch?

14. ¿Por qué o por qué no?

15. Desplace su conexión de estación de trabajo al puerto 11 en el switch. ¿Puede hacer Telnet al switch ahora?

16. ¿Por qué o por qué no?

17. Explique por qué falló la sesión de Telnet cuando se desplaza la estación de trabajo del puerto 11 (VLAN 1) al puerto 12 (VLAN 2) en el switch.

Práctica de laboratorio 3.4.4.1 Actualización del firmware del switch / TFTP- Descripción general

Duración estimada: 20 min.

Objetivos:

- Mostrar información acerca del firmware actual del switch.
 - Examinar las opciones de memoria y actualización del switch
- Utilizar un servidor TFTP para actualizar un switch a una nueva versión del software firmware

Información básica:

A medida que se lanzan nuevas versiones del software firmware de Cisco, es necesario actualizar periódicamente el firmware existente para soportar las características y las mejoras más recientes. En esta práctica de laboratorio, determinará cuál es la versión del firmware que el switch ejecuta en la actualidad y se familiarizará con los requisitos necesarios para realizar la actualización a una versión más reciente. También se repasa el proceso de descarga de una nueva imagen del firmware del switch desde Cisco Connection Online (CCO). En esta práctica de laboratorio se describe el método del servidor TFTP para actualizar el firmware. El objetivo principal de esta práctica de laboratorio es actualizar el switch a la versión de empresa.

Nota:

Si su switch actualmente tiene una versión más antigua del firmware edición estándar, debe actualizarse a la versión más reciente de la edición estándar primero y luego actualizarse a la edición de empresa.

Herramientas / Preparación:

Antes de iniciar esta práctica de laboratorio necesita conectar una estación de trabajo de PC con HyperTerminal con un switch mediante la interfaz de consola del switch con un cable rollover. También necesita una conexión Ethernet al switch. El instructor o el ayudante de laboratorio deben instalar un PC Windows 9x con un servidor TFTP y debe tener la imagen más reciente que se haya descargado del firmware en el disco duro del PC. Verifique si el switch puede acceder al servidor TFTP. El servidor TFTP de Cisco y las actualizaciones del firmware más recientes se pueden descargar desde los sitios Web que aparecen a continuación. Como es posible que sólo haya un switch disponible, el instructor debe como mínimo hacer una demostración con esta práctica de laboratorio; los estudiantes deben trabajar en grupos más grandes para poder trabajar en la práctica. Mientras un equipo está trabajando con el switch, los demás pueden realizar una investigación sobre switches en el sitio Web de Cisco, en los URL que aparecen a continuación.

Puede resultarle útil repasar los capítulos 2 y 3 de la Guía del segundo año de la Academia de networking de Cisco y la lección 3 del Semestre 3 del currículum en línea antes de empezar esta práctica de laboratorio. Aunque las instrucciones de esta práctica de laboratorio para descargar el software de imagen del firmware sólo pueden ser ejecutadas por una persona que tenga una cuenta de CCO, debe leerlas cuidadosamente para familiarizarse con el proceso.

Recursos requeridos:

- PC con monitor, teclado, ratón y cables de alimentación, etc.
- Sistema operativo Windows (Win 95, 98, NT o 2000) instalado en un PC
- Programa HyperTerminal configurado para acceder a la consola del router
- PC conectado al puerto de consola del switch, con un cable rollover y un adaptador DB-9/RJ45 o cable de módem nulo DB-9.
- PC conectado a un hub al que está conectado el router o a un cable crossover directamente al router

PC instalado en una red a la que el router pueda enviar y recibir, que ejecute un daemon (servidor) TFTP

Recursos de sitio Web:

LAN Switching basics General information on all Cisco products - (Ir al capítulo 22 - Switches) 1900 / 2820 series Ethernet switches 2900 series Fast Ethernet switches 3500 series Gigabit Ethernet switches Virtual LAN for 1900/2820 Switches

Notas:

Paso 1. Descargar la nueva versión del firmware del switch.

Vaya a **www.cisco.com** y conéctese con su cuenta CCO (su instructor o contacto de la academia debe poder hacer esto). Haga clic en **Software Center (Centro de Software)** bajo **Service and Support (Servicios y Asistencia).** Haga clic en **LAN Switching** Software (software de conmutación LAN), y entonces haga clic en **Catalyst 1900**, y luego haga clic en **Download Cisco Catalyst 1900 Software Image** (descargar imagen de software de Cisco Catalyst 1900).

NOTA: Si tiene el la edición estándar del firmware debe actualizarse a la versión más reciente y luego a la versión de empresa. Según la versión del firmware del switch, es posible que no pueda actualizarse a la edición de empresa del firmware.

Paso 2- Conectarse al switch.

Seleccione la opción [M] de Menú y luego [F] para Firmware

Paso 3. Verificar la versión del firmware actual.

Si el switch no tiene la edición de empresa del software, deberá actualizarse a la versión estándar del firmware actual, y luego actualizarse a la misma versión de la edición de empresa.

1. ¿Qué versión del firmware está ejecutando el switch?

Paso 4. Configurar la dirección IP del switch.

Bajo el menú principal, seleccione **[N] Network Management (administración de red)**, luego seleccione **[I] IP configuration (configuración IP)** y en seguida seleccione **[I] IP address (dirección IP)** y **[S] (máscara de subred)**. Asegúrese de que la dirección IP y la máscara de subred estén en la misma red que el servidor TFTP.

Paso 5. Prepararse para actualizar el firmware.

- a. Establezca la dirección IP del servidor TFTP con la opción **[S] TFTP server name or IP** address (nombre de servidor TFTP o dirección IP).
- b. Establezca el nombre de archivo de la actualización con **[F] Filename** (nombre de archivo) para actualizar el firmware

Paso 6. Instalar la actualización del firmware.

En la configuración del firmware seleccione **[T] para la actualización TFTP del sistema**. El switch le pide que confirme la actualización. Después de confirmar si desea proceder con la actualización de firmware, el switch no responde por aproximadamente 1 minuto. Esto es normal.

Paso 7. Confirmar la actualización del firmware.

En el menú principal seleccione la opción [M] de Menú y luego [F] para Firmware

2. ¿Qué versión del firmware está ejecutando el switch?

Práctica de laboratorio 3.4.4.2 VLAN multiswitch - Descripción general

Duración estimada: 60 min.

Objetivos:

Esta práctica de laboratorio sirve para practicar las siguientes tareas:

- Conectarse a través de la consola al switch para determinar la versión de firmware
- Verificar la dirección IP y la máscara de subred para el switch
- Usar la consola de administración para verificar las opciones del menú relacionadas con las VLAN
- Verificar los valores de red de las estaciones de trabajo para comprobar la compatibilidad con valores de los switches y routers
- Crear una nueva VLAN, nombrarla y desplazar puertos miembro a ella.
- Probar la funcionalidad de las VLAN desplazando una estación de trabajo de una VLAN
- a otra
 - Habilitar el enlace troncal ISL (enlace interswitch) en puertos troncales para los dos switches

Información básica:

En esta práctica de laboratorio se trabaja con redes de área local virtuales de Ethernet (VLAN). Las VLAN se pueden usar para separar grupos de usuarios según la función en lugar de la ubicación física. Normalmente todos los puertos de un switch se encuentran en la misma VLAN 1 por defecto. Un administrador de red puede crear VLAN adicionales y trasladar algunos puertos a esas VLAN para crear grupos aislados de usuarios, sin importar su ubicación física. Esto crea dominios de broadcast más pequeños que ayudan a reducir y localizar el tráfico de red. Si un switch con 24 puertos se divide en 2 VLAN de 12 puertos cada uno, los usuarios de una VLAN no podrán acceder a los recursos (como servidores o impresoras) en la otra VLAN. Las VLAN también se pueden crear usando puertos desde múltiples switches que se unen en un enlace troncal en un backbone. Para que dos VLAN se comuniquen deben estar conectadas a un router. La seguridad se puede controlar mediante las listas de control de acceso (ACL), que se tratarán en una práctica de laboratorio futura.

Accederá mediante la consola al switch y usará los menús de interfaz del usuario de consola de administración para ver las opciones disponibles para administrar las VLAN y verificará la configuración actual de la VLAN. También hará Telnet para acceder al switch y verificará algunos valores. También trasladará la conexión de una VLAN a otra para determinar los alcances del "Dominio de administración". Al administrar un switch, el dominio de administración siempre es VLAN 1. La estación de trabajo del administrador de red debe tener acceso a un puerto en el dominio de administración VLAN 1. Todos los puertos son asignados a VLAN 1 por defecto. Esta práctica de laboratorio también ayudará a demostrar cómo las VLAN se pueden usar para separar el tráfico y reducir los dominios de broadcast.

Herramientas / Preparación:

Antes de empezar con la práctica de laboratorio, el profesor o asistente de laboratorio debe tener dos switches disponibles con los valores de VLAN por defecto y cada switch debe ejecutar el firmware de edición de empresa. Si los switches no tienen esta edición, el firmware de edición de empresa debe ser descargado desde el sitio Web de Cisco por una persona que tenga una cuenta de conexión CCO (su contacto de la academia o su instructor). El procedimiento de actualización del firmware del switch se describió en la práctica de laboratorio anterior (3.4.4. Práctica de laboratorio 1). Una estación de trabaio con HyperTerminal debe estar disponible como consola y para hacer Telnet al switch. Como puede ser que sólo haya un par de switches disponibles, el instructor debe como mínimo hacer una demostración con esta práctica de laboratorio; los estudiantes deben trabajar en grupos más grandes para poder trabajar en la práctica. Mientras un equipo está trabajando con el switch, los demás pueden realizar una investigación sobre switches en el sitio Web de Cisco, en los URL que aparecen a continuación. Antes de comenzar con esta práctica de laboratorio, puede resultarle útil repasar el capítulo 3 (VLAN) de la Guía del segundo año de la Academia de networking de Cisco. También conviene repasar la Lección 3 en línea del Semestre 3. Se requieren los siguientes recursos:

- Dos estaciones de PC Windows con HyperTerminal instalado (configurado para la conexión de consola al switch y direcciones IP compatibles)
- Dos switches de Cisco (modelo 19xx o 28xx) con el software de edición de empresa, con por lo menos un puerto troncal 100BASE-TX (CAT 5 cobre) (A o B).
- Cable de consola (roll-over o cable nulo)
- Cable Ethernet CAT 5 desde cada estación de trabajo a un puerto Ethernet de switch
- Cable crossover CAT 5 para conectar los puertos troncales del switch (100BASE-TX)

Recursos de sitio Web:

LAN Switching basics General information on all Cisco products - (Ir al capítulo 22 - Switches) 1900 / 2820 series Ethernet switches 2900 series Fast Ethernet switches 3500 series Gigabit Ethernet switches Virtual LAN for 1900/2820 Switches

Notas:

Paso 1 - Acceder al switch LAN a través de la consola.

Acceda al switch a través de la consola, conectando el puerto serial de la estación de trabajo al puerto de consola del switch y responda a las siguientes preguntas. (Nota: Las respuestas varían según el número de modelo del switch). **Para esta práctica de laboratorio debe disponer del la edición de empresa del software para crear VLAN que abarquen múltiples switches.** Si el switch necesita actualizarse a la edición de empresa del software, consulte la práctica de laboratorio sobre actualización de firmware del switch. Puede ser necesario usar la opción **[F] Firmware** en el menú principal del switch para determinar las respuestas a las siguientes preguntas.

1. ¿Cuál es el número de modelo del switch?

Switch-A:

Switch-B:

2. ¿Este switch tiene software de edición estándar o para empresas?

Switch-A:

Switch-B:

3. ¿Cuál es la versión de firmware del switch?

Switch-A:

Switch-B:

4. ¿Cuál es la opción en el menú del switch que se usa para crear o modificar las VLAN?

Switch-A:

Switch-B:

Paso 2 - Verificar la dirección IP del switch y de las estaciones de trabajo conectadas.

5. Verifique la dirección IP y máscara de subred del switch y de las estaciones de trabajo para verificar que sean compatibles y se encuentren en la misma red. Registre sus valores a continuación:

IP del switch A:	Máscara de subred:	
IP del switch B:	Máscara de subred:	
IP de la Est. de trabajo 1	Máscara de subred:	
IP de la Est. de trabajo 2:	Máscara de subred:	

Paso 3. Entrar al modo de configuración de VLAN.

6. ¿Cuál es la cantidad máxima de VLAN que se pueden crear?

7. Seleccione la opción [L] List VLAN (Enumerar VLAN) en el submenú e introduzca la palabra ALL (Todas). ¿Cuántas VLAN aparecen actualmente?

8. Enumere las opciones en el menú y submenús de configuración de VLAN en la tabla siguiente:

Opciones de menú de VLAN de un Switch Ethernet Cisco Catalyst 1912 (10 Mbps)

Opción de menú	Descripción de la opción de menú VLAN	Opciones de submenú (enumerar dos o más)

Paso 4 - Configurar las VLAN con las opciones de menú VLAN.

NOTA: Los pasos siguientes se efectuaron en un switch Catalyst 1912 WS-C1912C-EN (12 puertos) con la versión de firmware de empresa V8.01.02 (Switch-A) y otro switch Catalyst 1924 WS-C1924C-EN (24 puertos) con la versión de firmware de empresa V8.01.02 (Switch-B). Sus respuestas pueden variar.

9. Verifique la configuración de la VLAN por defecto, seleccionando la opción [M] Modify VLAN (Modificar VLAN) y seleccione VLAN 1. ¿Cuáles son los puertos miembro actuales en VLAN 1?

10. Cree dos nuevas VLAN Ethernet y póngales un nombre. Póngale un nombre a cada una (por ej.,: su apellido y el número de la VLAN: reyes10 o reyes20). ¿Qué nombre les puso?

Para las dos VLAN creadas se usan los números 10 y 20. Asigne un SAID a cada VLAN usando la opción de VLAN [I] 802.10 SAID. Use SAID 10 y 20 para las VLAN 10 y 20. Asigne la primera mitad de los puertos a VLAN 10 y la segunda mitad a VLAN 20. Repita esto en el Switch-B con los mismos nombres, números de VLAN y el mismo SAID.

Paso 5. Habilitar el enlace troncal en el puerto B de Switch-A y Switch-B.

En la configuración de VLAN, seleccione [T] Trunk Configuration (configuración troncal) y seleccione puerto B. En el menú de configuración del enlace troncal B seleccione [T] Trunking (enlace troncal) y luego seleccione 1 para activar el enlace troncal. Repita el procedimiento para Switch-A y Switch-B. Por defecto, las VLAN 1-1005 pueden usar el puerto troncal.

NOTA: Se puede usar un cable crossover CAT 5 para conectar el puerto B de Switch-A al puerto B de Switch-B. Esto da por sentado que cada uno de los switches tiene por lo menos un puerto troncal 100BASE-TX (CAT 5 cobre) o puerto de backbone (puerto A o B). Algunos switches tienen un puerto troncal 100BASE-TX y un 100BASE-FX (fibra) y algunos tienen dos puertos 100BASE-FX, según el modelo.

Práctica de laboratorio 4.5.6: Diseño de LAN conmutada - Descripción general

Duración estimada: 60 min.

Objetivos:

- Analizar los requisitos para una red de área local simple con acceso a Internet.
- Diseñar una topología de Capa 1 y 2 tomando como base Ethernet conmutada y determinados requisitos.
- Determinar el tipo, número y ubicación de los switches Ethernet así como el cableado necesario tomando como base las ubicaciones del centro de cableado para MDF y múltiples IDF y un simple plano de piso.
- Investigar en el sitio web de Cisco y de los distribuidores de Cisco para averiguar modelos y costos

Información básica:

Esta práctica de laboratorio lo ayudará a prepararse para el Estudio de caso. En esta práctica de laboratorio, se le suministran algunos requisitos básicos para una LAN pequeña que abarca múltiples edificios. El enfoque se debe centrar en la topología física y en los componentes de la capa de enlace de datos. El objetivo es reemplazar una red Ethernet de cable fino 10BASE2 antigua con cableado y switches Ethernet de la tecnología actual basándose en los estándares de cableado estructurado y la topología en estrella extendida. Deberá decidir qué tipo de switches Ethernet utilizar y dónde colocarlos. También deberá determinar el tipo de cableado que se debe utilizar basándose en los requisitos indicados. Sus usuarios necesitarán acceder a varios servidores y necesitarán que se coloque en las ubicaciones más efectivas posibles. Deberá utilizar catálogos de distribuidores e investigación de Web para encontrar los números de los distintos modelos y los costos de varias soluciones Ethernet conmutadas.

Herramientas / Preparación:

Esta es una práctica de laboratorio de investigación y no requiere la configuración física de laboratorio. Necesitará acceder a los catálogos de equipos de comunicaciones de datos y a la Web para poder realizar investigaciones. Utilice el URL del sitio web de Cisco que aparece a continuación Se trabaja en grupos de 3 o más personas. Antes de comenzar con esta práctica de laboratorio, puede resultarle útil repasar el capítulo 4 (Diseño LAN) de la Guía del segundo año de la Academia de networking de Cisco. También conviene repasar la Lección 4 en línea del Semestre 3. Se requieren los siguientes recursos:

- PC con acceso a Internet para la investigación de productos
- Catálogos de distribuidores de equipos de comunicaciones de datos

Recursos de sitio Web:

- LAN Switching basics
- General information on all Cisco products (Ir al capítulo 22 Switches)
- 1900 / 2820 series Ethernet switches
- 2900 series Fast Ethernet switches
- <u>3500 series Gigabit Ethernet switches</u>
 - Cisco switch clustering technology

Notas:

Paso 1. Repaso de los requisitos

Está diseñando una LAN para una pequeña empresa con una ubicación y varios edificios que necesitan interconectarse. Utilice el diagrama y los requisitos del edificio indicados para decidir qué tipo de switches y cableado se deben tender y dónde.

- 1. Existen 3 edificios en un campus Administración, Ingeniería y Fabricación
- 2. Administración está en el Edificio A, Ingeniería en el edificio B y Fabricación en el edificio C
- 3. El edificio de Administración se encuentra entre los de Ingeniería y Fabricación
- 4. Las distancias entre los edificios aparecen en el diagrama
- 5. Existe un centro de el cableado en cada uno de los edificios
- 6. El centro de cableado del POP está en el edificio de Administración
- 7. Hay 35 PC y 5 impresoras que necesitan acceso de red en el edificio de Administración
- 8. Hay 27 PC y 3 impresoras que necesitan acceso de red en el edificio de Ingeniería
- 9. Hay 18 PC y 2 impresoras que necesitan acceso de red en el edificio de Fabricación
- 10. El cliente desea contar con la tecnología de conmutación Ethernet más rápida disponible para el backbone
- 11. El cliente desea mantener el precio bajo para las conexiones de estación de trabajo
- 12. Todos los usuarios necesitan acceso a Internet y dos servidores de archivo y de impresión centralizados
- 13. Los usuarios ingenieros necesitan acceso local a un servidor departamental de alto rendimiento



Red de datos de la empresa XYZ

Complete la tabla y conteste las siguientes preguntas basándose en su conocimiento del equipo de conmutación Ethernet, routers y los estándares del cableado estructurado.

1. Edificio Administración A - Equipo MDF / POP (40 datos)

Equipo Tipo	Modelo N°	Cantidad	N°/tipo de puertos	Descripción/Función	Costo

2. Edificio Ingeniería B: Equipo IDF 1 (30 datos)

Equipo Tipo	Modelo N°	Cantidad	N°/tipo de puertos	Descripción/Función	Costo
			(1)		

3. Edificio Fabricación C: Equipo IDF 2 (20 datos)

Equipo Tipo	Modelo N°	Cantidad	N°/tipo de puertos	Descripción/Función	Costo

4. ¿Qué tipo de cableado se debe tender desde los switches en el centro de el cableado a las estaciones de trabajo de escritorio de los usuarios y por qué?

¿Cuál será la velocidad de estos enlaces?

5.

- 6. ¿Cuáles son algunos términos relacionados con este tipo de cableado?
- 7. ¿Qué tipo de cableado se debe tender desde MDF/POP en el edificio A hasta los edificios B y C y por qué?
- 8. ¿Cuál será la velocidad de estos enlaces?
- 9. ¿Cuáles son algunos términos relacionados con este tipo de cableado?
- 10. ¿Por qué el centro de el cableado del edificio Administración es el mejor lugar para colocar el MDF?

Práctica de laboratorio 5.2.2: Protocolos enrutados y de enrutamiento - Descripción general

Topología de laboratorio de routers



Duración estimada: 30 min.

Objetivos:

- Comparar las características de los protocolos enrutados y de enrutamiento y proporcionar ejemplos de cada uno de ellos
- Examinar un router para determinar cuáles son los protocolos enrutados y de enrutamiento que están activos
- Practicar con los comandos para determinar cuáles son los protocolos enrutados y de enrutamiento que se reconocen
 - (show IP route, show protocols, show running config, router ?)
- Buscar una concordancia entre los términos correspondientes a los protocolos enrutados y de enrutamiento
- Diagramar la relación entre: enrutado & protocolos de enrutamiento dinámicos & protocolos estáticos, protocolos interiores versus exteriores, vector distancia, estado de enlace & protocolos de enrutamiento híbridos

Información básica

Esta práctica de laboratorio refuerza el conocimiento y la compresión de los protocolos enrutados y de enrutamiento, que son los protocolos principales que hacen posible el funcionamiento de un router. Se repasarán dos ejemplos de cada tipo de protocolo y se utilizarán varios comandos IOS en el router para descubrir qué protocolos enrutados y de enrutamiento se encuentran activos o en ejecución en el router. También se utilizará la función de ayuda para identificar otros protocolos que el router sería capaz de reconocer pero que no se encuentran en ejecución. Es fundamental comprender la diferencia entre protocolos enrutados y de enrutados y de enrutados y de enrutamiento para dominar los conceptos de internetworking.

Protocolos enrutados

Los protocolos son el lenguaje o las normas de comunicación entre los dispositivos en una red. Los protocolos enrutados son aquellos que se pueden enrutar. La información de direccionamiento de Capa 3 (de red) se coloca en el encabezado del paquete de datos que permite que el paquete atraviese múltiples redes para llegar a su destino. También se denominan protocolos enrutables, lo que significa que se pueden enrutar. Para que un protocolo se pueda enrutar, el método de direccionamiento debe tener por lo menos dos partes; un número de red y un número de nodo. Es la porción de red que corresponde a la dirección la que permite que un paquete se enrute desde una red a otra. Todos los dispositivos en una red generalmente ejecutan el mismo protocolo enrutado, que es similar a un lenguaje común, para poder comunicarse. La mayoría de los protocolos LAN son protocolos enrutados.

El protocolo enrutado más común es el Protocolo Internet o IP, que es un estándar internacional. IP a veces se denomina TCP/IP pero TCP en realidad es un protocolo de transporte (Capa 4) y no se involucra directamente con el protocolo IP enrutable que funciona en la Capa 3. Para que un dispositivo (estación de trabajo, servidor, router, etc.) se pueda comunicar en Internet, debe ejecutar el protocolo IP. Las direcciones IP son de 32 bits y contienen una porción de red y una porción de nodo que asigna, típicamente, el administrador de la red. Otros protocolos de LAN enrutados son Novell IPX, AppleTalk y Decnet.

Protocolos de enrutamiento

Los protocolos de enrutamiento son los protocolos que utilizan los routers para comunicarse entre sí a fin de intercambiar información de forma dinámica acerca de las redes que pueden alcanzar y de la conveniencia de las rutas disponibles. Normalmente se denominan protocolos de enrutamiento dinámico y facilitan el proceso de enrutamiento. No son necesarios en una red pequeña si se utilizan solamente rutas estáticas. Los paquetes de protocolo de enrutamiento ocupan ancho de banda y operan independientemente de los paquetes de datos enrutados que atraviesan la red. No hay ninguna información en un paquete IP que se relacione con el protocolo de enrutamiento que se utiliza. Los routers se envían entre sí periódicamente información acerca de las rutas (tablas de enrutamiento), de modo que cuando reciben un paquete de protocolo enrutado (como IP) saben a dónde deben enviarlo. Si comparamos la

dirección del protocolo enrutado con la dirección de una carta, se puede comparar el protocolo de enrutamiento con el mensajero que se traslada entre los routers para indicarles cuáles son la rutas que están abiertas y cuáles son las más rápidas. Los protocolos de enrutamiento se pueden clasificar en general según si son interiores o exteriores, y se subdividen por tipo: vector distancia o estado de enlace.

Protocolos de enrutamiento interiores

Los protocolos de enrutamiento interiores se utilizan dentro de una red privada. Por ejemplo, una empresa puede tener varias LAN en distintas ubicaciones geográficas, conectadas por routers y por enlaces de WAN dedicados (como T1 o Frame Relay). Si todos esos routers están bajo un sistema de administración común o autónomo (que no está conectado a través de Internet), entonces deben utilizar un protocolo de enrutamiento interior. Los protocolos de enrutamiento interior puede clasificarse de la siguiente manera: (1) Vector distancia, (2) Estado de enlace e (3) Híbrido. Estos tres tipos se distinguen en las métricas que emplean para seleccionar rutas y en la forma de que se almacenan y se intercambian las actualizaciones de tabla de enrutamiento.

Protocolos de enrutamiento exterior

Los protocolos de enrutamiento exteriores se utilizan para las comunicaciones entre sistemas autónomos y a través de Internet. Entre los ejemplos de protocolos exteriores se incluyen el Protocolo de gateway fronterizo (BGP) y el Protocolo de gateway exterior (EGP). BGP es el protocolo de enrutamiento exterior más común y su versión más reciente es BGP4.

Herramientas / Preparación:

Antes de comenzar esta práctica de laboratorio, el profesor o el ayudante de laboratorio debe tener la configuración de laboratorio estándar de 5 routers, con un protocolo de enrutamiento (RIP o IGRP) habilitado. Además, debe haber disponibles estaciones de trabajo con HyperTerminal para conectarse a través de la consola con los routers. Los estudiantes pueden trabajar individualmente o en equipos. Antes de comenzar esta práctica de laboratorio, puede resultarle útil repasar el capítulo 5 de la Guía del segundo año de la Academia de Networking de Cisco, sobre Protocolos de enrutamiento: IGRP. También debe repasar la lección 5 en línea del semestre 3. A continuación, presentamos una lista del equipo requerido.

- Configuración de laboratorio estándar de 5 routers de Cisco, con hubs y switches
- Estaciones de trabajo para conectarse a los routers
- Cable de consola (roll-over)
- Cable Ethernet CAT 5 desde la estación de trabajo al hub o switch

Recursos de sitio Web:

- Routing basics
- RIP routing protocol
- IGRP routing protocol
- EIGRP routing protocol
- OSPF routing protocol
- BGP routing protocol
- EGP routing protocol
- <u>Tech tips for IGRP and EIGRP routing protocol</u>
- <u>Configuring IP routing protocols</u>
- Basic IP addressing and Troubleshooting guide

Notas:

Paso 1 - Repasar los protocolos de enrutamiento de gateway interior.

1. La siguiente tabla suministra una lista de algunos de los protocolos de enrutamiento interior más comunes. Complete la tabla, proporcionando la información solicitada de acuerdo con su propio conocimiento. Puede buscar las respuestas en el libro de texto o en línea, o puede recurrir a los sitios de Web.

Protocolos de enrutamiento de gateway interior

Protocolo de enrutamiento	Tipo de protocolo: (vector distancia, estado de enlace, híbrido)	Desarrollado por: (Fabricante / Estándares)	Características/Notas
RIP (v1 y v2) (Protocolo de información de enrutamiento)			
IGRP (Protocolo de enrutamiento de gateway interior)			
OSPF (Primero la ruta libre más corta)			
EIGRP (Protocolo de enrutamiento de gateway interior mejorado)			

Paso 2 - Verificar cuáles son los protocolos de ENRUTAMIENTO que el router puede comprender.

Los protocolos de enrutamiento hacen posible que el router se entere de otras rutas. Para ver una lista de los protocolos de enrutamiento IP reconocidos y de las redes y rutas que se han aprendido, utilice el comando show IP route desde el modo usuario

Router> show IP route

2.

¿Cuáles son algunos de los protocolos de enrutamiento admitidos?

También puede ver los protocolos de enrutamiento admitidos en una lista por orden alfabético con las definiciones. Entre al modo privilegiado, luego al modo de configuración y luego utilice la ayuda escribiendo router ?.

Router#(config)# router ?

3.

¿Los protocolos de enrutamiento que aparecen en la lista son los mismos?

Paso 3 - Determinar cuáles son los protocolos de ENRUTAMIENTO que se utilizan.

Puede ver cuáles son las interfaces y las redes definidos para los protocolos de enrutamiento que están en uso. Esto significa que publicarán y recibirán actualizaciones de enrutamiento para esas interfaces. Utilice el comando show run para ver qué protocolo se encuentra activo y en qué interfaces se encuentra.

Router# show run

4. ¿Cuál es el protocolo de enrutamiento que se utiliza y cuáles son las redes que se publicarán?

Paso 4 - Verificar cuáles son los protocolos ENRUTADOS que el router puede comprender.

Los protocolos enrutados (o enrutables) permiten que los paquetes se muevan desde una red hacia otra. Para ver la lista de los protocolos enrutados soportados, entre al modo privilegiado, luego al modo de configuración y utilice la ayuda escribiendo ?. Aparecen muchos comandos pero usted debe ser capaz de seleccionar los protocolos enrutados.

Router(config)# ?

5. ¿Cuáles son los protocolos enrutados que aparecen en la lista?

Paso 5 - Determinar cuáles son los protocolos ENRUTADOS que se utilizan.

Cada router de nuestra práctica de laboratorio está conectado directamente a por lo menos una red, y la mayoría de los routers están conectados a 2 o más redes. Para ver cuáles son los protocolos enrutados que están en uso en el router, introduzca el comando show protocols en el modo usuario.

router> show protocols

6. ¿Cuáles son los protocolos enrutados que están en uso? ¿En qué interfaz o interfaces?

Paso 6 - Complete el diagrama de árbol de los protocolos enrutados y de enrutamiento.

7. Llene los cuadros en el diagrama de árbol que muestran la relación y los nombres de protocolo para los protocolos enrutados y de enrutamiento más comunes. Esto le ayudará a visualizar el árbol cuando trabaje con estos protocolos. Empiece desde el principio con las categorías enrutado y de enrutamiento, luego cree bifurcaciones para interior, exterior, vector distancia, estado de enlace, etc. Utilice las abreviaturas y las siglas de la leyenda que figura al pie del diagrama para llenar los cuadros. Debe utilizarlas todas.



Leyenda:

IP = Protocolo Internet, IPX = Intercambio de paquetes de internetworking, A/T = AppleTalk, D.V. = Vector distancia, L.S. = Estado de enlace, HYB = Híbrido, BGP = Protocolo de gateway fronterizo, EGP = Protocolo de gateway exterior, RIP = Protocolo de información de enrutamiento, IGRP = Protocolo de enrutamiento de gateway interior, OSPF = Primero la ruta libre más corta, EIGRP = Protocolo de enrutamiento de gateway interior mejorado, INTERIOR, EXTERIOR

Práctica de laboratorio 5.4.3: Migración de RIP a IGRP - Descripción general

Duración estimada: 30 min.

Objetivos:

- Verificar si los protocolos de enrutamiento funcionan correctamente
- Verificar la tabla de enrutamiento e interpretar las entradas de red
- Verificar las rutas estáticas y eliminarlas si es necesario
- Comparar RIP con IGRP basándose en la distancia administrativa
- Convertir una red de router basada en RIP en IGRP

Información básica:

En esta práctica de laboratorio trabajará con dos protocolos de enrutamiento interior dinámicos: Protocolo de información de enrutamiento (RIP) y Protocolo de enrutamiento de gateway interior (IGRP). Los protocolos de enrutamiento son los protocolos que utilizan los routers para comunicarse entre sí a fin de intercambiar información de forma dinámica acerca de las redes que pueden alcanzar y de la conveniencia de las rutas disponibles. Los protocolos enrutados (tales como IP e IPX) son aquellos protocolos que se pueden enrutar entre redes para permitir que los paquetes se desplacen de una ubicación a otra. Los routers pueden ejecutar múltiples protocolos de enrutamiento y enrutados.

Tanto RIP como IGRP son protocolos de enrutamiento por vector distancia. RIP es el protocolo de enrutamiento más antiguo y utiliza solamente el número de saltos como métrica para determinar la mejor ruta. IGRP es un protocolo patentado por Cisco que utiliza métricas, tales como el ancho de banda y el retardo, para determinar la mejor ruta. Puede resultar conveniente que una red de routers que utiliza RIP se convierta a IGRP, ya que este protocolo tiene una limitación de número de saltos mucho mayor y utiliza el ancho de banda como métrica, lo que da como resultado mejores decisiones de enrutamiento cuando se trabaja con una internetwork con rutas alternativas.

Usted se conectará con el router a través de la consola y verificará el estado de la tabla de enrutamiento IP, así como también las redes que pueden ser alcanzadas por cada router. Agregará IGRP a un router que tiene solamente RIP y luego eliminará RIP. La habilidad para aplicar e interpretar los protocolos de enrutamiento es esencial para el mantenimiento de las internetworks.

Herramientas / Preparación:

Antes de comenzar esta práctica de laboratorio, el profesor o el ayudante de laboratorio debe tener la configuración de laboratorio estándar de 5 routers, con RIP habilitado. Las estaciones de trabajo con HyperTerminal deben estar disponibles para conectarse a través de la consola con los routers. Se trabaja individualmente o en equipos. Antes de comenzar esta práctica de laboratorio, puede resultarle útil repasar el capítulo 5 de la Guía del segundo año de la Academia de Networking de Cisco, sobre Protocolos de enrutamiento: IGRP. También conviene repasar la Lección 5 en línea del Semestre 3. Se requieren los siguientes recursos:

- Configuración de laboratorio estándar de 5 routers de Cisco, con hubs y switches
- Estaciones de trabajo para conectarse a los routers
- Cable de consola (roll-over)
- Cable Ethernet CAT 5 desde la estación de trabajo al hub o switch

Recursos de la Web:

- Routing basics
- General information on routers
- 2500 series routers
- <u>1600 series routers</u>
- Terms and acronyms
- IP routing protocol IOS command summary

Notas:

Paso 1. Verificar que los routers conozcan las demás redes del laboratorio.

1. Para mostrar en pantalla la tabla de enrutamiento y ver las actualizaciones de enrutamiento que se han producido y las redes que el router conoce, emita el siguiente comando:

router> show IP route

2. ¿Qué letra aparece en la primera columna de la tabla de enrutamiento para cualquier red/subred conectada directamente al router?

3. ¿Qué letra(s) puede(n) aparecer en la primera columna de la tabla de enrutamiento para cualquier otra red que NO esté directamente conectada al router? (consulte la leyenda en la parte superior de la pantalla del comando show IP route)

Paso 2. Determinar las redes que están conectadas directamente.

Cada router de nuestro laboratorio está conectado directamente a por lo menos una red, y la mayoría de los routers están conectados a 2 o más redes.

1. En la siguiente tabla, haga una lista de las redes (clase A, B o C, NO las subredes) a las cuales cada router está directamente conectado (utilizará esta información más adelante cuando habilite IGRP).

2. ¿Cuál es la diferencia entre la dirección de interfaz de un router y la dirección de la red conectada?

Lab-A		
Lab-B		
Lab-C		
Lab-D		
Lab-E		

Paso 3. Determinar si hay rutas estáticas y eliminarlas.

1. ¿Qué letra aparece en la primera columna de la tabla de enrutamiento para cualquier red/subred para la que hay una ruta estática?

2. Si hay alguna ruta estática configurada en los routers en esta práctica de laboratorio es necesario eliminarla, ya que nuestro objetivo es que los routers aprendan las rutas a través del protocolo de enrutamiento IGRP. Para descubrir las sentencias de configuración para las rutas estáticas, emita el siguiente comando. ¿Hay alguna ruta estática?

router#show running-config

(tenga en cuenta cualquier comando que tenga la forma **"IP route ..."**, que debe estar cerca del final del resultado)

3. Entre al modo de configuración y elimine cualquier ruta estática con el comando:

router#config term

4. Elimine cada una de las rutas estáticas con un comando NO que tenga la forma:

router(config)#no IP route ...

(asegúrese de introducir exactamente lo que encontró en el comando show runningconfig, pero con un "**no**" delante).

Paso 4. Rutas conocidas con RIP e IGRP.

1. ¿Qué letra aparece en la primera columna de la tabla de enrutamiento para cualquier red/subred aprendida a través de RIP?

Una vez que ha realizado la conversión a IGRP con éxito y por completo, cada una de las entradas aprendidas a través de RIP se debe reemplazar por una entrada similar.

2. ¿Qué letra aparecerá en la primera columna cuando se esté aprendiendo la red/subred a través de IGRP?

Paso 5. Habilitar el enrutamiento IGRP.

1. Emita los siguientes comandos:

router(config)#router igrp 100

```
router(config-router)#network a.b.c.d
```

(donde a.b.c.d es la dirección de red, por ejemplo, 204.204.7.0)

(Agregue una sentencia de red para cada red directamente conectada al router que se está configurando. Para ello, consulte la tabla que completó anteriormente)

Paso 6. Verificar que IGRP se encuentre en ejecución y que esté configurado correctamente.

1. Emita el siguiente comando:

Router> show IP protocol

2. En este punto, todavía está ejecutando dos protocolos de enrutamiento para IP, RIP e IGRP, y ambos deben figurar en la lista. El resultado incluye la distancia administrativa de los dos protocolos de enrutamiento; complete esos valores a continuación.

RIP: _____

IGRP:

La distancia administrativa se utiliza para seleccionar el protocolo de enrutamiento que se prefiere cuando hay más de un protocolo en uso. El valor más bajo indica mayor preferencia. Como IGRP tiene una distancia administrativa más baja, será el protocolo preferido. Sin embargo, si alguno de los routers en nuestro laboratorio todavía no se ha configurado correctamente para el uso de IGRP, la información de RIP será la que se aprenda y se utilice. Continúe emitiendo el comando show IP route hasta que no haya más información de RIP en la tabla y luego desactive RIP.

Paso 7. ¿Cuál es el comando que se utiliza para desactivar el protocolo de enrutamiento RIP?

Práctica de laboratorio 5.4.6.1: Configuración de IGRP - Descripción general

Duración estimada: 30 min.

Objetivos:

- Aprender a configurar IGRP como el protocolo de enrutamiento de la red
 - Ajustar las métricas IGRP configurables

Información básica

En esta práctica de laboratorio, trabajará con el Protocolo de enrutamiento de gateway interior (IGRP) de Cisco. Los protocolos de enrutamiento son los protocolos que utilizan los routers para comunicarse entre sí a fin de intercambiar información acerca de las redes que pueden alcanzar y de la conveniencia de las rutas disponibles. Los protocolos enrutados (tales como IP e IPX) son aquellos protocolos que se pueden enrutar entre redes para permitir que los paquetes se desplacen de una ubicación a otra. Los routers pueden ejecutar múltiples protocolos de enrutados.

IGRP es un protocolo de enrutamiento por vector distancia dinámico desarrollado por Cisco a mediados de la década del 80 para el enrutamiento en un sistema autónomo que contiene redes grandes y complejas con diferentes características de ancho de banda y retardo. El distrito escolar ha decidido implementar IGRP como el protocolo de enrutamiento. Se han realizado varios pedidos a InterNIC, quien ha emitido un número de Sistema autónomo de 100 a la Oficina de Distrito.

Implementación de IGRP de Cisco

IGRP utiliza una combinación de métricas que el usuario puede configurar, incluyendo retardo de internetwork, ancho de banda, confiabilidad y carga. IGRP también publica tres tipos de rutas: interior, sistema y exterior. Las rutas interiores son rutas entre subredes en la red conectada a una interfaz de router. Si la red está conectada a un router que no está dividido en subredes, IGRP no publica rutas interiores. Las rutas de sistema son rutas hacia redes ubicadas dentro de un sistema autónomo. El software Cisco IOS deriva rutas de sistema desde interfaces de red conectadas directamente y de información de ruta de sistema suministrada por otros routers que utilizan IGRP o servidores de acceso. Las rutas de sistema no incluyen información de subred. Las rutas exteriores son rutas hacia redes ubicadas fuera del sistema autónomo que se tienen en cuenta al identificar un gateway de último recurso. El software Cisco IOS elige un gateway de último recurso de la lista de rutas exteriores que suministra IGRP. El software utiliza el gateway (router) de último recurso si no tiene una mejor ruta para el paquete y el destino no es una red conectada. Si el sistema autónomo tiene más de una

conexión hacia una red externa, los distintos routers pueden seleccionar distintos routers exteriores como el gateway de último recurso.

Herramientas / Preparación:

Antes de comenzar esta práctica de laboratorio, el profesor o el ayudante de laboratorio debe haber configurado el laboratorio estándar de 5 routers y debe haber eliminado de éste todos los protocolos dinámicos y las rutas estáticas. Esto se lleva a cabo emitiendo los comandos no router igrp xxx y no ip route xxx.xxx.xxx desde el nivel de comando Router(config)# del nivel enable exec user. Se trabaja individualmente o en equipos. Antes de comenzar esta práctica de laboratorio, puede resultarle útil repasar el capítulo 5 de la Guía del segundo año de la Academia de Networking de Cisco, sobre Protocolos de enrutamiento: IGRP. También conviene repasar la Lección 4 en línea del Semestre 3. Se requieren los siguientes recursos.

- Configuración de laboratorio estándar de 5 routers de Cisco, con hubs y switches
- Estación de trabajo conectada al puerto de consola del router
 - Cable de consola (roll-over)

Recursos de la Web:

Routing basics General information on routers 2500 series routers 1600 series routers Terms and acronyms IP routing protocol IOS command summary

Notas:

Ejecute los siguientes pasos utilizando uno de los 5 routers del laboratorio. El indicador del router que aparece aquí es el indicador por defecto de "Router" suponiendo que no se ha asignado ningún nombre de host al router. El indicador verdadero puede variar (por ej.: LAB-A o LAB-B, etc.)

Paso 1 - Entrar al modo user exec.

Paso 2 - Hacer ping a todas las interfaces en el router y a todas las interfaces en los routers vecinos conectados directamente.

Documente en su diario de ingeniería de práctica de laboratorio las respuestas obtenidas mediante el comando ping de ICMP.

¿Cuáles son las interfaces del router que respondieron con un ping exitoso?

Paso 3 - Mostrar en pantalla los protocolos de enrutamiento actuales en uso mediante el siguiente comando:

Router>show ip protocols ¿Hay algún protocolo de enrutamiento definido?

(Si lo hay, se debe eliminar y luego debe repetir los pasos 1 y 2; consulte la práctica de laboratorio 5.4.3 para saber cómo se lleva a cabo la eliminación)

Paso 4 - Entrar al modo exec privilegiado con la contraseña class, utilizando el siguiente comando:

Router>enable Contraseña: class

Paso 5 - Mostrar en pantalla la configuración actual que se ejecuta en la RAM mediante el siguiente comando:

Router**#show running-config** ¿Hay alguna ruta estática definida?

(Si la hay, se debe eliminar; consulte para ello la práctica de laboratorio 5.4.3)

Paso 6 - Entrar al modo de configuración con el siguiente comando:

Router#config term

Paso 7 - Habilitar IGRP en este router con el siguiente comando:

Router(config)#router igrp 100 ¿Qué cambió en el indicador del router?

Paso 8 - Definir cuáles son las redes que utilizarán IGRP introduciendo el siguiente comando:

Router(config-router)**#network xxx.xxx.xxx**.**xxx** (Donde xxx.xxx.xxx.xxx es la dirección IP de una de las redes conectadas directamente al router).

1. ¿Cuál fue la respuesta del router?

Paso 9 - Repetir el paso 8 para todas las redes directamente conectadas al router.

Paso 10 - Introducir Exit (salir).

Paso 11 - Introducir CNTL-Z.

Paso 12 - Mostrar en pantalla el archivo de configuración actual del router en la RAM mediante el siguiente comando:

Router#show running-config

¿El protocolo IGRP del router está activado y publica las redes que ha definido?

Paso 13 - Introducir el siguiente comando en el indicador de modo privilegiado:

Router#copy run start ¿Qué hace este comando?

Paso 14 - Mostrar en pantalla los protocolos de enrutamiento actuales en uso mediante el siguiente comando:

Router#show ip protocols

Anote en su Diario de ingeniería de Práctica de laboratorio cualquier información importante obtenida mediante este comando. ¿Qué protocolo de enrutamiento apareció?

Paso 15 - Mostrar en pantalla la tabla de enrutamiento IP para ver cuáles son las redes que este router conoce.

Router#show ip route

Anote en su Diario de ingeniería de Práctica de laboratorio cualquier información importante obtenida mediante este comando. ¿Cuáles son las redes que aparecen en la lista?

Paso 16 - Mostrar en pantalla las interfaces del router y sus estadísticas.

Router#show ip interface

Anote en su Diario de ingeniería de Práctica de laboratorio cualquier información importante obtenida mediante este comando. ¿Cuáles son las interfaces que están en uso?

Paso 17 - Habilitar la depuración de IGRP con el siguiente comando:

Router#debug ip igrp transactions

Anote en su Diario de ingeniería de Práctica de laboratorio cualquier información importante obtenida mediante este comando. ¿Cuál fue el efecto de este comando?

Paso 18 - Verificar las configuraciones básicas por defecto actuales para los temporizadores con el siguiente comando:

Router#show ip protocol

¿Cuál es la configuración actual para los cuatro temporizadores básicos?

Update (actualización):

Invalid (no válido):

Hold down (Espera):

Flushed (Purgado):

Paso 19 - Volver a configurar los temporizadores de red IGRP a sus valores por defecto con el siguiente conjunto de comandos:

Router#config term Router(config)#router igrp 100 Router(config-router)#no timers basic ¿Cuál es el propósito de este comando?

Paso 20 - Asegurarse de que el router ya no esté recibiendo rutas, mediante el siguiente comando:

Router#show ip route

Paso 21 - Ajustar los temporizadores de red utilizando el siguiente comando.

Todos los dispositivos en un sistema autónomo IGRP deben usar los temporizadores de manera uniforme. La uniformidad es esencial con respecto a la frecuencia de envío de las actualizaciones y la duración de la espera. Use el siguiente conjunto de comandos para ajustar los temporizadores en configuraciones distintas de aquéllas por defecto del paso 18:

Router# config term Router(config)#router igrp 100 Router(config-router)#timers basic update invalid holddown flush [sleeptime] (se debe reemplazar cada una de las palabras que aparecen en cursiva por un número de segundos)

Anote en su Diario de ingeniería de Práctica de laboratorio cualquier información importante obtenida mediante este comando y el significado de su emisión.

Paso 22 - Establecer un diámetro máximo de red de 2 saltos mediante el siguiente conjunto de comandos:

Router#config term Router(config)#router igrp 100 Router(config-router)#metric maximum-hops 2

Paso 23 - Desactivar la depuración del protocolo IP mediante el siguiente comando:

Router#no debug ip igrp transactions

Anote en su Diario de ingeniería de Práctica de laboratorio cualquier información importante obtenida mediante este comando

Práctica de laboratorio 5.4.6.2: IGRP de múltiples rutas - Descripción general

Duración estimada: 60 min.

Objetivos:

- Trabajar con métricas de IGRP utilizadas en la selección de rutas
- Comprender la ruta que se selecciona para enrutar datos a un host en particular.

Información básica

En una práctica de laboratorio anterior, se describió cómo configurar el protocolo de enrutamiento RIP en los routers de Cisco. En esta práctica de laboratorio, configurará los routers para utilizar IGRP y observará cómo IGRP utiliza las métricas para seleccionar la mejor ruta.

Inicialmente, un router debe consultar entradas sobre las redes o subredes directamente conectadas a él. Cada interfaz se debe configurar con una dirección IP y una máscara de subred. La fuente inicial de esta información proviene del usuario que la escribe en un archivo de configuración. IGRP (Protocolo de enrutamiento de gateway interior) es un protocolo de enrutamiento por vector distancia desarrollado por Cisco para resolver problemas relacionados con el enrutamiento en redes grandes y heterogéneas.

RIP envía actualizaciones de enrutamiento cada 30 segundos y utiliza solamente el número de saltos para determinar la mejor ruta. IGRP envía actualizaciones de enrutamiento a intervalos de 90 segundos y utiliza una combinación de variables para determinar la mejor ruta para enrutar paquetes. Las variables que conforman esta métrica compuesta incluyen ancho de banda, retardo, carga, confiabilidad y MTU (unidad máxima de transmisión). En el sitio 'Introducción a IGRP' que aparece en la sección Recursos de la Web de esta práctica de laboratorio hay información detallada acerca de la forma en que IGRP calcula la mejor ruta.

IGRP adopta una táctica más inteligente para determinar la mejor ruta que RIP. RIP sólo cuenta el número de routers (saltos) desde el punto A hasta el punto B, mientras que IGRP tiene en cuenta, entre otros factores, la velocidad de los diversos enlaces antes de determinar la mejor ruta.

En esta práctica de laboratorio se agrega un enlace WAN entre Lab-A y Lab-E. Este enlace se configurará para una velocidad de 56Kbps. Los demás enlaces de WAN se configuran para 1.544 Kbps (velocidad T1) por defecto. Examinará las tablas de enrutamiento y determinará cuál es la ruta que tomarán los datos. Por último, deshabilitará uno de los enlaces más rápidos entre los routers obligando que los datos se enruten a través del enlace WAN de 56Kbps.

Herramientas / Preparación:
Antes de iniciar esta práctica de laboratorio, debe tener disponible el equipo de laboratorio estándar de 5 routers. El instructor o el ayudante de laboratorio debe preconfigurar los routers y las estaciones de trabajo con las configuraciones IP correctas antes de comenzar con la práctica de laboratorio. Se trabaja en grupos de 3 o más personas. Antes de empezar esta práctica de laboratorio, puede resultarle útil repasar el capítulo 5 de la Guía del segundo año de la Academia de Networking de Cisco y el capítulo 5 en línea del Semestre 3.

Recursos requeridos:

- (5) estaciones de trabajo de PC (mín.) con el sistema operativo Windows e HyperTerminal instalados.
- (5) routers Cisco (modelo de la serie 1600 o de la serie 2500 con IOS 12.0.9 o una versión posterior).
- (4) hubs Ethernet (10BASE-T con 4 a 8 puertos).
- (1) switch Ethernet (Cisco Catalyst 1900 u otro similar).
- (5) cables de consola serial para conectar la estación de trabajo al puerto de consola (con convertidores de RJ-45 a DB9).
- (4) conjuntos de cables seriales WAN V.35 (DTE macho / DCE hembra) para conectarse de router a router.
- Cables Ethernet CAT5 de conexión directa para conectar los routers y estaciones de trabajo a hubs y switches.
- Transceivers AUI (DB15) a Ethernet RJ-45 (la cantidad depende de la cantidad de routers con puertos AUI) para convertir las interfaces del router AUI a 10BASE-T RJ-45

Recursos de la Web:

Routing basics General information on routers 2500 series routers 1600 series routers Terms and acronyms IP routing protocol IOS command summary Introduction to IGRP

Paso 1 - Conectar el router Lab-A a Lab-E.

Conecte el lado DCE de un cable serial de WAN V.35 en el puerto Serial 0 de **Lab-E**. Conecte el otro extremo del cable (el extremo DTE) al puerto Serial 1 de **Lab-A**.

Paso 2 - Configurar el puerto serial en Lab-E.

En Lab-E, entre al modo EXEC privilegiado escribiendo el comando enable. Si se le pide que lo haga, introduzca la contraseña class. Entre al modo de configuración global introduciendo el comando configure terminal (abreviatura config t). Entre al modo de configuración de interfaz para el puerto Serial 0 introduciendo el comando interface serial 0 (abreviatura int s 0). Asigne la dirección IP 220.68.33.1 al puerto serial introduciendo el comando ig address 220.68.33.1 255.255.255.0. Este enlace de WAN es un circuito de 56 Kbps, de modo que introduzca el comando bandwidth 56. Asigne la velocidad de reloj de 56000 bits por segundo introduciendo el comando clock rate 56000. Active la interfaz introduciendo el comando el comando no shutdown. Escriba la secuencia clave Control+Z para volver a la interfaz de línea de comando.

Paso 3 - Configurar el puerto serial en Lab-A.

En Lab-A, entre al modo EXEC privilegiado escribiendo el comando enable. Si se le pide que lo haga, introduzca la contraseña **class**. Entre al modo de configuración global introduciendo el comando **configure terminal** (abreviatura **config**t). Entre al modo de configuración de interfaz para el puerto Serial 1 introduciendo el comando interface Serial 1 (abreviatura int s 1).

Asigne la dirección IP 220.68.33.2 al puerto serial introduciendo el comando ip address 220.68.33.2 255.255.255.0. Este enlace de WAN es un circuito de 56 Kbps, de modo que introduzca el comando bandwidth 56. Active la interfaz introduciendo el comando no shutdown. Escriba la secuencia clave Control+Z para volver a la interfaz de línea de comando.

Paso 4 - Documentar el cambio en la topología de red.

Para completar con éxito esta práctica de laboratorio, debe consultar el diagrama de topología que aparece al comienzo de esta práctica de laboratorio. Dibuje un enlace WAN (que se indica a través de una línea en forma de rayo) entre Lab-A y Lab-E. Indique el número de red **220.68.33.0** colocándolo sobre este enlace. Indique el punto en el que la línea se conecta a Lab-E como S0 (DCE), con una dirección IP **220.68.33.1**. Indique el punto en el que la línea se conecta a conecta a Lab-A como S1 con una dirección IP de **220.68.33.2**.

Paso 5 - Configurar el enrutamiento IGRP en cada router.

Cada router en el laboratorio se debe configurar con IGRP y el mismo número de sistema autónomo. Para los fines de esta práctica de laboratorio, utilice el número **10**. En cada router, entre al modo EXEC privilegiado escribiendo el comando **enable**. Si se le pide que lo haga, introduzca la contraseña **class**. Entre al modo de configuración global introduciendo el comando **configure terminal** (abreviatura **config** t). Para asegurarse de que el enrutamiento RIP no esté en uso en los routers del laboratorio, introduzca el comando no router rip. Para comenzar a configurar IGRP introduzca el comando **router igrp 10** (donde 10 es el número de sistema autónomo que se le ha asignado).

1. ¿Qué cambió en el indicador? Router-name(config-router)#

IGRP requiere que el administrador del router introduzca el número de red de todas las redes que están conectadas físicamente a él. El comando para hacer esto es network xxx.xxx.xxx. (donde xxx.xxx.xxx.xxx es la dirección IP de la red conectada a la interfaz, no la dirección IP de la interfaz en sí misma). Consulte el diagrama de topología de red que aparece al comienzo de esta práctica de laboratorio con respecto a estos números. Asegúrese de incluir la dirección IP de las redes en los puertos Ethernet así como también las de los puertos seriales (consulte el ejemplo que se suministra a continuación). Escriba la secuencia clave Control+Z para volver a la interfaz de línea de comando. Guarde la configuración del router en la NVRAM introduciendo el comando copy running-config startup-config (abreviatura copy run start).

Ejemplo para Lab-A:

```
Lab-A(config)# router igrp 10
Lab-A(config-router)# network 205.7.5.0
Lab-A(config-router)# network 192.5.5.0
Lab-A(config-router)# network 201.100.11.0
Lab-A(config-router)# network 220.68.33.0
```

Paso 6 - Examinar la tabla de enrutamiento.

Conéctese al router Lab-C y emita el comando show ip route.

2. Registre los resultados a continuación:

Observará que la "**C**" en la primera columna indica que la red está conectada directamente al router. La "**I**" en la primera columna indica que la red se conoció a través de IGRP. El primer número entre corchetes indica la distancia calculada hacia el router en particular. El segundo número indica la métrica calculada hacia el router en particular.

Paso 7 - Examinar la ruta que atraviesan los datos.

Desde Lab-C, siga la ruta que atraviesan los datos para llegar a la interfaz S0 en Lab-E. Emita el comando traceroute 220.68.33.1 (abreviatura tr 220.68.33.1).

3. ¿Cuál es la ruta que atraviesan los datos?

Paso 8 - Examinar la ruta que atraviesan los datos entre dos routers distintos.

Conéctese a Lab-E. Haga trace desde Lab-E hacia la interfaz Ethernet 1 del router Lab-A introduciendo el comando traceroute 192.5.5.1 (abreviatura tr 192.5.5.1).

4. ¿Cuál es la ruta que sigue el comando traceroute?

5. ¿Por qué la ruta no se desplazó desde Lab-E a Lab-A?

Paso 9 - Desactivar uno de los enlaces rápidos entre los routers.

Como la red de routers tiene más de una ruta para enrutar los datos, hay algo de redundancia en el sistema. Si uno de los enlaces entre los routers deja de funcionar, los datos se pueden enrutar a través de una ruta alternativa. Este enrutamiento se produce una vez que la red ha convergido.

Desde Lab-E, emita el comando show ip route.

6. Registre los resultados a continuación.

Desconecte el cable de la interfaz Ethernet 0 de Lab-E. El resultado del comando show ip route (anterior) indica que todo el tráfico desde Lab-E se enrutó a través de la interfaz Ethernet 0.

Introducción del comando traceroute 192.5.5.1 (abreviatura tr 192.5.5.1).

7. ¿Cuál es la ruta que sigue ahora el comando traceroute?

8. Registre los resultados a continuación.

Tenga en cuenta que la métrica de IGRP (el segundo número entre corchetes) en cada ruta ha aumentado significativamente a partir de los resultados que registró en la pregunta 6. Esto indica que el enlace WAN de 56Kbps, entre Lab-E y Lab-A, es más lento. Aunque es más lento, ésta es la única manera de enrutar el tráfico desde Lab-E.

Paso 10 - Examinar el enrutamiento del tráfico desde otro router. Conéctese a Lab-C. Observe que la red tarda en converger entre los pasos 9 y 10. Introduzca el comando clear ip route * para hacer que el router borre toda la información de la tabla de enrutamiento y obtenga nueva información de los demás routers a través de un broadcast. Emita el comando show ip route, y compare los resultados con los resultados que registró en la pregunta 2.

9. ¿Alguna de las rutas ha cambiado?

10. ¿Cuál es la interfaz que utiliza esta ruta ahora?

Examine la ruta que toman los datos ahora para ir a la interfaz Serial 0 en Lab-E. Introduzca el comando traceroute 220.68.33.1 (abreviatura tr 220.68.33.1).

11. ¿Cuál es la ruta que sigue ahora el comando traceroute?

Práctica de laboratorio 5.4.6.3: Neotrace y traceroute - Descripción general

Duración estimada: 15 min.

Objetivos:

- Utilizar el programa NeoTrace para verificar la ruta de red desde el router origen hacia el router destino con una representación gráfica.
- Verificar que la capa de red entre origen, destino y cada router que encuentre en el camino esté funcionando correctamente. Recuperar información para evaluar la confiabilidad de ruta de extremo a extremo.
- Determinar los retardos en cada punto de la ruta y si es posible alcanzar el host.

Información básica:

En esta práctica de laboratorio, utilizará el programa shareware **NeoTrace** para determinar la ruta que atraviesan los datos a través de una internetwork. En el semestre 2 completó una práctica de laboratorio utilizando el comando traceroute del software Cisco IOS. NeoTrace utiliza gráficos para describir los resultados del comando traceroute. Además, NeoTrace muestra la información "Whois" para cada router, buscando el propietario del nombre de dominio y rotulando esta información para cada router en la ruta de datos.

El comando **traceroute** utiliza paquetes ICMP y el mensaje de error generado por los routers cuando el paquete supera su Tiempo de **E**x istencia (TTL). Al iniciar el comando traceroute hacia un host objetivo el router envía un paquete de petición de eco ICMP con el TTL establecido en uno (1). El primer router en la ruta hacia el host objetivo recibe el paquete de petición de eco ICMP y establece el TTL en cero (0). El primer router vuelve a envíar entonces un mensaje ICMP de tiempo excedido nuevamente al origen. El router origen envía entonces un paquete de petición de eco ICMP y establece el TTL en uno (1) y lo envía al siguiente router en la ruta hacia el host objetivo. El segundo router recibe la petición de eco ICMP y establece el TTL en uno (1) y lo envía al siguiente router en la ruta hacia el host objetivo. El segundo router recibe la petición de eco ICMP y establece el TTL en uno (1) y lo envía al siguiente router en la ruta hacia el host objetivo. El segundo router recibe la petición de eco ICMP y establece el TTL en uno (1) y lo envía al siguiente router en la ruta hacia el host objetivo. El segundo router recibe la petición de eco ICMP y establece el TTL en uno (0) luego, envía un mensaje de tiempo excedido ICMP nuevamente al origen. El origen envía entonces una petición eco ICMP con un TTL establecido en 3. Este ciclo continúa hasta que se recibe una respuesta de eco ICMP del host objetivo o hasta que se recibe un mensaje ICMP destino inalcanzable. Esto le permite determinar cuál es el último router que se alcanzó en la ruta hacia el host objetivo. Esta es una técnica de resolución de problemas denominada aislamiento de fallas.

Herramientas / Preparación:

Antes de comenzar esta práctica de laboratorio, necesita una estación de trabajo PC con acceso a Internet y NeoTrace instalado. Puede descargar una versión de evaluación de NeoTrace. Examine el acuerdo de licencia que se suministra con NeoTrace para asegurarse de que se cumplan las normas de uso del shareware. La ubicación del programa NeoTrace se puede encontrar a continuación en Recursos de la Web.

Recursos requeridos:

- PC con monitor, teclado, ratón y cables de alimentación, etc.
- Sistema operativo Windows (Win 95, 98, NT o 2000) instalado en un PC
- PC con el programa NeoTrace instalado, conectado a los routers de laboratorio
- PC con el programa NeoTrace instalado y acceso a Internet

Recursos de la Web:

Routing basics General information on routers 2500 series routers 1600 series routers Terms and acronyms IP routing protocol IOS command summary NeoTrace

Paso 1 - Ejecutar el programa NeoTrace.

Inicie el programa NeoTrace haciendo clic en el botón Inicio de Windows, luego en Programas. Haga clic en el grupo de programa NeoTrace y luego haga clic en el icono NeoTrace. Si debe instalar NeoTrace, descárguelo del sitio Web que aparece en la lista anterior.

Si esta es la primera vez que se ejecuta el programa, debe completar los espacios en blanco en la pantalla Home Location. Esto permite que el programa busque la latitud y la longitud de su ubicación. Haga clic en el botón "Try NeoTrace" para continuar.

Paso 2 - Introducir la dirección de un recurso de Internet al que desea hacer trace.

En el campo dirección, escriba **www.cisco.com** y presione Intro. La dirección del sitio al que está haciendo trace puede ser cualquier dirección IP o computador al que se pueda acceder desde su ubicación, ya sea en Internet o en su LAN/WAN privada.

Observará que a medida que se ejecuta el proceso de trace, se visualiza una serie de segmentos con puntos y líneas. Una vez que se completa el comando traceroute, la pantalla muestra un mapa de las ubicaciones aproximadas de los routers entre su ubicación y la del sitio Web de Cisco.

Coloque el puntero del ratón cerca del punto verde al lado de San José, California. Si hace clic con el botón izquierdo del ratón, el zoom se aproxima, y si hace clic con el botón derecho del ratón, el zoom se aleja. Aproxime el zoom hasta que vea el punto (círculo) verde con un solo segmento de línea conectado a él. Coloque el puntero del ratón en este punto.



1. ¿Cuál es la información que aparece en pantalla? (Las respuestas varían)

Paso 3 - Mostrar información acerca de los nodos.

Haga clic en la ficha **Nodes** (nodos) en la parte izquierda de la pantalla. Aparece en pantalla un diagrama de bloque de la ruta que se toma para llegar al sitio Web de Cisco. Observará que periódicamente los segmentos de línea entre cada nodo, o router, se ponen de color verde. NeoTrace está ejecutando el comando traceroute nuevamente para verificar la ruta hacia el

destino, dado que esta ruta puede cambiar. Observará que el tiempo promedio (expresado en milisegundos) puede cambiar cada vez que se ejecuta el comando traceroute. También aparece en pantalla el nombre de DNS de cada nodo.

😨 NeoTrace: www.cisc	o.com						
Ele Edit View Help							
Address www.cisco.com		×	I Lince Se	nve Print (CB O	Qations .	
Undes 101-03	e0.cg-cisco.cgc Avg Time	atm1-0.8 do-cieco. Avig Tar maricopa edu x 0 ms	dit maicopa e: 3ms 61.atm3000 A	edu faŭ phraecust.ph vg Time: 4 m faŭ	00 phras gi Avg T ex usivest e 00 phras gi	2 physic up mer 4 ms	west net
Avg Time 2 st-circopin2-400s Avg Time 2	slebb11-stk-8-0. Avg Time	Avg Im spintlink, net 23 ms wyper Cit Avg Im	si-gw12-a An co.com e: 33 ms	na-1-1-1.spri rg Time: 13 n	Avg (ntink.net 15	me: 4 ms	
WWW.CIICO.COM	pigpen.cis Avg Time	co.com 73 ma					

Paso 4 - Mostrar información de Lista

Haga clic en la ficha List (Lista) en la parte izquierda de la pantalla. NeoTrace muestra en pantalla los resultados del comando traceroute de modo muy similar al del comando traceroute de Cisco IOS: Observará que periódicamente aparece una flecha a la izquierda de la lista. NeoTrace está ejecutando el comando traceroute nuevamente para verificar la ruta hacia el destino, dado que esta ruta puede cambiar.

			11	Constant of the
#	IP Address	Name	ma	Network.
1	140.198.131.57	C101-03	0	
2	140.198.128.1	e0.cg-cisco.cgc.maricopa.edu	1	Maricopa Community Co
3	140.198.254.25	atm1+0.8.do-cisco.dist.maricopa.edu	3	Maricopa Community Co
4	206.80.195.185	61.atm3-0-0.phnx-cust.phnx.uswest.net	5	U S WEST Internet Service
5	206.80.192.251	fa0-0-0.phnx-gw2.phnx.uswest.net	6	U S WEST Internet Service
6	206.80.192.251	fa0-0-0.phnx-gw2.phnx.uswest.net	4	U S WEST Internet Service
7	144.228.207.205	sl-gw12-ana-1-1-1.sprintlink.net	14	Sprint (NET-SPRINT-IN
8	144.232.8.89	sl-bb10-stk-6-0.sprintlink.net	26	Sprint/United Information
9	144.232.4.106	sl-bb11-stk-8-0.sprintlink.net	23	Sprint/United Information
10	144.232.4.78	sl-gw10-stk-8-0-0.sprintlink.net	23	Sprint/United Information
11	144.228.146.14	sl-ciscopsn2-4-0-0.sprintlink.net	28	Sprint (NET-SPRINT-INI
12	192.31.7.9	pigpen.cisco.com	31	Cisco Systems, Inc. [NE
13	198.133.219.25	www.cisco.com	31	Cisco Systems, Inc. (NE

Paso 5 - Mostrar información gráfica.

Haga clic en la ficha Graph (Gráficos) en la parte izquierda de la pantalla. NeoTrace muestra en pantalla los resultados del comando traceroute como un gráfico de líneas. Este gráfico muestra el tiempo actual como una línea gris, y el tiempo promedio como una línea azul. El acceso vertical representa cada nodo o router en la ruta hacia el destino. Si se coloca el puntero del ratón sobre cualquiera de estos nodos, aparece en pantalla la información "Whois" (quién es) que se detecta para ese router en particular. El acceso horizontal representa el tiempo en milisegundos.



Práctica de laboratorio 6.3.6 ACL estándar - Descripción general

Duración estimada: 60 min.

Objetivos:

Esta práctica de laboratorio sirve para practicar las siguientes tareas:

- Repasar las características y capacidades de las Listas de control de acceso IP estándar (ACL)
- Desarrollar una ACL estándar para permitir o denegar tráfico específico
- Aplicar una ACL IP estándar a una interfaz de router
- Probar la ACL para determinar si se lograron los resultados deseados
- Eliminar una ACL de una interfaz de router
- Eliminar una ACL de un router

Información básica:

En esta práctica de laboratorio se trabaja con Listas de control de acceso estándar (ACL) para regular el tráfico que se permite pasar a través de un router según el origen, ya sea un host específico (normalmente una estación de trabajo o servidor) o una red completa (cualquier host o servidor en esa red). Una ACL estándar es una herramienta simple y efectiva para controlar qué paquetes pueden pasar a través de un router desde una red a otra. Las ACL estándar son una forma básica de control con capacidades limitadas. Pueden filtrar (permitir o denegar) paquetes que salen de o entran a una interfaz de router utilizando sólo la dirección IP de la red o host origen. Por lo tanto, se deben aplicar cerca de la dirección destino, ya que dicha dirección no se puede especificar.

Otros protocolos enrutados (o enrutables) como IPX o AppleTalk también pueden tener ACL o filtros pero esta práctica de laboratorio se concentra en las ACL IP. Cuando se aplica una ACL IP estándar, ésta filtra (permite o deniega) todo el conjunto de protocolo IP (IP, TCP, SMTP, HTTP, Telnet etc.). Cuando se crean las ACL IP estándar se numeran del 1 al 99. En la práctica de laboratorio siguiente se trabaja con las ACL extendidas, que se numeran del 100 al 199. Consulte la lección de texto o en línea para conocer la numeración de ACL para IPX y AppleTalk.

Estos son los pasos necesarios para usar las ACL de forma efectiva:

- Determinar los requisitos de la ACL (según las necesidades de seguridad, etc.)
- Desarrollar la ACL
- Verificar las sentencias en la ACL
- Aplicar la ACL a una interfaz de router
- Verificar que la ACL se aplique correctamente a la interfaz que se desea
- Verificar que la ACL funcione correctamente

Herramientas / Preparación:

Antes de comenzar esta práctica de laboratorio, el profesor o el ayudante de laboratorio debe haber configurado el laboratorio estándar de 5 routers. Se trabaja individualmente o en equipos. Antes de comenzar con esta práctica de laboratorio, puede resultarle útil repasar el capítulo 6 (ACL) de la Guía del segundo año de la Academia de Networking de Cisco. También conviene repasar el capítulo 6 en línea del Semestre 3. Se requiere el siguiente equipo:

- Configuración de laboratorio estándar de 5 routers de Cisco, con hubs y switches
 - Estación de trabajo conectada al puerto de consola del router mediante un cable rollover

Recursos de sitio Web:

LAN Switching basics General information on all Cisco products - (Ir al capítulo 22 - Switches) 1900 / 2820 series Ethernet switches 2900 series Fast Ethernet switches Terms and acronyms IP routing protocol IOS command summary Access Control Lists - Overview and Guidelines

Notas:

En esta práctica de laboratorio se desarrolla, aplica y prueba una ACL IP estándar. El Ejercicio A es obligatorio, mientras que el B es opcional pero recomendado. En el Ejercicio A se deben bloquear paquetes desde un host o red específico/a, impidiendo que accedan a cualquier host u otra red. En el Ejercicio B se bloquea el tráfico desde todos los hosts en una red específica,

impidiendo que accedan a cualquier host en una red completa. Se suministran las respuestas para ambos ejercicios. Consulte el diagrama de laboratorio estándar en la sección de descripción general.

Ejercicio A (obligatorio).

La ACL 1 impide que el tráfico IP desde un host específico (estación de trabajo con dirección IP 192.5.5.2) conectada al hub Ethernet de la interfaz E0 del Router LAB-A, alcance una red completa (210.93.105.0, la red entre los Routers LAB-D y LAB-E)

Ejercicio B (opcional)

La ACL 2 impide que el tráfico IP desde todos los hosts en una red específica 219.17.100.0 (una red Ethernet conectada al router LAB-B) alcance una red completa 223.8.151.0 (una red Ethernet conectada al router LAB-C)

Paso 1 - Determinar los requisitos de la ACL.

¿Cuál es tráfico (paquetes) que se bloquea (deniega) o se permite, y de qué hosts o redes proviene? Como se usa una ACL IP estándar, sólo se puede filtrar según la dirección origen. Con el ejercicio A, se desea bloquear el tráfico desde la dirección de host 192.5.5.2 desde una Ethernet en el Router LAB-A. Con el Ejercicio B, se desea bloquear el tráfico desde la dirección de red 219.17.100.0 en el Router LAB-B.

Paso 2 - Desarrollar la ACL.

Definir las sentencias ACL en modo Router(config)#. Las sentencias ACL son aditivas. Cada sentencia se agrega a la ACL. Si hay más de una sentencia en la ACL (lo que es típico) y se desea cambiar una sentencia anterior, se debe borrar la ACL y comenzar de nuevo. En estos ejemplos se bloquean paquetes desde sólo una dirección de host IP o una red. El formato o sintaxis de la sentencia de ACL IP estándar aparece a continuación:

access-list list# {permit / deny} source IP address [wildcard mask] [log]

(NOTA: Se puede usar cualquier número entre 1 y 99 para una ACL IP estándar Para eliminar la ACL, repita la parte access-list # del comando, con la palabra NO adelante).

Complete el comando ACL con la dirección origen y máscara wildcard correctas para lograr los requisitos del Ejercicio A o B (o ambos). La primera sentencia se usaría para ACL 1. La segunda sentencia se usaría para ACL 2.

Ejercicio A. access-list 1 deny _____

Ejercicio B. access-list 2 deny ______

1. ¿Cuál es el propósito de un cero (0) en una máscara wildcard?

2. ¿Cuántos bits representa cada cero decimal en la máscara wildcard anterior?

3. ¿Cuál es el propósito de un 255 en una máscara wildcard?

4. ¿Cuántos bits representa el 255?

5. Como las ACL siempre terminan con un "deny any" implícito, si se utilizan una de las sentencias anteriores esto haría que esta lista denegara una sola dirección origen, pero también denegaría implícitamente cualquier otra dirección origen. Nuestro objetivo es sólo denegar el acceso desde un solo host, de manera que es necesario agregar una segunda sentencia para permitir todo el tráfico restante. Introduzca la segunda sentencia de ACL que permite todo el tráfico restante (la misma sentencia se debe utilizar para el Ejercicio A o B:

6. ¿Por qué ambas sentencias usan el mismo número de ACL (1)?

7. ¿Qué sucedería si la primera sentencia fuera "Access-list 1" y la segunda "Access-list 2"?

Paso 3 - Verificar las sentencias en la ACL.

Utilice el siguiente comando para controlar sus sentencias y verificar que todo se haya escrito correctamente. Si desea corregir un error o hacer un cambio en una sentencia existente se debe eliminar la ACL y comenzar de nuevo. Para eliminar la ACL, repita la parte access-list # del comando, con la palabra NO adelante.

Router#show access-list 1

1. ¿Cuántas sentencias hay en la ACL?

Paso 4 - Aplicar la ACL a una interfaz de router.

Como las ACL estándar sólo pueden especificar o verificar direcciones origen, se debe aplicar el filtro lo más cerca posible del destino. ¿A qué router y a qué interfaz se puede aplicar la ACL para cada uno de los ejercicios de ejemplo, A o B? Consulte el diagrama de laboratorio estándar y llene la tabla siguiente con la dirección (o direcciones) IP que se deben bloquear, la red a la cual no deben acceder, el router donde se debe aplicar la ACL, la interfaz a la que se aplicará y si se bloquea la entrada o la salida (IN o OUT)

Ejercicio	Host IP o red que se debe denegar (bloquear)	Red a la que no deben acceder los paquetes	Router donde se debe aplicar la ACL	Interfaz donde se debe aplicar la ACL (S0, S1, E0, etc)	¿Bloque entrante o saliente? (IN о OUT)
A (ACL 1)					
B (ACL 2)					

Nota: Recuerde que debe colocar las ACL estándar cerca del destino

Introduzca los siguientes comandos para aplicar la ACL 1 a la interfaz S1 para bloquear los paquetes entrantes en la interfaz S1 para el router LAB-D. El verdadero nombre del router (por ej., LAB-D), debe aparecer en lugar de "Router" en el indicador. Para la ACL 2, la ACL se aplicaría a la interfaz E0 en LAB-C para paquetes salientes.

Router(config)#interface Serial 1 Router(config-if)#ip access-group 1 in

Paso 5 - Verificar si la ACL se aplica a la interfaz correcta:

Use el siguiente comando para verificar si la ACL se aplica a la interfaz correcta en el router correcto:

Router#show running-config

1. ¿Cuáles fueron los resultados que demuestran que la ACL se ha aplicado correctamente?

NOTA: Para eliminar una ACL de una interfaz, se debe configurar en primer lugar la interfaz como en el Paso 4 y luego repetir el segundo comando con la palabra NO adelante (no ip access-group 1).

Paso 6 - Verificar que la ACL funcione correctamente

Pruebe la ACL intentando enviar paquetes desde la red origen que se debe permitir o denegar. Emita varios comandos ping para probar estas ACL. Se indican varias pruebas para cada ejercicio.

Ejercicio	Prueba n⁰	Ping desde	A	¿Debe tener éxito?	¿Lo tuvo?
A	1	Estación de trabajo (192.5.5.2) conectada al router LAB-A	Estación de trabajo (210.93.105.2) conectada al router LAB-E		
	2	Estación de trabajo (192.5.5.2) conectada al router LAB-A	Router LAB-C Interfaz S0 (204.204.7.1)		
В	1	Estación de trabajo (219.17.100.X) conectada al Router LAB-B	Router LAB-E Interfaz E0 (210.93.105.2) o estación de trabajo (210.93.105.X)		
	2	Estación de trabajo (219.17.100.X) conectada al Router LAB-B	Router LAB-C Interfaz E0 (223.8.151.1)		
	3	Estación de trabajo (219.17.100.X) conectada al Router LAB-B	Estación de trabajo (223.8.151.2) conectada al router LAB-C		

Práctica de laboratorio 6.8.1.1 ACL extendidas - Descripción general

Duración estimada: 60 min.

Objetivos:

Esta práctica de laboratorio sirve para practicar las siguientes tareas:

- Repasar las características y capacidades de las listas de control de acceso IP extendidas (ACL)
- Desarrollar una ACL IP extendida para permitir o denegar tráfico específico
- Aplicar una ACL IP extendida a una interfaz de router
- Probar la ACL para determinar si se lograron los resultados deseados

Información básica:

Las ACL extendidas son una forma más avanzada de control con mayor flexibilidad en la forma en que se controlan los paquetes. Las ACL extendidas pueden filtrar (permitir o denegar) paquetes según su dirección origen o destino y el tipo de tráfico (por ej., FTP, Telnet, http, etc.). Como las ACL extendidas pueden bloquear el tráfico según la dirección destino, se pueden ubicar cerca del origen, lo que ayuda a reducir el tráfico de red.

En esta práctica de laboratorio se trabaja con las ACL extendidas para regular el tráfico que se permite que pase a través del router, según el origen y el tipo de tráfico. Las ACL son una herramienta importante para controlar qué paquetes, y qué tipo de paquetes pueden pasar a través de un router desde una red a otra.

Existen diferentes tipos de ACL para diferentes protocolos enrutados como IP, Novell IPX y AppleTalk. En esta práctica de laboratorio, se trabaja sólo con ACL IP extendidas, creadas con un número del 100 al 199.

Estos son los pasos necesarios para usar las ACL de forma efectiva:

- 1. Determinar los requisitos de la ACL (según las necesidades de seguridad de la empresa, etc.)
- 2. Desarrollar la ACL.
- 3. Verificar las sentencias en la ACL
- 4. Aplicar la ACL a una interfaz de router.
- 5. Verificar que la ACL se aplique correctamente a la interfaz que se desea.
- 6. Verificar que la ACL funcione correctamente

Herramientas / Preparación:

Antes de comenzar esta práctica de laboratorio, el profesor o el ayudante de laboratorio debe haber configurado el laboratorio estándar de 5 routers. Se trabaja individualmente o en equipos. Antes de comenzar con esta práctica de laboratorio, puede resultarle útil repasar el capítulo 6 (ACL) de la Guía del segundo año de la Academia de Networking de Cisco. También conviene repasar el capítulo 6 en línea del Semestre 3. Se requiere el siguiente equipo:

- Configuración de laboratorio estándar de 5 routers de Cisco, con hubs y switches
 - Estación de trabajo conectada al puerto de consola del router mediante un cable rollover

Recursos de sitio Web:

LAN Switching basics General information on all Cisco products - (Ir al capítulo 22 - Switches) 1900 / 2820 series Ethernet switches 2900 series Fast Ethernet switches Terms and acronyms IP routing protocol IOS command summary Access Control Lists - Overview and Guidelines Notas:

En esta práctica de laboratorio se desarrollará, aplicará y probará una ACL IP extendida utilizando la siguiente configuración de laboratorio. Puede hacer el Ejercicio A o el Ejercicio B que se describen en el Paso 1 que aparece a continuación.

Paso 1 - Determinar los requisitos de ACL.

¿Cuál es tráfico (paquetes) que se bloquea (deniega) o se permite? Como usará una ACL IP extendida, se puede controlar no sólo la dirección origen, sino también la dirección destino. También se pueden seleccionar los protocolos específicos en el conjunto de protocolos IP que se desea permitir o evitar que accedan a la red destino (por ej., TCP. UDP, ICMP, HTTP, Telnet etc.).

Ejercicio A: Evitar que el tráfico **Telnet** desde un host específico 192.5.5.2 (una estación de trabajo conectada al router LAB-A) alcance una red completa 210.93.105.0 (la red ubicada entre los Routers LAB-D y LAB-E)

Ejercicio B: Evitar que el tráfico de **Telnet** desde un host específico 210.93.105.2 (una estación de trabajo conectada al router LAB-E) alcance la red completa 192.5.5.0 (desde el router LAB-A).

Paso 2 - Desarrollar la ACL.

Definir las sentencias ACL en el modo Router (config)#. Las sentencias ACL son aditivas. Cada sentencia se agrega a la ACL. Si hay más de una sentencia en la ACL (lo que es típico) y se desea cambiar una sentencia anterior, se debe borrar la ACL y comenzar de nuevo. En estos ejemplos se bloquean paquetes sólo desde una dirección IP de host o una red según la red destino y el protocolo IP de nivel superior (por ej., telnet) que se utiliza. El formato o sintaxis de las sentencias de la ACL IP extendida aparece a continuación:

access-list list# {permit/deny} [protocol] source IP wildcard mask [port] dest. IP wildcard mask [port] [established] [log] [other options]

(Nota: Se puede usar cualquier número entre 100 y 199 para una ACL IP extendida)

Complete el comando ACL con las direcciones origen y destino correctas para lograr los requisitos del Ejercicio A o B (o ambos). Para las listas de acceso extendidas, también se debe especificar el protocolo (IP, TCP, UDP, ICMP). Como se está filtrando telnet, que usa TCP, recuerde incluir TCP en el comando.

Ejercicio A (ACL 101) access-list 101 deny

Ejercicio B (ACL 102) access-list 102 deny _____ ____ 1. ¿Por qué la máscara wildcard origen se determina como 0.0.0.0?

2. ¿Por qué la máscara wildcard destino se determina como 0.0.0.255?

3. ¿Qué se verifica con "eq telnet"?

4. ¿Qué significa si se omite eq telnet?

5. Como las ACL siempre terminan con un "deny any" implícito, si se utilizan una de las sentencias anteriores esto haría que esta lista denegara una sola dirección origen, pero también denegaría implícitamente cualquier otra dirección origen. Nuestro objetivo es sólo denegar el acceso a un solo host, de manera que es necesario agregar una segunda sentencia para permitir todo el tráfico restante. Introduzca la segunda sentencia de ACL que permite todo el tráfico restante (la misma sentencia se debe utilizar para el Ejercicio A o B):

Paso 3 - Verificar las sentencias en la ACL.

Utilice el siguiente comando para comprobar sus sentencias y verificar que todo se haya escrito correctamente. Si desea corregir un error o hacer un cambio en una sentencia existente se debe eliminar la ACL y comenzar de nuevo. Para eliminar la ACL, repita la parte access-list # del comando, con la palabra NO adelante.

Router#show access-list 101

1. ¿Cuántas sentencias hay en la ACL?

Paso 4 - Aplicar la ACL a una interfaz de router.

Como ahora se utilizan ACL extendidas y se pueden filtrar la dirección origen y destino, se puede aplicar el filtro lo más cerca posible del origen, lo que ahorra ancho de banda. También se debe recordar que se puede decidir aplicar la ACL a los paquetes entrantes o salientes. A menos que se especifique IN (entrante), la ACL se aplica sólo a los paquetes OUT (salientes) (IN y OUT siempre se consideran desde fuera del router). ¿A qué router y a qué interfaz se puede aplicar la ACL para cada uno de los ejercicios de ejemplo, A o B? Consulte el diagrama de laboratorio extendido y responda las siguientes preguntas.

Ejercicio A.

1. ¿En qué router, LAB-B o LAB-D, aplicaría el filtro que evitaría que los paquetes de telnet de LAB-A se transmitan a la LAN D/E (red 210.93.105.0)?

^{2. ¿}En qué interfaz se puede aplicar esta lista?

3. Complete los comandos que aplicarían esta lista a esa interfaz:

Router(config)# _____ Router(config-if)# _____

Ejercicio B.

1. ¿En qué router, lab-b o lab-d, aplicaría el filtro que evitaría que los paquetes del router LAB-E se transmitan a la LAN A (red 201.100.11.0)?

2. ¿En qué interfaz se puede aplicar esta lista?

3. Complete los comandos que aplicarían esta lista a esa interfaz:

Router(config)#_____ Router(config-if)#_____

Paso 5 - Verificar si la ACL se aplica a la interfaz correcta:

Use el siguiente comando para verificar si la ACL se aplica a la interfaz correcta en el router correcto:

Router#show running-config

```
1. ¿Cuáles fueron los resultados que demuestran que la ACL se ha aplicado correctamente?
```

NOTA: Para eliminar una ACL de una interfaz, se debe configurar en primer lugar la interfaz como en el Paso 4 y luego repetir el segundo comando con la palabra NO adelante (no ip access-group 101 in).

Paso 6 - Verificar que la ACL funcione correctamente

Pruebe la ACL intentando enviar paquetes desde la red origen que se debe permitir o denegar. Emita varios comandos ping para probar estas ACL. Se indican varias pruebas para cada ejercicio.

Ejercici	ο	Prueba	n⁰	Telnet desde		Α	¿Debe tener éxito?	¿Lo tuvo?
A	1		Estación de trabajo (192.5.5.2) conectada al router Lab-A		Estación de trabajo (210.93.105.2) conectada al router Lan-E			
	2			Estación de trabajo (192.5.5.2) conectada al router Lab-A		Estación de trabajo (223.8.151.2) conectada al router Lab-C		
Ejercic io	Pru	eba n⁰	Telne	t desde	Α		¿Debe tener éxito?	¿Lo tuvo?
В	B 1 Estac 3 1 (210. conec Lab-E		Estac (210.9 conec Lab-E	ión de trabajo 93.105.2) tada al router	Estac (192.ť router	ión de trabajo 5.5.2) conectada al [.] Lab-A		
2 Estac (210. conec Lab-E		ión de trabajo 93.105.2) tada al router	rabajo Estación de trabajo 2) (219.17.100.2) router conectada al router Lab- B					

Use el siguiente comando con uno de los routers en el que se aplicó la ACL para verificar que los paquetes se bloqueen:

Router#show access-list 101

1. ¿Cuál fue el resultado del comando? ¿Cómo puede comprobar si la ACL funciona?

Práctica de laboratorio 6.8.1.2 ACL extendidas de Internet- Descripción general

Duración estimada: 90 min.

Objetivos:

Esta práctica de laboratorio sirve para practicar las siguientes tareas:

- Diseñar y planificar una ACL, según requisitos de seguridad específicos
- Trabajar con las capacidades más avanzadas de las listas de control de acceso IP extendidas (ACL)
 - Desarrollar una ACL extendida con múltiples sentencias
- Desarrollar una ACL extendida para controlar el tráfico de Internet utilizando uno o más routers

 Desarrollar una ACL IP extendida para permitir o denegar otro tráfico específico del protocolo IP

Información básica:

Esta práctica de laboratorio es un ejercicio de práctica que simula una situación de la realidad. Se trabaja con múltiples Listas de control de acceso extendidas (ACL) para simular la regulación del tráfico al que se permite pasar a través de múltiples routers a varios servidores e Internet. Este es primariamente un ejercicio por escrito para practicar el análisis de los requisitos de seguridad y diseñar un plan de ACL. Se pueden configurar la mayoría de las ACL en los routers indicados en la sección de respuestas, pero no se pueden probar en realidad algunas de las capacidades de filtrado de las ACL en algunos casos.

Las ACL extendidas proporcionan una forma más avanzada de filtrado con mayor flexibilidad en la forma en que se controlan los paquetes. Las ACL extendidas pueden filtrar (permitir o denegar) paquetes según su dirección origen o destino y el tipo de tráfico (por ej., FTP, Telnet, HTTP etc.). Como las ACL extendidas pueden bloquear según la dirección destino, se pueden ubicar cerca del origen, lo que ayuda a reducir el tráfico de red.

En esta práctica de laboratorio se trabaja con múltiples Listas de control de acceso extendidas (ACL) para regular el tráfico que puede pasar a través de múltiples routers, según el origen, destino y tipo de tráfico.

Estos son los pasos necesarios para usar las ACL de forma efectiva:

- 1. Determinar los requisitos de la ACL (según las necesidades de seguridad de la empresa, etc.)
- 2. Desarrollar la ACL.
- 3. Verificar las sentencias en la ACL
- 4. Aplicar la ACL a una interfaz de router.
- 5. Verificar que la ACL se aplique correctamente a la interfaz que se desea.
- 6. Verificar que la ACL funcione correctamente

Herramientas / Preparación:

Esta es principalmente una práctica por escrito pero es aconsejable tener acceso al laboratorio de 5 routers. Debe disponerse de una pizarra para anotar las ideas sobre diferentes formas de proporcionar la seguridad deseada. Se trabaja en equipos de 2 o 3 personas. Antes de comenzar con esta práctica de laboratorio, puede resultarle útil repasar el capítulo 6 (ACL) de la Guía del segundo año de la Academia de Networking de Cisco. También conviene repasar el capítulo 6 en línea del Semestre 3. Se requiere el siguiente equipo:

- Configuración de laboratorio estándar de 5 routers de Cisco, con hubs y switches
 Estación de trabajo conectada al puerto de consola del router mediante un cable
- rollover

Recursos de sitio Web:

LAN Switching basics General information on all Cisco products - (Ir al capítulo 22 - Switches) 1900 / 2820 series Ethernet switches 2900 series Fast Ethernet switches Terms and acronyms IP routing protocol IOS command summary Access Control Lists - Overview and Guidelines

Notas:

	_
	_

En esta práctica de laboratorio se diseña un plan de seguridad que utiliza múltiples ACL extendidas y determinará dónde se deben aplicar sobre la base de la siguiente configuración de laboratorio estándar. Puede haber más de una respuesta correcta.

Se comienza con la configuración estándar de laboratorio que aparece en la descripción general y entonces se dibuja un diagrama detallado de todos los routers, servidores y redes para ayudar a obtener los requisitos. Use el espacio suministrado en la página siguiente para diagramar los requisitos enumerados a continuación y a ayudar a determinar cuáles son las ACL que se necesitan y dónde deben ubicarse.

Paso 1 - Definir los requisitos de la ACL.

A continuación se suministran los requisitos y algunos supuestos para esta práctica de laboratorio. En general es mejor intentar usar la menor cantidad posible de listas de acceso y tener en cuenta el potencial de crecimiento de la red. En este ejercicio se usan ACL extendidas.

Supongamos que sus servidores empresariales se ubican en la red 219.17.100.0 (desde LAB-B).

- 1. Se debe permitir acceso a través de la Web (protocolo http) a su servidor web 219.17.100.80 para cualquier persona
- 2. Se debe permitir el acceso a través de DNS a su servidor DNS 219.17.100.53
- 3. Se debe permitir que el personal docente tenga pleno acceso desde la red 223.8.151.0 a cualquiera de estos servidores.
- 4. No se debe permitir otro acceso a ningún servidor en la red 219.17.100.0

Suponga que todos los estudiantes se encuentran en la red 210.93.105.0, y se desea controlar el acceso hacia o desde esa red. Supongamos que el router Lab-A le pertenece a su ISP y no tiene control sobre él.

- 1. NO se debe permitir que los estudiantes usen FTP a Internet (¡posibles problemas de virus!)
- Se debe permitir que los estudiantes tengan cualquier otro tipo de acceso a Internet
 Se debe permitir que los estudiantes tengan acceso a la red del cuerpo docente
- 223.8.151.0 para pasar mensajes de correo electrónico (SMTP)
- 4. Se debe denegar a los estudiantes cualquier otro tipo de acceso a la red del cuerpo docente 223.8.151.0

Paso 2 - Desarrollar una o más ACL.

Agrupe las sentencias según sus características comunes y la ubicación donde usted considera que se debe aplicar la ACL. Intente crear la menor cantidad posible de ACL y mantener la flexibilidad. El formato o sintaxis de las sentencias de la ACL IP extendida que se utilizan aparece a continuación:

access-list list# {permit/deny} [protocol] source IP wildcard mask [port] dest. IP wildcard mask [port] [established] [log] [other options]

(Nota: Se puede usar cualquier número entre 100 y 199 para una ACL IP extendida)

Paso 3 - Aplicar y verificar las ACL con los routers del laboratorio (si están disponibles).

Si tiene acceso a los routers en el laboratorio puede aplicar y verificar las ACL que ha creado. Puede que no sea posible probar todas las capacidades de filtrado de las ACL, ya que no dispondrá de un servidor HTTP o DNS o acceso a Internet, pero se puede probar la mayor parte del filtrado. Recuerde que sólo se puede aplicar una ACL por protocolo (como IP) por dirección (entrante o saliente (IN or OUT)).

Diagrame los routers y servidores e indique la ubicación de las ACL (router e interface, entrante o saliente) según los requisitos de seguridad.

Actividad de laboratorio interactiva (Flash, 514 kB)

Antes de realizar la actividad de laboratorio propiamente dicha, le recomendamos que lleve a cabo esta actividad preparatoria para probar su conocimiento de la sintaxis de comando de las Listas de control de acceso estándar (ACL).

Actividad de sintaxis interactiva (Flash, 135 kB)

Utilice esta actividad para poner a prueba su conocimiento de la sintaxis de los parámetros de las Listas de control de acceso (ACL) extendidas.

Práctica de laboratorio 7.4.3 Enrutamiento IPX - Descripción general

Duración estimada: 90 min.

Objetivos:

Esta práctica de laboratorio sirve para practicar las siguientes tareas:

- Familiarizarse con el protocolo NetWare IPX de Novell y su uso en las internetworks.
 - Configurar los routers de laboratorio para enrutar el protocolo Novell IPX y el protocolo IP
 - Suministrar soporte para los clientes y servidores NetWare que ejecutan IPX

Información básica:

En las prácticas de laboratorio anteriores ha estado trabajando con el protocolo enrutado TCP/IP o el Protocolo Internet (IP). En esta práctica de laboratorio trabajará con el protocolo enrutado de Intercambio de paquetes de internetworking (IPX) de Novell. Los protocolos de capa 3 del modelo OSI, como IP e IPX, contienen información en sus paquetes que indica la red de proveniencia del paquete y a qué red se enviará. Los protocolos enrutables (como IP e IPX) son aquellos que pueden permitir que los paquetes se enruten entre redes y que les permiten que se dirijan desde una ubicación hacia otra. Los routers pueden ejecutar múltiples protocolos de enrutamiento (por ej., RIP e IGRP) y enrutados (IP e IPX). Para poder enrutar tanto IP como IPX, el router debe mantener múltiples tablas de enrutamiento, una para cada tipo de protocolo enrutado que se reconoce.

Implementación de Novell IPX/SPX

IPX es un protocolo enrutado propietario y desarrollado por Novell Inc. para ser utilizado con el Sistema operativo de red NetWare. Se utiliza ampliamente con redes de área amplia y local privadas que tienen servidores NetWare de Novell. Las versiones anteriores de NetWare (3x y la mayoría de las versiones 4.x) utilizan IPX como su protocolo principal. Para brindar soporte a estos servidores, es necesario ejecutar el protocolo IPX en los routers, los servidores y las estaciones de trabajo. Las versiones más recientes, tales como NetWare 5.0, pueden ejecutar IP de forma nativa. Es posible tener una red Novell de múltiples routers que utilice sólo el protocolo IPX, pero para acceder a Internet todavía se requiere el protocolo IP. IPX no admite subredes y no se puede enrutar a través de Internet

El sistema operativo de red de Novell utiliza dos protocolos principales, IPX y SPX, para ayudar a asegurar el envío de paquetes. IPX tiene la responsabilidad del enrutamiento a nivel de capa 3 para que los paquetes lleguen desde una red a otra. El Intercambio secuencial de paquetes o SPX es un protocolo de envío de paquetes orientado a conexión similar a TCP. Una dirección IP está formada por 2 partes; una porción de red y una porción de host. La porción de red de una dirección IPX es un número hexadecimal de 32 bits y la porción de host es la dirección MAC de 48 bits de la NIC (para el servidor, la estación de trabajo, etc.). Como la dirección de host o de nodo es su dirección MAC, no es necesario asignar una dirección de host como sucede en el caso de IP. No se requiere ARP porque se conoce la dirección MAC.

Herramientas / Preparación:

Antes de comenzar esta práctica de laboratorio, el profesor o el ayudante de laboratorio debe haber configurado el laboratorio estándar de 5 routers. Antes de comenzar con esta práctica de laboratorio, puede resultarle útil repasar el capítulo 7 (Novell IPX) de la Guía del segundo año de la Academia de Networking de Cisco. También conviene repasar el capítulo 7 en línea del Semestre 3. Se requiere el siguiente equipo:

- Configuración de laboratorio estándar de 5 routers de Cisco, con hubs y switches
 - Estación de trabajo conectada al puerto de consola del router
 - Cable de consola (roll-over)

Recursos de sitio Web:

•

Routing basics General information on routers 2500 series routers 1600 series routers Terms and acronyms Routing Novell IPX Troubleshooting Novell IPX Novell IPX Commands

Los siguientes comandos IOS relacionados con IPX servirán de ayuda para la información y el diagnóstico de fallas de la conectividad IPX.

Comandos de conectividad / diagnóstico de fallas de IPX

Show ipx interface	Muestra el estado de las interfaces IPX y de los parámetros (tipo de trama) configurados de IPX en cada interfaz
Show ipx route	Muestra el contenido de la tabla de enrutamiento IPX con las redes IPX conocidas
Show ipx servers	Enumera los servidores Novell que ejecutan IPX que se detectan a través de las publicaciones SAP
Show ipx traffic	Muestra la información del tráfico IPX incluyendo el número y el tipo de paquetes IPX transmitidos y recibidos por el router
Debug ipx routing activity	Muestra información dinámica acerca de los paquetes de actualización de enrutamiento IPX que se transmiten y se reciben (cada 60 segundos).
Debug ipx sap	Muestra la dinámica acerca de los paquetes del Protocolo de publicación de servicio (SAP) IPX que se transmiten o se reciben
Ping	Utilice la versión extendida (ping, luego presione intro) para especificar una dirección de nodo IPX.

Paso 1 - Determinar la cantidad de redes que se necesitan.

¿Cuántas redes IPX se necesitan (redes LAN y WAN) para nuestro laboratorio de 5 routers?

(Consulte el diagrama estándar de 5 routers. ¿Cuántas redes IP hay?)

Paso 2 - Repasar el direccionamiento IPX correspondiente

Repase la estructura del esquema de direccionamiento IPX y conteste las siguientes preguntas:

1) ¿6F es un número de red IPX válido?

¿Por qué? (o por qué no)

(ayuda: ¿los números de red IPX se representan en números decimales o en hexadecimales?)

2) ¿1a2b3c4d5e es un número de red IPX válido?

¿Por qué? (o por qué no)

(ayuda: ¿qué longitud tienen los números de red IPX? ¿Cuántos bits? ¿Cuántos dígitos hexadecimales representa esto?)

Paso 3 - Habilitar el enrutamiento IPX

Utilice el siguiente comando para habilitar el enrutamiento IPX para cada router. Esto habilita RIP y SAP IPX. Luego de habilitar IPX en el router y mientras aún se encuentra en el modo de configuración IPX, vaya al paso 4 y seleccione las interfaces que enrutan IPX y asígneles los números de red.

Router(config)# ipx routing

Paso 4 - Crear números de red IPX:

Utilice el diagrama estándar de 5 routers como guía para crear números de red exclusivos para cada "cable" o red. Complete la tabla que aparece a continuación con el número de modelo de cada router y las direcciones de red IPX que debe utilizar. No todos los routers deben utilizar o utilizan todas las interfaces descritas. Recuerde que las interfaces seriales entre dos routers comparten el mismo número de red. Los números de red IPX hexadecimales pueden estar formados por números del 0 al 9 y letras de la A a la F y pueden variar desde 1 a FFFFFFF.

Nombre del	Número de	Ethernet 0	Ethernet 1	Serial 0	Serial 1
router	modelo	Red IPX	Red IPX	Direccion IPX	Direction IPX
Lab-A					
Lab-B					
Lab-C					
Lab-D					
Lab-E					

Paso 5 - Asignar números de red IPX a interfaces

En cada una de las interfaces en cada router, configure el número de red IPX a partir de la tabla que se suministró anteriormente:

Router(config)# interface E0 (Selecciona la interfaz Ethernet E0) Router(config-if)# ipx network A2C (A2C = número de red IPX único)

Paso 6 - Determinar si hay rutas redundantes.

1) ¿Hay alguna ruta redundante en nuestro laboratorio? Es decir, ¿hay dos o más formas en las que los paquetes pueden dirigirse desde un lugar hacia otro?

2) En el caso de que haya rutas redundantes (2) y desea compartir la carga de tráfico IPX entre esas 2 rutas posibles, es necesario informarle al router que acepte múltiples rutas. Complete los comandos que debe utilizar:

Router(config)# ipx

Paso 7 - Verificar las tablas de enrutamiento.

Dado que RIP IPX se habilita automáticamente cuando se habilita el enrutamiento IPX, ahora puede controlar cada una de las tablas de enrutamiento del router para verificar que todos los routers han aprendido todas las redes IPX:

Router# show ipx route

Paso 8 - Hacer telnet a un router vecino.

Haga telnet a otro router y emita un comando show running-config para saber cuál es la interfaz que está en uso. Utilice el siguiente comando para encontrar la dirección IPX de una de las interfaces Ethernet.

Router# show ipx interface e0

1) ¿Cuál fue la dirección IPX de la interfaz?

2) ¿Cuál de las porciones corresponde a la dirección de red?

3) ¿Cuál de las porciones corresponde a la dirección MAC de la interfaz?

Paso 9 - Hacer ping a la interfaz del router vecino

Vuelva al router en el que se encontraba y emita el comando ping, recordando que debe colocar un punto entre el número de red y la dirección MAC, y luego de cada 4 dígitos de la dirección MAC. Introduzca aquí un comando ping IPX de ejemplo.

Router# ping ipx

Paso 10 - Reflexión:

En el diario, escriba acerca de las diferencias entre las tablas de enrutamiento IPX e IP.