# DISEÑO Y MONTAJE DE LAS PRÁCTICAS DE CONFIGURACIÓN DEL ROUTER Y ACL PARA EL LABORATORIO DE REDES DE LA CUTB

**ZAIDY LUCÍA SEQUEDA ANGARITA**

**WILLIAM ANTONIO ARTEAGA PICO**

**CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR**

**CENTRO DE EDUCACIÓN PERMANENTE**

**MINOR EN COMUNICACIONES Y REDES PARA COMPUTADORES**

**CARTAGENA DE INDIAS**

**2003**

# DISEÑO Y MONTAJE DE LAS PRÁCTICAS DE CONFIGURACIÓN DEL ROUTER Y ACL PARA EL LABORATORIO DE REDES DE LA CUTB

**ZAIDY LUCÍA SEQUEDA ANGARITA**

**WILLIAM ANTONIO ARTEAGA PICO**

**Monografía presentada como**
**requisito para optar al título de**
**Ingeniero Electrónico e Ingeniero Electricista**

**Asesor:**

**ISAAC ZÚÑIGA SILGADO**

**Ingeniero de Sistemas**

**CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR**

**CENTRO DE EDUCACIÓN PERMANENTE**

**MINOR EN COMUNICACIONES Y REDES PARA COMPUTADORES**

**CARTAGENA**

**2003**

**Nota de aceptación**

_____

_____

_____

_____

_____

_____

**Firma del Presidente del jurado**

_____

**Firma del jurado**

_____

**Firma del jurado**

**Cartagena, Junio 17 de 2003**

**CONTENIDO**

## LISTA DE FIGURAS

Pág.

## LISTA DE ANEXOS

## RESUMEN

El mundo tecnológico ha avanzado vertiginosamente a través de la implementación de redes en las diferentes organizaciones y estableciendo conexión entre ellas para llegar a constituir una gran red a nivel mundial que se compone de elementos cada vez más pequeños y que requieren de un estudio detallado.

La base de las redes la constituye el modelo OSI y su protocolo paralelo TCP/IP. Por medio de ellos, es posible entender cómo se realiza la comunicación entre dos computadores y cómo se van conformando las redes empezando por una red de área local (LAN). Todo esto incluye unos estándares de trabajo, como también el establecimiento de protocolos que hacen posible el envío y recepción de la información que se transmite por la red desde una estación origen hasta una estación destino. También incluyen los dispositivos de manejo en las redes LAN, tipos de servicios, direccionamiento MAC e IP, manejo de subredes y encapsulamiento de los datos a transmitir. Lo anterior se explica en el capítulo 1.

Luego de conocer las características más importantes de las redes LAN, es posible comprender el establecimiento de redes más complejas; es el caso de las redes de área amplia (WAN). En el capítulo dos se explican las características más importantes de estas redes haciendo referencia especial al dispositivo que

logra la conexión y comunicación entre redes que se encuentran a gran distancia: el router. De este elemento se estudian sus componentes internos, sus modos de configuración y la labor que desarrolla en el proceso de enrutamiento incluyendo la descripción de los protocolos de enrutamiento y la configuración de los mismos en el router.

En el capítulo tres se menciona otra característica del router que tiene que ver con el establecimiento de un mecanismo de seguridad que complementa al resto de medidas que se hayan tomado para proteger la información. Es el caso de las listas de control de acceso (ACL), las cuales permiten o rechazan el acceso a la información. Este procedimiento se compone de distintas configuraciones que dependen del modo como se decida proteger la información.

En el capítulo cuatro, se mencionan algunas formas de probar el funcionamiento de una red a través de diferentes comandos como Telnet, ping y trace. También se hace referencia al uso de comandos para guardar la información en otra fuente y la labor de recuperación de dicha información a través de los comandos designados para ello. Finalmente, se mencionan el proceso de recuperación de contraseña del router y los diferentes fallas que pueden presentarse en el manejo de las redes, en general.

El capítulo 5 trata de manera más extendida algunas de las tecnologías de redes de área amplia (WAN) que funcionan en la capa de enlace de datos del modelo OSI: tecnologías PPP, X.25, Frame Relay y ATM. El protocolo PPP funciona punto a punto, conectando un dispositivo con otro con una encapsulación y direccionamiento mínimo. Los protocolos X.25, Frame Relay y ATM no funcionan en un entorno estricto de enlaces serie punto a punto, sino que utilizan circuitos virtuales para trasladar lo datos.

Para cada uno de los capítulos se han implementado una serie de prácticas de laboratorio que complementan los conceptos mencionados. El montaje y desarrollo de los mismos se explica en los anexos del trabajo.

# INTRODUCCIÓN

El mundo de las redes ha revolucionado las comunicaciones y ha permitido que lugares remotos puedan mantenerse en contacto para diversos fines, tanto comerciales como de investigación y entretenimiento. Sin embargo, detrás de estas tecnologías existe un gran compendio teórico que debe estudiarse para el mayor entendimiento de las redes y de sus múltiples aplicaciones y beneficios.

Dentro de este gran contenido teórico resalta la importancia de los dispositivos que hacen posible la comunicación dentro de un pequeño espacio geográfico hasta cubrir los lugares más remotos. Es el caso de los *routers*, los cuales realizan operaciones internas para llevar la información de una red a otra.

Estas operaciones tienen como objetivo preparar al *router* para la labor por la cual fueron creados: el enrutamiento de paquetes de una red a otra. Por ello, es necesario conocer los elementos que lo componen, el proceso de configuración inicial y de establecimiento de protocolos de enrutamiento, como también la labor de seguridad que se puede desempeñar a partir de ellos.

Es por esto, que se ha decidido llevar a cabo la conformación de prácticas de laboratorio referentes al tema del *router* que cubren los temas anteriormente

mencionados con el fin de familiarizar al estudiante que se interesa por el tema de las redes con los aspectos más importantes que tienen que ver con el establecimiento de redes a nivel local y de mayor cobertura, como el caso de las redes WAN, a partir del conocimiento de los procesos que se pueden llevar a cabo en el *router* como preparación a la labor de enrutamiento y seguridad.

# 1. FUNDAMENTOS DE REDES

## 1.1 GENERALIDADES

Desde un inicio, los computadores eran considerados elementos aislados, donde cada uno operaba como una estación de trabajo independiente. Esto trajo como consecuencia continuos desplazamientos del usuario y dificultad al implementar una administración conjunta de todos los equipos.

Debido a esto y al vertiginoso crecimiento de las organizaciones fue necesario unir a los equipos entre si para compartir archivos y periféricos entre los diferentes computadores. De esta manera surgió el concepto de “redes de computadores” . Sin embargo, cada institución le entregó la implementación de sus redes a empresas diferentes, cada una de ellas con unos modelos de red que usaban protocolos y arquitecturas diferentes. Esto dificultó la posibilidad de lograr un puente entre las distintas empresas que permitiera compartir cierta información y en general, cualquier tipo de comunicación.

Fue así que se llegó a la conclusión de que se debían unir las redes entre si a través de una arquitectura de red con un modelo común que hiciese posible dicha interconexión. Por ello, la Organización Internacional para la Normalización (ISO)

realizó varias investigaciones acerca de los esquemas de red y elaboró el modelo de referencia OSI en 1984.

El modelo OSI *(Open System Interconection)* proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red utilizados por las empresas a nivel mundial. Este modelo teórico de arquitectura de red es independiente de los protocolos usados y constituye la base de estudio para el diseño y manejo del tema de las redes.

## 1.2 EL MODELO OSI

### 1.2.1 Modelo de red: Estructura en capas

El proceso de intercomunicación entre dos computadores es complejo ya que son muchos los elementos que intervienen en el esquema de intercambio de datos entre equipos diferentes. Para facilitar esto, la ISO dividió el modelo de referencia OSI en capas, donde cada capa realiza una función específica con el fin de asegurar que los paquetes de datos puedan viajar en la red desde el origen hasta el destino. Un paquete de datos es una unidad de información, lógicamente agrupada, que se desplaza entre los sistemas de computación. Para que los paquetes de datos puedan viajar desde el origen hasta su destino a través de una

red, es importante establecer un lenguaje común (o protocolo) entre los diferentes dispositivos de la red. Esto permite que un proceso que se ejecuta en un computador, pueda comunicarse con un proceso similar en otro si tienen implementados los mismos protocolos de comunicaciones de capas OSI. La división de la red en siete capas presenta las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas que permitan un aprendizaje más simple.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Logra que los distintos tipos de hardware y software de red comunicarse entre sí de una forma totalmente definida.
- Impide que los cambios en una capa puedan afectar las demás capas, de manera que se puedan desarrollar con más rapidez.

### 1.2.2 Funciones de las capas del modelo OSI

#### 1.2.2.1 Capa 7: La capa de aplicación

Es la capa más cercana al usuario, y está relacionada con las funciones de más alto nivel que proporcionan soporte a las aplicaciones o actividades del sistema, suministrando servicios de red a las aplicaciones del usuario y definiendo los

protocolos usados por las aplicaciones individuales (ver figura1). En esta capa se establece la disponibilidad de los diversos elementos que deben participar en la comunicación, sincroniza las aplicaciones que cooperan entre sí y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos. Algunos ejemplos de procesos de aplicación son: programas de hojas de cálculo, programas de procesamiento de texto, transferencia de archivos (ftp), *login* remoto (rlogin, telnet), correo electrónico (*mail* - smtp), páginas web (http).

#### 1.2.2.2 Capa 6: La capa de presentación

Esta capa proporciona sus servicios a la capa de aplicación, garantizando que la información que envía la capa de aplicación de un sistema pueda ser entendida y utilizada por la capa de aplicación de otro (figura 1). También se encarga del establecimiento y terminación de la conexión de sesión cuando existan varias alternativas disponibles. Las operaciones de esta capa son:

- Traducir entre varios formatos de datos utilizando un formato común, estableciendo la sintaxis y la semántica de la información transmitida.
- Definir la estructura de los datos a transmitir.
- Dar formato a la información para visualizarla o imprimirla.
- Comprimir los datos si es necesario y aplicarles procesos criptográficos.

#### 1.2.2.3 Capa 5: La capa de sesión

Esta capa brinda sus servicios a la capa de presentación, proporcionando el medio necesario para que las entidades de presentación organicen y sincronicen su diálogo y procedan al intercambio de datos (ver figura 1). Las principales funciones son:

- Establecer, administrar y finalizar las sesiones entre dos *hosts* que se están comunicando.
- Restaurar la sesión a partir de un punto seguro y sin perdida de datos si esta llegara a fallar por motivos ajenos al usuario o, de no ser posible esto, terminar la sesión de forma ordenada revisando y recuperando todas sus funciones.
- Sincronizar el diálogo entre las capas de presentación de dos *hosts* que se estén comunicando.
- Ofrecer disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.

#### 1.2.2.4 Capa 4: La capa de transporte

Brinda su apoyo a la capa de sesión, efectuando la transferencia de datos entre dos entidades de sesión. También suministra un servicio de transporte de datos

que se encarga de asuntos como la implementación del transporte y el cuidado en lograr una transferencia de datos segura y económica (ver figura 1). Las principales funciones de esta capa son:

- Controlar la interacción entre procesos usuarios, proporcionar controles de integración entre usuarios de la red para prevenir pérdidas o doble procesamiento de transmisiones y realizar funciones de control y numeración de unidades de información, fragmentación y reensamblaje de mensajes.
- Controlar el flujo de transacciones y direccionamiento de máquinas a procesos de usuario y garantizar la transferencia de información a través de la subred.
- Asegurar que se reciban todos los datos y en el orden adecuado, realizando un control de extremo a extremo y aceptar los datos del nivel de sesión, fragmentándolos en segmentos.

#### 1.2.2.5 Capa 3: La capa de red

Esta capa proporciona sus servicios a la capa de transporte, brindando conectividad y selección de ruta entre dos sistemas de *hosts* que pueden estar ubicados en redes geográficamente distintas. También se ocupa de aspectos como la contabilidad de paquetes, conmutación y enrutamiento de la información para la selección de la ruta más adecuada (ver figura 1). Las funciones de la capa de red son:

- Dividir los mensajes de la capa de transporte en “paquetes” y ensamblarlos al final. También enviar los paquetes de nodo a nodo utilizando un circuito virtual o un datagrama.
- Conocer la topología de la subred y manejar el caso en que las fuente y el destino están en redes distintas. Esto lo logra enviando la información a través de la subred, mirando las direcciones del paquete para determinar los métodos de conmutación y enrutamiento que deben establecerse para que la información llegue al destino a través de los enrutadores intermedios (*routers*).
- Controlar la congestión de la subred.

#### 1.2.2.6 Capa 2: La capa de enlace de datos

Esta capa proporciona sus servicios a la capa de red, suministrando un tránsito de datos confiable a través de un enlace físico. Para ello, se ocupa del direccionamiento físico, la topología de red[*], el acceso a la red, la notificación de errores, formación y entrega ordenada de tramas y control de flujo (ver figura 1). Las principales funciones de esta capa son:

- Establecer los medios necesarios para una comunicación confiable y eficiente entre dos máquinas en red.

[*] CHOMICZ, Bob. Instalaciones de fibra óptica. Madrid: McGraw-Hill, 1998. Págs. 181-185

- Agregar una secuencia especial de bits al principio y al final del flujo inicial de bits de los paquetes, estructurando este flujo bajo un formato predefinido llamado trama.
- Sincronizar el envío de las tramas de manera confiable y libre de errores.
- Controlar la congestión de la red y regular la velocidad de tráfico de datos.
- Controlar el flujo de tramas mediante protocolos que prohiben que el remitente envíe tramas sin la autorización explícita del receptor, sincronizando así su emisión y recepción.
- Manejar los soportes físicos de la red: secuencia, enlace lógico y acceso al medio.

#### 1.2.2.7 Capa 1: La capa física

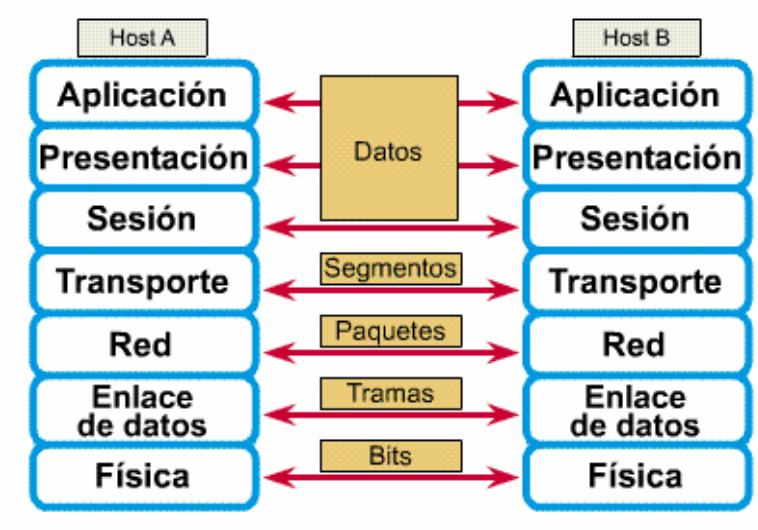
Esta capa se encarga de transmitir bits por un canal de comunicación, de manera que cuanto envíe el emisor llegue sin alteración al receptor (ver figura 1). En esta capa se definen las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales, relacionando la agrupación de circuitos físicos a través de los cuales los bits son movidos. Aquí se manejan características como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares.

**Figura 1. Funciones de las capas del Modelo OSI**


### 1.2.3 Comunicaciones de par a par

La comunicación par a par se refiere a que cada capa del modelo OSI en el origen debe comunicarse con su capa igual en el lugar destino para lograr que los paquetes viajen desde el origen hasta su destino. Las reglas y convenciones que controlan esta conversación se denominan protocolo de la capa n, y manejan el formato y significado de las unidades de datos intercambiadas. Durante este proceso, cada protocolo de capa intercambia información, que se conoce como unidades de datos de protocolo (PDU),entre capas iguales. Cada capa de comunicación, en el computador origen, se comunica con un PDU específico de capa y con su capa igual en el computador destino (Ver figura 2).

**Figura 2. Comunicación de par a par**




Los paquetes de datos de una red parten de un origen y se envían a un destino. Cada capa depende de la función de servicio de la capa OSI que se encuentra debajo de ella. Para lograr esto, la capa inferior utiliza el encapsulamiento para colocar la PDU de la capa superior en su campo de datos, luego le agrega un encabezado e información final que la capa necesite para ejecutar su función. Así, los datos se desplazan a través de las capas, recibiendo información adicional.

### 1.2.4 Tipos de Servicios

#### 1.2.4.1 Servicios orientados a la conexión

En ellos la conexión es un medio a través del cual se envía la información de forma continua, por lo que los mensajes llegan en el orden que fueron enviados y

sin errores. La comunicación en este caso es dúplex, y el control de flujo automático. Una analogía es el sistema telefónico.

#### 1.2.4.2 Servicios sin conexión

Aquí cada mensaje lleva la dirección completa de su destino, la información no se envía de forma continua y el enrutamiento de cada mensaje es independiente. Por ello, no es un servicio confiable ya que sólo lleva los bits. En este caso la capa de red ni garantiza el orden de los paquetes ni controla su flujo, y los paquetes deben llevar sus direcciones completas de destino. Una analogía sería el caso del sistema de correo convencional.

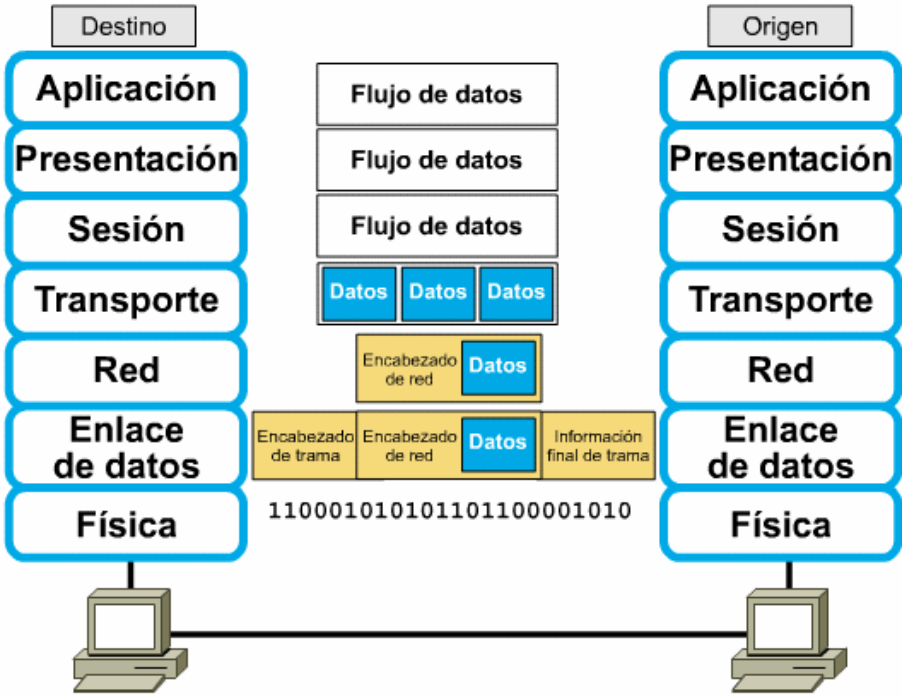
### 1.2.5 Encapsulamiento de datos

Para que un computador origen envíe datos a un computador destino, se deben colocar paquetes que se puedan administrar y rastrear a través de un proceso denominado encapsulamiento. Las tres capas superiores (aplicación, presentación y sesión) preparan los datos para su transmisión creando un formato común para la transmisión.

Una vez pasados a formato común, el encapsulamiento rodea los datos con la información de protocolo necesaria antes de que se una al tránsito de la red. Por lo tanto, a medida que los datos se desplazan a través de las capas del modelo

OSI, reciben encabezados. El encapsulamiento se efectúa en este orden (ver la figura 3):

**Figura 3. Encapsulamiento de Datos**




- En primer lugar, se crean los datos (capa de Presentación). Esto ocurre cuando el usuario envía un mensaje de correo electrónico. Los caracteres alfanuméricos se convierten en datos para que puedan recorrer la *internetwork*.
- Luego se empaquetan los datos para ser transportados de extremo a extremo (capa Transporte). Aquí se dividen los datos en segmentos y se les asignan números de secuencia para asegurarse de que los *hosts* receptores vuelvan a unir los datos en el orden correcto. Luego los empaqueta para ser

transportados por la *internetwork*. Después se agrega la dirección de red al encabezado (capa de Red). Aquí se encapsula el segmento creando un paquete o datagrama, agregándole una dirección de red destino y origen, por lo general IP. Con esto, los datos se colocan en un paquete que contiene el encabezado de red con las direcciones lógicas de origen y destino. Estas direcciones ayudan a los dispositivos de red a enviar los paquetes a través de la red por una ruta seleccionada.

- Luego se agrega la dirección local al encabezado de enlace de datos (capa Enlace de datos). Aquí continúa el encapsulamiento del paquete, con la creación de una trama. Le agrega a la trama la dirección local (MAC de la tarjeta de red, única para cada tarjeta) origen y destino. Luego, la capa de enlace de datos transmite los bits binarios de la trama a través de los medios de la capa física. La trama le permite conectarse al próximo dispositivo de red conectado directamente en el enlace. Cada dispositivo en la ruta de red seleccionada requiere el entramado para poder conectarse al siguiente dispositivo.
- Finalmente, se transmite el tren de bits creado. (Capa Física). Este tren se transmite a través de los medios físicos (cableado, etc.). Una función de temporización permite que los dispositivos distingan estos bits a medida que se trasladan por el medio.

## 1.3 REDES DE ÁREA LOCAL (LAN)

### 1.3.1 Dispositivos y tecnologías LAN

Las redes de área local* (LAN) se componen de computadores, tarjetas de interfaz de red, medios de *networking*, dispositivos de control del tráfico de red y dispositivos periféricos. A través de las LAN es posible que en una empresa se puedan compartir elementos como archivos e impresoras y mantener comunicación por medio de correo electrónico. Las características principales de las LAN son las siguientes:

- La red opera dentro de un área geográfica limitada (un edificio, por ejemplo).
- Las LAN se componen de múltiples dispositivos de escritorio conectados (normalmente PC) con acceso a medios de ancho de banda elevado.
- Una LAN conecta computadores y servicios a un medio común de Capa 1.

Los dispositivos LAN incluyen:

- **Puentes** que conectan los segmentos LAN y ayudan a filtrar el tráfico.

*

hhttp://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=10541632648683 31,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

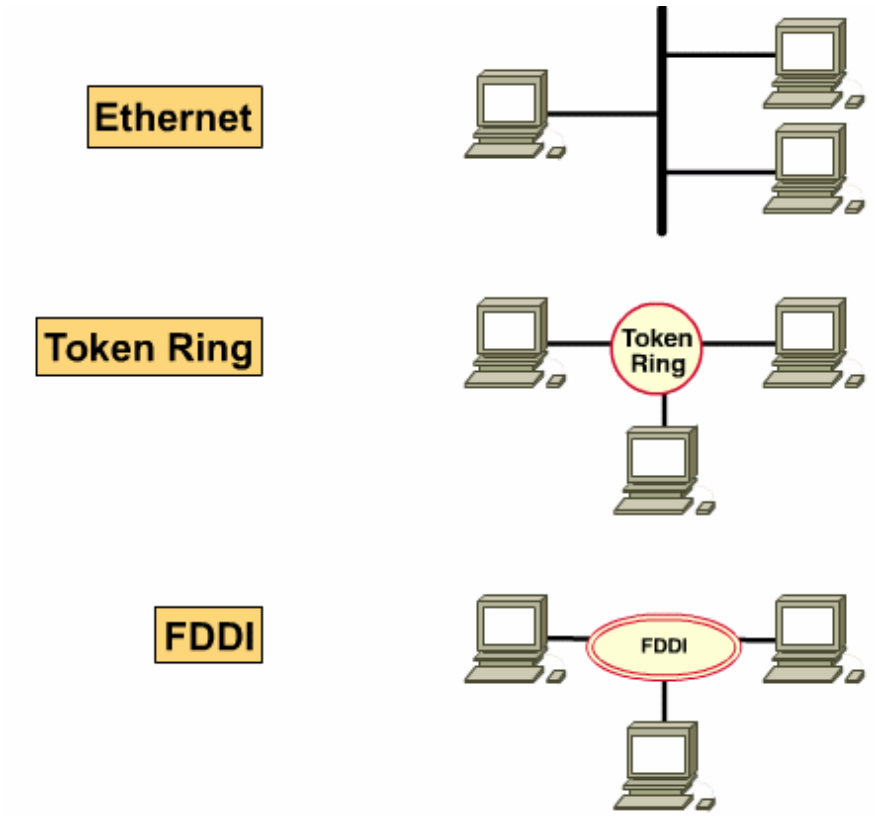
- ***Hubs*** que concentran las conexiones LAN y permiten el uso de medios de cobre de par trenzado.
- ***Switches* Ethernet** que brindan ancho de banda dedicado *full dúplex* a tráfico proveniente de estaciones de trabajo o segmentos.
- **Routers** que ofrecen varios servicios, incluyendo *internetworking* y control de tráfico *broadcast*.

Existen tres tecnologías a las cuales pertenecen la mayoría de las redes LAN:

- **Ethernet:** Es la tecnología LAN más importante y se ejecuta en gran parte de las redes LAN (ver figura 4). Consiste en una topología de bus lógica (el flujo de información se ubica en un bus lineal) y en estrella física o estrella extendida (cableada en forma de estrella).
- **Token-Ring:** Es una tecnología desarrollada por IBM, apareció después de Ethernet y hoy en día se usa en una gran cantidad de redes IBM (ver figura 4). Consta de una topología de anillo lógica (flujo de información se controla en un anillo) y topología física en estrella.
- **FDDI:** También utiliza tokens[*], y actualmente es una LAN que se usa ampliamente en los campus (ver figura 4). Consta de una topología de anillo lógica y topología física de anillo doble (cableada en forma de anillo doble).

[*] CHOMICZ, Bob. Instalaciones de fibra óptica. Madrid: McGraw-Hill, 1998. Págs. 144-146

**Figura 4. Tecnologías LAN**




En una LAN, la capa física proporciona acceso a los medios de red. La capa de enlace de datos brinda soporte para las comunicaciones a través de diferentes tipos de enlaces de datos, tales como los medios Ethernet/IEEE 802.3. Los medios de capa 1 más utilizados son: coaxial, fibra óptica[*] y cable de par trenzado.

[*] CHOMICZ, Bob. Instalaciones de fibra óptica. Madrid: McGraw-Hill, 1998. Págs. 1-10

### 1.3.2 Acceso múltiple con detección de portadora y detección de colisiones

Una LAN Ethernet se denomina red de acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD). Esto quiere decir que la transmisión de un nodo atraviesa toda la red y es recibida y examinada por cada nodo. Cuando una estación desea transmitir una señal, verifica la red para determinar si alguna otra estación se encuentra transmitiendo. Si la red no está en uso, la estación comienza la transmisión. En esta tecnología sólo existe una transmisión por vez en un momento determinado.

### 1.3.3 Direccionamiento lógico (IP)

Resulta muy conveniente conocer el proceso con el cual la información localiza sistemas informáticos específicos en una red. Para ello, se utilizan diversos esquemas de direccionamiento que dependen de los protocolos que se manejen.

Las direcciones de la capa de enlace de datos y de la capa de red son dos tipos de direcciones de gran importancia. Las direcciones de la capa de enlace de datos (direcciones físicas o direcciones MAC) son normalmente únicas para cada conexión de red y constan de un direccionamiento plano. Las direcciones de capa de red (direcciones lógicas o direcciones IP para el conjunto de protocolo Internet) existen en la Capa 3 y son de carácter jerárquico.

### 1.3.4 Direccionamiento MAC

Para que múltiples estaciones puedan compartir los mismos medios y aún así identificarse entre sí, las subcapas MAC definen las direcciones de enlace de datos (direcciones MAC). Cada interfaz LAN posee una dirección MAC exclusiva que se encuentra grabada de forma indeleble en la ROM de la mayoría de las NIC. Cuando se inicializa la NIC, esta dirección se copia en la RAM.

Antes de que los dispositivos directamente conectados en la misma LAN puedan intercambiar una trama de datos, el dispositivo origen debe tener la dirección MAC del dispositivo destino. Una manera de que el emisor pueda asegurarse de que encontrará las direcciones MAC que necesita es utilizar un ARP (Protocolo de Resolución de Direcciones). Este tema se ampliará más adelante.

## 1.4 DIRECCIONAMIENTO TCP/IP

### 1.4.1 TCP/IP

Aunque el modelo OSI sea universalmente reconocido, el estándar abierto de Internet desde el punto de vista histórico y técnico es el Protocolo de control de

transmisión/Protocolo Internet (TCP/IP)[*]. El modelo de referencia TCP/IP y la pila de protocolo TCP/IP hacen que sea posible la comunicación entre dos computadores, desde cualquier parte del mundo, a casi la velocidad de la luz. El modelo TCP/IP está basado en el tipo de red *packet-switched* (de conmutación de paquetes), y tiene cuatro capas: la capa de aplicación, la capa de transporte, la capa de Internet y la capa de red.

#### 1.4.1.1 Capa de aplicación

Los diseñadores de TCP/IP sintieron que los protocolos de nivel superior deberían incluir los detalles de las capas de sesión y presentación. Entonces crearon una capa de aplicación que maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. De esta manera, el modelo combina todos los elementos relacionados con las aplicaciones en una sola capa y supone estos datos están correctamente empaquetados para la siguiente capa.

#### 1.4.1.2 Capa de transporte

Permite que capas pares en los *host* de origen y destino puedan conversar. También maneja los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Utiliza servicios de la

[*] http://www.cnice.mecd.es/tecnologica/experto/protocolos

capa de red para proveer un servicio eficiente y confiable a los procesos de la capa de aplicación.

#### 1.4.1.3 Capa de Internet

Esta capa se encarga de enviar paquetes origen desde cualquier red en *Internetwork* de redes y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que se utilizaron para llegar hasta allí. En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes. Durante su transmisión los paquetes pueden ser divididos en fragmentos, que se montan de nuevo en el destino. En una comunicación con arquitectura TCP/IP ambos *host* pueden introducir paquetes en la red, viajando estos independientemente de cual sea su destino. Por ello, no hay garantía ninguna de entrega de los paquetes ni de orden en los mismos.

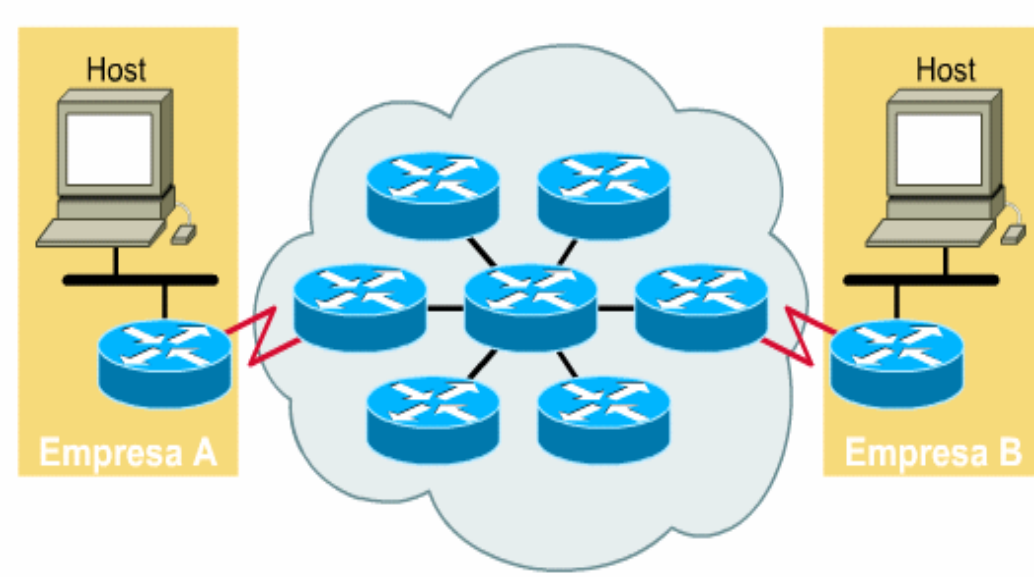
#### 1.4.1.4 Capa de red

Esta capa se ocupa de todos los aspectos que requiere un paquete IP para realizar un enlace físico y luego realizar otro enlace físico. Esta capa incluye los detalles de tecnología de LAN y WAN, y de los detalles de las capas física y de enlace de datos del modelo OSI.

### 1.4.2 Entorno TCP/IP

En un entorno TCP/IP, las estaciones finales se comunican con servidores u estaciones finales ya que cada nodo posee una dirección lógica de 32 bits exclusiva conocida como dirección IP. Así que, cada organización que logra conectarse a la *internetwork* puede verse como una sola red (ver figura 5). A su vez, cada red de la empresa tiene una dirección. Los *hosts* de esta red comparten la misma dirección de red, pero cada *host* tiene una dirección exclusiva de *host* en dicha red.

**Figura 5. Entorno TCP/IP**



### 1.4.3 Subredes

Cuando una red maneja rangos de direcciones IP[*] significativos resulta más conveniente transformar estas IPs a un rango propio más fácil de administrar.

Las subredes mejoran la eficiencia del direccionamiento de la red. La adición de subredes no cambia la manera en que el mundo exterior visualiza la red, pero hace que dentro de la organización exista una estructura adicional. Los *routers* determinan la red destino utilizando la dirección de subred, que limita la cantidad de tráfico en los demás segmentos de la red. Desde el punto de vista del direccionamiento, las subredes son una extensión del número de una red. Los administradores de red determinan el tamaño de las subredes según las necesidades de expansión de sus organizaciones. Los dispositivos de red usan máscaras de subred para identificar qué parte de la dirección le corresponde a la red y qué parte representa el direccionamiento del *host*.

La máscara de subred es un conjunto de 32 bits que permiten separar de una dirección IP la parte del identificador de la subred de la parte del nodo. Con el uso de las máscaras de subred se logra también la perfecta separación de IPs de una red en departamentos y estaciones, ya que con los datos de la IP y de la máscara de subred de cada equipo el servidor sabe en todo momento hacia qué estación

[*] GARZÓN, Gonzalo. Módulo de Informática Básica. Cartagena: CUTB, 2002. Págs.76-79

de trabajo van los paquetes y si debe enviarlos directamente o enrutarlos al exterior.

A la hora de asignar direcciones IP a una red se considera el tamaño y las necesidades de ésta, por lo que se distinguen 3 tipos principales de redes para la asignación de direcciones IP:

#### 1.4.3.1 Redes de clase A

Estas redes necesitan de un gran número de direcciones IP, debido al número de *host* que comprenden. A este tipo de redes se les asigna un rango de direcciones IP identificado por el primer grupo de 3 dígitos (primer octeto de la IP), de tal forma que disponen de los otros 3 grupos siguientes para asignar direcciones a sus *host*. El número de direcciones resultante es muy elevado, por lo que las redes de clase A corresponden fundamentalmente a organismos gubernamentales, grandes universidades, etc.

#### 1.4.3.2 Redes de clase B

Estas redes manejan un número de direcciones IP intermedio para conectar todos sus *host* con Internet. A este tipo de redes se les asigna un rango de direcciones IP identificado por los dos primeros grupos de 3 dígitos (primer y segundo octetos de la IP), de tal forma que disponen de los otros 2 grupos siguientes para asignar

direcciones a sus *host*. El número de direcciones resultante es de 64.000, por lo que las redes de clase B* corresponden fundamentalmente a grandes empresas, organizaciones gubernamentales o universidades de tipo medio, etc.

#### 1.4.3.3 Redes de clase C

Estas redes necesitan de un número de direcciones IP pequeño para conectar los host con Internet. A este tipo de redes se les asigna un rango de direcciones IP identificado por los tres primeros grupos de 3 dígitos (primero, segundo y tercer octetos de la IP), de tal forma que disponen de un sólo grupo para asignar direcciones a los *host*. El número de direcciones resultante es de 256, por lo que las redes de clase C corresponden fundamentalmente a pequeñas empresas, organismos locales, etc.

#### 1.4.3.4 Ejemplo de subredes

En el siguiente ejemplo se va a considerar una red pública, es decir, formada por *host* con direcciones IP públicas, que pueden ser vistas por todos las máquinas conectadas a Internet. El desarrollo es también válido para redes privadas y, en general, para toda red corporativa.

---

* http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

Se tomará como ejemplo una red de clase C, pero el procedimiento es útil para cualquier tipo de red, sea de clase A, B o C. Entonces, se determina la red, con dirección IP **210.25.2.0**, por lo que se debe asignar a los *host* de la misma todas las direcciones IP del rango 210.25.2.1 al 210.25.2.254, ya que la dirección 210.25.2.0 será la de la propia red y la 210.25.2.255 será la dirección de broadcast general. A continuación se muestra la dirección de red en binario:

210.25.2.0 = 11010010.00011001.00000010.**00000000**

Con lo que se tienen 24 bits para identificar la red y 8 bits para identificar los *host* (en negrilla). La máscara de red será:

11111111.11111111.11111111.00000000 = 255.255.255.0

Para crear subredes a partir de una dirección IP de red, la idea es "robar" bits a los host, pasándolos a los de identificación de red. Se roba el número de bits necesarios para obtener las subredes que se requieran, teniendo en cuenta que cuántos más bits se tomen, más subredes se obtendrán, pero con menos *host* cada una. Por lo tanto, el número de bits a tomar depende de las necesidades de funcionamiento de la red final.

Para calcular la máscara de subred basta con presentar la dirección propia de la subred en binario, poner a 1 todos los bits que se dejen para la parte de red

(incluyendo los robados a la porción de *host*), y poner a 0 todos los bits que queden para los *host*. Luego, se pasa la dirección binaria resultante a formato decimal separado por puntos, y ésa será la máscara de la subred. Por ejemplo, si se tiene la dirección de clase B:

150.10.x.x = 10010110.00001010.**hhhhhhhh.hhhhhhhh**

y se quitan 4 bits a la porción de *host* para crear subredes:

10010110.00001010.rrrr**hhhh.hhhhhhhh**

la máscara de subred es:

11111111.11111111.1111**0000.000000** = 255.255.240.0

Para crear las subredes se quitan *bits* sucesivos a la porción de *host*, calculando en cada caso las subredes obtenidas, sus direcciones IP y sus máscaras de subred. Para ello, se pasa la dirección IP a binario, se toman los *bits* "robados" a la porción de *host* y se varían de todas las formas posibles: 0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111. Lo anterior, en el caso de 4 *bits*. Luego se calculan las IP de los *host* correspondientes a cada una de las variaciones hallando los márgenes de las mismas, ya que estarán entre el valores mínimo y el máximo al variar los

*bits* de la porción de *host* entre todos 0 (dirección de subred) y todos 1 (dirección de *broadcast* correspondiente). Si quitamos un sólo bit a la parte de *host*:

parte de red: 11010010.00011001.00000010.r

parte de *host*: **hhhhhhh**

Permutando los bits de host robados para obtener las subredes obtenidas: $2^1=2$

Es decir, 2 subredes (11010010.00011001.00000010.0 y 11010010.00011001.00000010.1 ). Pero no se puede disponer de la subred que toma el 0, ya que entonces contendría la IP de la red original, ni de la que toma el 1, ya que contendría la dirección de *broadcast* de la red original. Es decir, robando 1 sólo bit no se pueden crear subredes.

Como regla general, el número de subredes obtenidas al quitar n bits a la porción de host será $2^2$-2, y el número de *host* disponible en cada subred será $2^{(8-n)}$-2, ya que toda subred debe tener su propia dirección de red y su propia dirección de *broadcast*.

Si se quitan 2 bits a la parte de *host*:

parte de red: 11010010.00011001.00000010.rr

parte de *host:* **hhhhhh**

número de subredes válidas: $2^2$-2=2

número de *host* válidos por subred: $2^6$-2=62

Las direcciones de subred se obtienen haciendo las combinaciones posibles con los 2 bits robados:

11010010.00011001.00000010. **00** 000000 a 11010010.00011001.00000010. **00** 111111 =210.25.2.0 a 210.25.2.63 (no vale, al contener la dirección de red de la red original).

11010010.00011001.00000010.**01**000000 a 11010010.00011001.00000010.**01**111111 = 210.25.2.64 a 210.25.2.127

Subred válida, con dirección de red=210.25.2.64, *broadcast*=210.25.2.127 y 62 direcciones IP para *host*, que son las comprendidas entre las dos anteriores (de la 210.25.2.65 a la 210.25.2.126).

Máscara de subred: 11111111.11111111.11111111.11000000 = 255.255.255.192

11010010.00011001.00000010.**10** 000000 a 11010010.00011001.00000010.**10** 111111 = 210.25.2.128 a 210.25.2.191

Subred válida, con dirección de red=210.25.2.128, *broadcast*=210.25.2.191 y 62 direcciones IP para *host*, que son las comprendidas entre las dos anteriores (de la 210.25.2.129 a la 210.25.2.190).

Máscara de subred: 11111111.11111111.11111111.11000000 = 255.255.255.192

11010010.00011001.00000010.**11** 000000 a 11010010.00011001.00000010. **11**111111 = 210.25.2.192 a 210.25.2.225 (no vale, al contener la dirección de broadcast de la red original).

Finalmente, se obtienen dos subredes válidas, con 62 direcciones IP válidas cada una, es decir, no se toma el siguiente número de direcciones IP para *host:*

(256-2)-(62+62)=130

La máscara de subred es la misma para todas las subredes obtenidas robando 2 bist a la porción de *host*, y lo mismo ocurre para el robo de otro número de bits.

Cuando se roban 3 bits:

parte de red: 11010010.00011001.00000010.rrr

parte de *host:* **hhhhh**

número de subredes válidas: $2^3$-2=6

número de *host* válidos por subred: $2^5$-2=30

Las direcciones de subred se obtienen haciendo las combinaciones posibles con los 3 bits robados:

11010010.00011001.00000010. **000**00000 a 11010010.00011001.00000010.**000** 11111 (no vale, al contener la dirección de red de la red original).

11010010.00011001.00000010.**001** 00000 a 11010010.00011001.00000010. **001**11111 = 210.25.2.32 a 210.25.2.63

Subred válida, con dirección de red=210.25.2.32, *broadcast*=210.25.2.63 y 30 direcciones IP para *host*, que son las comprendidas entre las dos anteriores (de la 210.25.2.33 a la 210.25.2.62).

11010010.00011001.00000010.**010** 00000 a 11010010.00011001.00000010.**010** 11111 = 210.25.2.64 a 210.25.2.95

Subred válida, con dirección de red=210.25.2.64, *broadcast*=210.25.2.95 y 30 direcciones IP para *host*, que son las comprendidas entre las dos anteriores (de la 210.25.2.65 a la 210.25.2.94).

11010010.00011001.00000010.**011** 00000 a 11010010.00011001.00000010.**011** 11111 = 210.25.2.96 a 210.25.2.127

Subred válida, con dirección de red=210.25.2.96, *broadcast*=210.25.2.127 y 30 direcciones IP para *host*, que son las comprendidas entre las dos anteriores (de la 210.25.2.97 a la 210.25.2.126).

11010010.00011001.00000010.**100** 00000 a 11010010.00011001.00000010.**100** 11111 = 210.25.2.128 a 210.25.2.159

Subred válida, con dirección de red=210.25.2.128, *broadcast*=210.25.2.159 y 30 direcciones IP para *host*, que son las comprendidas entre las dos anteriores (de la 210.25.2.129 a la 210.25.2.158).

11010010.00011001.00000010.**101** 00000 a 11010010.00011001.00000010.**101** 11111 = 210.25.2.160 a 210.25.2.191

Subred válida, con dirección de red=210.25.2.160, *broadcast*=210.25.2.191 y 30 direcciones IP para *host*, que son las comprendidas entre las dos anteriores (de la 210.25.2.161 a la 210.25.2.190).

11010010.00011001.00000010.**110** 00000 a 11010010.00011001.00000010.**110** 11111 = 210.25.2.192 a 210.25.2.223

Subred válida, con dirección de red=210.25.2.192, *broadcast*=210.25.2.223 y 30 direcciones IP para *host*, que son las comprendidas entre las dos anteriores (de la 210.25.2.193 a la 210.25.2.222).

11010010.00011001.00000010. **111**00000 a 11010010.00011001.00000010. **111**11111 = 210.25.2.224 a 210.25.2.255 (no vale, al contener la dirección de *broadcast* de la red original).

Máscara de subred para todas ellas:

11111111.11111111.11111111.11100000 = 255.255.255.224

Se obtienen 6 subredes válidas, con 30 direcciones IP válidas para *host* cada una, es decir, no se toma el siguiente número de direcciones IP para *host*:

(256-2)-(30+30+30+30+30+30)=74

De la misma forma se procede para el robo de 4, 5 y 6 bits (de 7 no se puede ya que entonces las subredes resultantes sólo podrían tener 2 direcciones IP, una para la subred y otra de *broadcast*, con lo que no podrían tener *host*). Cada vez que se pide prestado otro bit del campo de *host*, la cantidad de subredes totales posibles se duplica, mientras que la cantidad de direcciones de *host* totales que se pueden asignar se reduce a la mitad.

# 2. CONFIGURACIÓN DEL ROUTER

## 2.1 CARACTERÍSTICAS DE LAS WAN

Una WAN* (red de área amplia) opera en la capa física y la capa de enlace de datos del modelo OSI interconectando redes LAN que normalmente se encuentran separadas por grandes áreas geográficas. Las WAN llevan a cabo el intercambio de paquetes y tramas de datos entre *routers* y puentes y las LAN que soportan. Las características de las redes WAN son:

- Operan dentro de un área geográfica mayor que el de las redes LAN locales.
- Usan conexiones seriales de diversos tipos para acceder al ancho de banda dentro de áreas geográficas extensas.

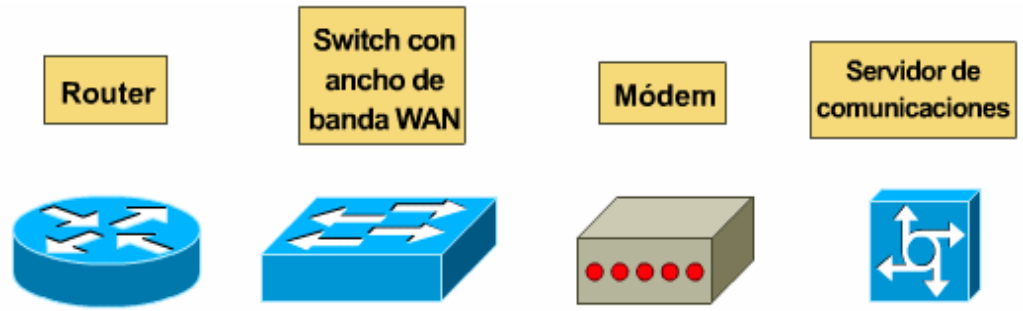
Los dispositivos que se utilizan a nivel WAN son (ver figura 6):

- **Routers:** ofrecen varios servicios, entre ellos *internetworking* y puertos de interfaz WAN.

*
http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

- ***Switches*:** utilizan al ancho de banda de las WAN para la comunicación de voz, datos y video.
- ***Módems*:** servicios de interfaz con calidad de voz; unidades de servicio de canal y unidades de servicio de datos (CSU/DSU) que realizan interfaz con servicios T1/E1; y Adaptadores de Terminal y Terminación de red 1 (TA/NT1) que realizan interfaz con los servicios de la Red digital de servicios integrados (RDSI).
- **Servidores de comunicaciones:** concentran la comunicación de usuarios de servicios de acceso telefónico.

**Figura 6. Dispositivos WAN**




### 2.1.1 Estándares WAN

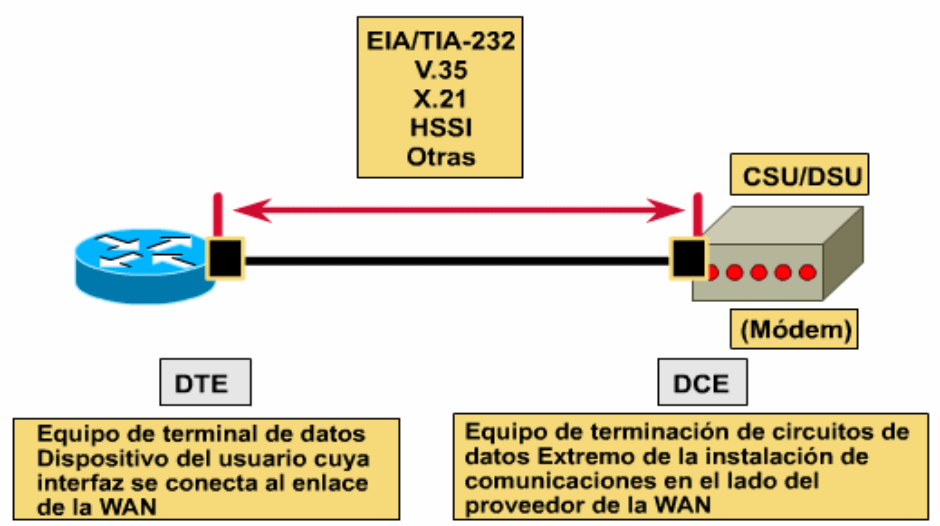
Los protocolos de la capa física de las WAN describen cómo suministrar conexiones eléctricas, mecánicas, operacionales y funcionales para los servicios WAN. Estos servicios a menudo se obtienen de proveedores de servicios WAN

como los RBOC, proveedores alternos y empresas de servicios postales, telefónicos y telegráficos (PTT).

Los protocolos de enlace de datos de las WAN describen cómo se transportan las tramas entre sistemas a través de un solo enlace de datos. Incluyen protocolos diseñados para operar a través de servicios de conmutación punto a punto, multipunto y multiacceso, como *Frame Relay*.

Los estándares WAN describen los requisitos de la capa física y de la capa de enlace de datos. La capa física de las WAN (ver figura 7) describe la interfaz entre el equipo terminal de datos (DTE) y el equipo de terminación de circuito de datos (DCE).

**Figura 7. Capa Física WAN**



Normalmente el DCE es el proveedor del servicio, mientras que el DTE es el dispositivo conectado. En este modelo, los servicios ofrecidos al DTE están disponibles a través de un módem o CSU/DSU.

A continuación se muestran los encapsulamientos de enlace de datos comunes asociados con las líneas síncronas seriales:

- **Control de Enlace de Datos de Alto Nivel (HDLC):** HDLC admite configuraciones punto a punto y multipunto con un gasto mínimo .
- **Frame Relay:** Usa instalaciones digitales de alta calidad y entramado simplificado sin mecanismos de corrección de errores, lo que significa que puede enviar información de Capa 2 mucho más rápidamente que otros protocolos WAN.
- **Protocolo Punto a Punto (PPP):** Contiene un campo de protocolo para identificar el protocolo de capa de red.
- **Protocolo de Control de Enlace de Datos Simple (SDLC):** Protocolo de enlace de datos WAN diseñado por IBM para los entornos de la Arquitectura de sistemas de red (SNA). Ha sido reemplazado en gran parte por el más versátil HDLC.
- **Protocolo Internet de Enlace Serial (SLIP):** Protocolo de enlace de datos WAN utilizado para transportar paquetes IP. Ha sido reemplazado en varias aplicaciones por el más versátil PPP.

- **Procedimiento de Acceso al Enlace Balanceado (LAPB):** Protocolo de enlace de datos utilizado por X.25. Posee amplias capacidades de verificación de errores.
- **Procedimiento de Acceso al Enlace en el Canal D (LAPD):** Protocolo de enlace de datos WAN utilizado para señalización y para configuración de llamada del Canal D de RDSI. Las transmisiones de datos tienen lugar en los canales B de RDSI.
- **Trama de Procedimiento de Acceso a Enlaces (LAPF):** Para servicios de portadora en modo de trama, un protocolo de enlace de datos WAN, similar a LAPD, utilizado con tecnologías *Frame Relay*.

### 2.1.2 Tecnologías WAN

Estas tecnologías se dividen en servicios conmutados por circuito, conmutados por celdas, digitales dedicados y analógicos (ver figura 8).

#### 2.1.2.1 Servicios conmutados por circuitos

a. **POTS (Servicio telefónico analógico):** No es un servicio informático de datos pero se menciona porque muchas de sus tecnologías forman parte de la infraestructura de datos y porque es un modelo confiable y de fácil uso para una red WAN. El medio típico es la línea telefónica de par de cobre.

b. **RDSI (Red Digital de Servicios Integrados) de banda angosta:** Fue el primer servicio de acceso telefónico totalmente digital. Su costo es moderado. El ancho de banda máximo es de 128 kbps para la BRI (Interfaz de Acceso Básico) de menor costo y de aproximadamente 2 Mbps para la PRI (Interfaz de Acceso Principal). El medio típico es el cable de cobre de par trenzado.

#### 2.1.2.2 Servicios conmutado por paquetes

a. **X.25:** Tecnología más antigua pero todavía ampliamente utilizada, que posee amplias capacidades de verificación de errores heredadas de la época en que los enlaces de las WAN eran más susceptibles a los errores, lo que hace que su confiabilidad sea muy grande, pero al mismo tiempo limita su ancho de banda. Este tema se ampliará en el capítulo 5.

b. **Frame Relay:** Versión conmutada por paquetes del RDSI de banda angosta. Es más eficiente que X.25, con servicios similares. El ancho de banda máximo es de 44,736 Mbps. Es de uso generalizado, el costo es de moderado a bajo. Este tema se explicará más detalladamente en el capítulo 5.

#### 2.1.2.3 Servicios conmutados por celdas

a. **ATM (Modo de Transferencia Asíncrona):** Es una tecnología WAN (e inclusive LAN) cuya importancia va en aumento y guarda relación con RDSI de

banda ancha. Utiliza tramas pequeñas, de longitud fija (53 bytes) para transportar los datos. El ancho de banda máximo es actualmente de 622 Mbps, aunque se están desarrollando velocidades mayores. Los medios típicos son el cable de cobre de par trenzado y el cable de fibra óptica. Este tema se ampliará en el capitulo 5.

b. **SMDS (Servicio de datos multimegabit conmutado):** Relacionado con ATM y utilizado en las MAN. El ancho de banda máximo es de 44,736 Mbps. Los medios típicos son el cable de cobre de par trenzado y el cable de fibra óptica.

#### 2.1.2.4 Servicios digitales dedicados

a. **T1, T3, E1, E3:** Estas tecnologías usan la multiplexación por división de tiempo para "dividir" y asignar ranuras de tiempo para la transmisión de datos. Los medios utilizados son normalmente el cable de cobre de par trenzado y el cable de fibra óptica. Los anchos de banda manejados son: T1: 1.544 Mbps; T3: 44.736 Mbps; E1: 2.48 Mbps y E3: 34.368 Mbps .

b. **xDSL (Digital Subscriber Line - Línea Digital del Suscriptor):** Tecnología WAN nueva y en desarrollo para uso doméstico. Su ancho de banda disminuye a medida que aumenta la distancia desde los equipos de las compañías telefónicas. Las velocidades máximas de 51,84 Mbps son posibles en las cercanías de una central telefónica. Son más comunes los anchos de banda

mucho menores (desde 100 kbps hasta varios Mbps). La **x** indica toda la familia de tecnologías DSL, entre ellas: HDSL (DSL de alta velocidad de bits), SDSL (DSL de línea única), ADSL (DSL asimétrica), VDSL (DSL de muy alta velocidad de bits), RADSL (DSL adaptable a la velocidad).

c. **SONET (Red óptica Síncrona):** Conjunto de tecnologías de capa física de muy alta velocidad, diseñadas para cables de fibra óptica, pero que también pueden funcionar con cables de cobre. Están implementadas a diferentes niveles de portadora óptica (OC) desde los 51,84 Mbps (OC-1) hasta los 9,952 Mbps (OC-192). Puede alcanzar estas velocidades de datos mediante el uso de multiplexación por división de longitud de onda (WDM). Su uso es generalizado entre las entidades backbone de Internet.

#### 2.1.2.5 Otros servicios WAN

a. **Módems de acceso telefónico (conmutación analógica):** Su velocidad es limitada, pero son muy versátiles y de gran uso. Funcionan con la red telefónica existente. El ancho de banda máximo aproximado es de 56 kbps. El costo es bajo y el medio típico es la línea telefónica de par trenzado.

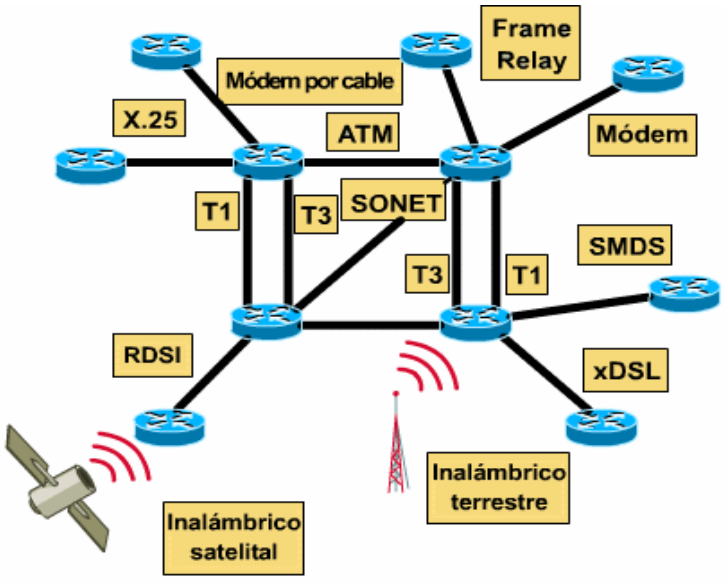
b. **Módems por cable (analógico compartido):** Colocan señales de datos en el mismo cable que las señales de televisión. El ancho de banda máximo disponible puede ser de 10 Mbps, aunque esto se degrada a medida que más

usuarios se conectan a un segmento determinado de la red . El medio típico es el cable coaxial.

c. **Inalámbrico:** No se necesita un medio porque las señales son ondas electromagnéticas. Existen varios enlaces WAN inalámbricos, dos de los cuales son:

- **Terrestre:** Anchos de banda normalmente dentro del intervalo de 11 Mbps (por ej., microondas). Normalmente se requiere línea de vista.
- **Satélite:** Puede servir a los usuarios móviles (por ej., red telefónica celular) y usuarios remotos.

**Figura 8. Tecnologías WAN**



## 2.2 ROUTERS

### 2.2.1 Generalidades sobre routers

Un *router*[*] tiene los mismos componentes básicos de un computador (CPU, memoria, interfaces y un bus) pero no lo es ya que sólo se dedica al enrutamiento. Los *routers* utilizan el software denominado Sistema Operativo de *Internetworking* (IOS) para ejecutar archivos de configuración. Estos archivos controlan el flujo de tráfico a los *routers*. Específicamente, al usar protocolos de enrutamiento para dirigir los protocolos enrutados y las tablas de enrutamiento, toman decisiones con respecto a la mejor ruta para los paquetes. Los componentes internos del *router* son los siguientes (figura 9):

#### 2.2.1.1 RAM/DRAM

Almacena tablas de enrutamiento, caché ARP, caché de conmutación rápida, búfering de paquetes (RAM compartida) y colas de espera de paquetes. La RAM también proporciona memoria temporal y/o de ejecución para el archivo de configuración del router, mientras éste se enciende. El contenido de la RAM se pierde cuando se apaga o se reinicia el *router*.

---

[*] http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

#### 2.2.1.2 NVRAM

RAM no volátil. Almacena el archivo de configuración de inicio/copia de respaldo del archivo de configuración de un *router*. El contenido no se elimina cuando se apaga o se reinicia el *router.*

#### 2.2.1.3 Flash

ROM borrable y reprogramable. Contiene la imagen y microcódigo del sistema operativo. Permite actualizar el software sin eliminar y reemplazar chips en el procesador. El contenido se conserva cuando se apaga o reinicia el r*outer*. Se pueden almacenar múltiples versiones del software IOS en la memoria *Flash.*

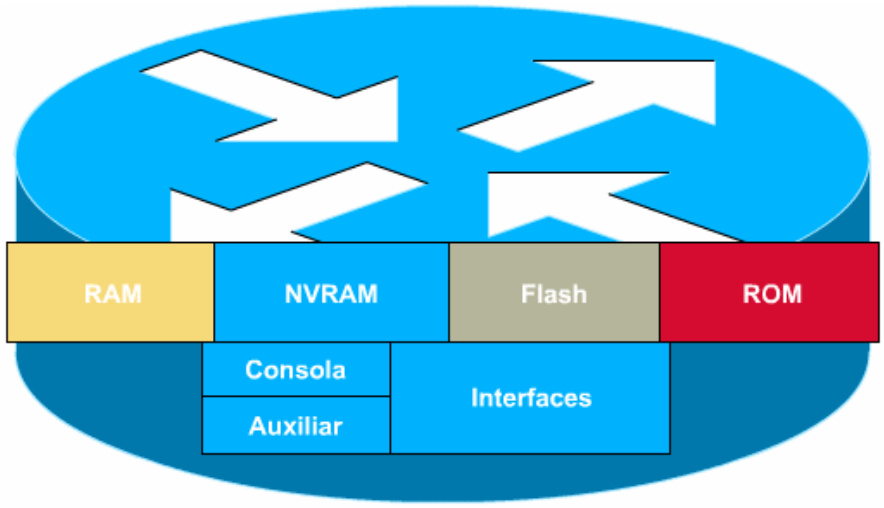
#### 2.2.1.4 ROM

Contiene diagnósticos de encendido, un programa *bootstrap* y software del sistema operativo. Las actualizaciones de software en ROM requieren el reemplazo de chips enchufables en el CPU.

#### 2.2.1.5 Interfaz

Conexión de red a través de la cual los paquetes entran y salen de un *router.* Puede estar en un *motherboard* o en un módulo de interfaz separado.

**Figura 9. Componentes de la configuración interna del router**




### 2.2.2 Routers y WAN

Los *routers* tienen interfaces LAN y WAN. Se pueden utilizar para segmentar dispositivos LAN y para conectarlos entre sí se utilizan las tecnologías WAN, constituyendo sistemas autónomos y el *backbone* de Internet.

Debido a que los routers son los dispositivos de backbone de las redes internas, extensas y de Internet, operan en la Capa 3 del modelo OSI, tomando decisiones basadas en direcciones de red. Las dos funciones principales de los routers son la selección de mejores rutas para los paquetes de datos entrantes, y la conmutación de paquetes a la interfaz de salida correspondiente.

## 2.3 MODO DE CONFIGURACIÓN DEL ROUTER

### 2.3.1 Modos del router

Un *router* puede operarse desde diferentes modos, sea para acceder desde la consola o mediante una sesión Telnet a través del puerto correspondiente. Los modos del *router* son los siguientes:

- **Modo EXEC usuario [router>]:** Aquí el usuario puede visualizar información acerca del *router*, pero no puede realizar cambios.
- **Modo EXEC privilegiado [router#]:** Soporta los comandos de depuración y prueba, el examen detallado del *router*, la manipulación de los archivos de configuración, y el acceso a los modos de configuración.
- **Modo de configuración inicial (setup):** Muestra en la consola un diálogo interactivo basado en indicadores que ayuda al nuevo usuario a crear una configuración básica inicial.
- **Modo de configuración global [router(config)#]:** Implementa comandos más complejos de una línea que ejecutan tareas simples de configuración.
- **Otros modos de configuración [router(config-modo)#]:** Permiten configuraciones más detalladas de múltiples líneas.
- **Modo RXBOOT:** Modo de mantenimiento que se puede usar, entre otras cosas, para recuperar contraseñas perdidas.

### 2.3.2 Uso de los modos de configuración del router

El modo EXEC interpreta los comandos que se escriben y realiza las operaciones correspondientes. Existen dos modos* EXEC. Los comandos EXEC disponibles en el modo usuario son un subconjunto de los comandos EXEC disponibles en el modo privilegiado. Desde el modo privilegiado, también se puede acceder al modo de configuración global y a los modos de configuración específicos, algunos de los cuales se suministran en la siguiente tabla:

**Tabla 1. Modos de configuración específicos del router**

| Modo de configuración | Indicador |
|---|---|
| Interface (Interfaz) | Router(config-if)# |
| Subinterface (Subinterfaz) | Router(config-subif)# |
| Controller (Controlador) | Router(config-controller)# |
| Map-list (Lista de mapa) | Router(config-map-list)# |
| Map-class (Clase de mapa) | Router(config-map-class)# |
| Line (Línea) | Router(config-line)# |
| Router | Router(config-router)# |
| IPX-router (Router IPX) | Router(config-ipx-router)# |
| Route-map (Mapas de router) | Router(config-route-map)# |

*
http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

### 2.3.2 Modo de configuración global

Los comandos de configuración global se aplican a las funciones que afectan al sistema en su totalidad. El comando EXEC privilegiado configure se utiliza para entrar al modo de configuración global. Cuando se introduce este comando, EXEC pide introducir la fuente de los comandos de configuración.

Se puede especificar como fuentes, la terminal, la NVRAM o un archivo guardado en el servidor de red. La opción por defecto es escribir los comandos desde la consola de terminal. Si se presiona la tecla Retorno, se inicia este método de configuración.

Los comandos que habilitan una función de enrutamiento o interfaz en particular comienzan con los comandos de configuración global:

- Para configurar un protocolo de enrutamiento (indicador config-router) primero se debe introducir un tipo de comando de protocolo de *router* global.
- Para configurar una interfaz (indicador config-if) primero se debe introducir el comando global de tipo y número de interfaz. Una vez que ha introducido comandos en cualquiera de estos modos, se termina introduciendo el comando **exit.**

### 2.3.3 Configuración de los protocolos de enrutamiento

Cuando se habilita un protocolo de enrutamiento mediante un comando global, aparece el indicador del modo de configuración del *router:*

**Router (config-router)# .**

Para obtener una lista de los subcomandos de configuración del protocolo de enrutamiento se escribe un signo de interrogación (?).

### 2.3.4 Comandos de configuración de la interfaz

Como todas las interfaces de router se inician automáticamente en el modo administrativamente desactivado, muchas funciones se activan por interfaz. Los comandos de configuración de interfaz modifican la operación de un puerto Ethernet, Token Ring o serial. Los subcomandos de interfaz siempre se colocan a continuación de un comando de interfaz porque el comando de interfaz define el tipo de interfaz. Los comandos de configuración de interfaz son los siguientes:

- En el siguiente comando, el tipo de argumento incluye serial, ethernet, token ring y otros:

  **router(config)# interface type port.**

  **Router(config)# interface type slot/port**

- El siguiente comando se utiliza para desactivar la interfaz de forma administrativa:

  **Router(config-if)# shutdown**

- El siguiente, se usa para activar una interfaz que se ha desactivado

  **router(config-if)# no shutdown**

- El siguiente, se utiliza para salir del modo de configuración de interfaz actual:

  **router(config-if)# exit**

### 2.3.5 Configuración de una interfaz específica

En los enlaces seriales, uno de los lados (el DCE) debe suministrar una señal de temporización; el otro lado es un DTE. Si se quiere utilizar una interfaz para suministrar temporización, se debe especificar una velocidad mediante el comando **clock rate** . El comando **bandwidth** permite reemplazar el ancho de banda por defecto que aparece al aplicar el comando **show interfaces.**

## 2.4 GENERALIDADES SOBRE EL ENRUTAMIENTO

El enrutamiento es el proceso de enviar un paquete basándose en la IP del destino de manera que todo *host* IP pueda manejar su propio tráfico. Para lograr

dicho proceso se utilizan tablas de enrutamiento para determinar la ruta que siguen los paquetes en la red. El contenido de esas tablas puede generarse manualmente o automáticamente a través de protocolos dinámicos.

El elemento que se encarga de hacer posible el enrutamiento[*] es llamado enrutador (*router*) y tiene la responsabilidad de encaminar el tráfico entre dos redes (*Gateway* -puerta de enlace-). De esta manera, pueden enviarse los paquetes IP a través de la red. Sin embargo, existen dos formas de entregar un paquete IP:

- **Entrega Directa:** En este caso, el paquete se entrega al equipo de destino y este se encuentra en la misma red física. De manera que, el paquete se encapsula en una trama de interfaz de red (Ethernet, Token ring, etc) y se envía a la dirección física del *host* de destino obtenida mediante ARP.
- **Entrega Indirecta:** En este modo, el paquete se entrega a un nodo intermedio debido a que el equipo de destino no se encuentra en la misma red física. Aquí, el paquete se encapsula pero se envía a la dirección física de un *router*.

Teniendo en cuenta la información anterior, las tablas de enrutamiento guardan información acerca de las redes IP a las cuales tiene acceso y el modo de acceder a ellas, directa o indirectamente.

[*] http://www.cnice.mecd.es/tecnologica/experto/protocolos

Cada vez que sea necesario enviar un paquete habrá que obtener la IP de reenvío, si es una entrega directa será la del destino, si es indirecta será la del siguiente encaminador; y la interfaz que hay que utilizar para el envío. Esta información la da la Tabla de Rutas. Estas tablas contienen la siguiente información:

- **Destino:** Se refiere a direcciones de subred o de red.
- **Máscara de red:** Determina si una dirección IP corresponde con la dirección de destino.
- **Gateway (*next router):*** Muestra la dirección IP del siguiente router en el camino hacia el destino para entregas indirectas.
- **Indicadores (*FLAGS*)**: Proporcionan información adicional del tipo de ruta y su estado:
  - U: ruta activa, se puede utilizar.
  - G: *Gateway*, indica que es una ruta de entrega indirecta.
  - H: Ruta directa a un *host.*
  - D: Esa se ha obtenido mediante un mensaje "*Route Redirect*".
- **Interfaz:** Identificación del interfaz asociado a esa ruta.
- **Métrica:** Indica el costo de la ruta para poder elegir la de menor costo cuando se tengan rutas alternativas.

En las rutas que aparecen en las tablas pueden observarse diferentes tipos:

- **Rutas a redes conectadas directamente:** Corresponden a redes conectadas directamente a algún interface de *host:* el *gateway* aparece en blanco o con la IP del interface.
- **Rutas a redes remotas:** no están conectadas directamente pero son accesibles mediante *routers*, en el *gateway* aparece la IP del siguiente encaminador.
- **Rutas a host:** Se referiere a la ruta de un host concreto [un único equipo] en el cual, el destino de la ruta aparece la IP del host y en la máscara un valor de todo "unos" [255.255.255.255].
- **Ruta por defecto:** Es la ruta a utilizar cuando la IP del destino no concuerda con ninguna de las entradas de la tabla, se reconocen porque tanto en el destino como en la máscara se encontran valores "cero" [0.0.0.0].

Para seleccionar la mejor ruta para el envío de un paquete, el proceso es así:

- Para cada entrada de la tabla se realiza un AND lógico entre la IP de destino y la máscara de red, el resultado se compara con el valor de destino de la ruta para comprobar el grado de coincidencia.
- Se toma la entrada con mayor nivel de coincidencia, en la que concuerde un número mayor de bits. Entre diversas entradas con el mismo nivel de coincidencia se toma la de menor métrica.

- Si no hay coincidencia con ninguna ruta y existe un *gateway* por defecto, se opta por él, si no lo hay se produce un error de enrutamiento. Si se trata de un *host,* el error se comunica a la capa superior Si es el caso de un encaminador, el error se comunica mediante un mensaje ICMP[*] de "*host unreachable*" dirigido a la IP de origen del paquete.

## 2.5 ENRUTAMIENTO ESTÁTICO Y DINÁMICO

En el manejo de las redes, específicamente en el modo en que la información de ruta llega a la tabla de enrutamiento, se pueden establecer dos tipos de enrutamiento. En uno, el administrador de red puede introducir manualmente la información en el *router* (Rutas estáticas). En el otro modo, los *routers* pueden captar la información, en un instante, uno de otro. A esta forma de aprender automáticamente las rutas se conoce como Rutas Dinámicas.

El enrutamiento estático puede resultar inútil cuando el *router* es capaz de saber automáticamente cuál es la información de la ruta. Sin embargo, un administrador puede utilizar el ingreso manual para controlar la ruta que un *router* seleccionará. Por ejemplo, si se desea probar un enlace particular de la red o para conservar el ancho de banda en las redes WAN.

[*] http://www.cnice.mecd.es/tecnologica/experto/protocolos

El enrutamiento dinámico, se produce cuando los routers se envían entre sí mensajes periódicos de actualización de enrutamiento. Cada vez que un router recibe un mensaje que contiene nueva información, vuelve a calcular una nueva mejor ruta y envía esta nueva información actualizada a los demás *routers*. Al usar el enrutamiento dinámico, los *routers* se pueden adaptar a los cambios en las condiciones de las redes. Los protocolos RIP, IGRP, EIGRP y OSPF son ejemplos de protocolos de enrutamiento dinámico.

## 2.6 PROTOCOLOS DE ENRUTAMIENTO DINÁMICO

Existe dos tipos de protocolos de enrutamiento:

- **EGP (protocolos de enrutamiento de gateway exterior):** Este tipo de protocolo enruta datos entre sistemas autónomos.
- **IGP (protocolos de enrutamiento de gateway interior):** Estos protocolos enrutan los datos en un sistema autónomo.

Entre los ejemplos de los protocolos IGP se encuentran RIP, IGRP, EIGRP y OSPF; los cuales, se explicarán a continuación.

### 2.6.1 Protocolo de información de enrutamiento (RIP)

Es el protocolo más común para transferir información de enrutamiento entre *routers* ubicados en la misma red y se encarga de calcular las distancias hacia un destino. RIP permite que los *routers* que usan este protocolo actualicen sus tablas de enrutamiento a intervalos programables, normalmente cada 30 segundos.

Este protocolo también permite que el *router* determine cuál es la ruta que usará para enviar datos, basándose en un concepto que se conoce como vector-distancia. Siempre que se transportan datos en un *router* y, por lo tanto, a través de un nuevo número de red, se considera que han realizado un salto.

Si hay múltiples rutas hacia un destino, el *router* selecciona la ruta que tiene el menor número de saltos. Sin embargo, el número de saltos es el único método utilizado como métrica de enrutamiento para averiguar la mejor ruta, pero esto no quiere decir que la ruta escogida sea la más rápida.

El protocolo RIP permite un máximo de 15 saltos a través de los cuales se pueden enviar datos si el destino se encuentra demasiado lejos. Si la red destino está ubicada a más de 15 *routers* de distancia, se le considera inalcanzable.

Para usar la configuración RIP se utilizan básicamente los siguientes comandos:

- El comando **router rip** selecciona a RIP como el protocolo de enrutamiento.
- El comando **network** asigna una dirección de clase de red a la cual un *router* se conectará directamente. El proceso de enrutamiento asocia interfaces con direcciones de red y empieza a utilizar RIP en las redes especificadas.

En el monitoreo del flujo de paquete IP se utilizan los siguientes comandos:

- El comando **show ip protocol** muestra valores acerca de temporizadores de enrutamiento e información de red, asociados con todo el router. Se utiliza principalmente para identificar un *router* que parece estar entregando información de enrutamiento incorrecta.
- El comando **show ip route** muestra el contenido de la tabla de enrutamiento IP, que contiene entradas para todas las redes y subredes conocidas, junto con un código que indica de qué manera se obtuvo la información.
- El comando **debug ip rip** muestra las actualizaciones de enrutamiento RIP a medida que se envían y reciben.

### 2.6.2 Protocolo de enrutamiento de gateway interior (IGRP)

El IGRP es un protocolo desarrollado por Cisco Systems y fue creado para darle solución a problemas como el enrutamiento en grandes redes en donde era complicado manejar otro tipo de protocolos como el RIP. IGRP también es un

protocolo de vector distancia, sin embargo, al determinar cuál es la mejor ruta también tiene en cuenta elementos como, por ejemplo, el ancho de banda, la carga, el retardo y la confiabilidad. También incluye la cuenta de saltos y la MTU (*Maximun Transfer Unit*)[*]. IGRP envía actualizaciones de enrutamiento a intervalos de 90 segundos, publicando las redes en un sistema autónomo en particular. Algunas de las características de IGRP muestran lo siguiente:

- Versatilidad que permite manejar automáticamente topologías indefinidas y complejas.
- Flexibilidad para segmentos con distintas características de ancho de banda y de retardo.
- Escalabilidad para operar en redes de gran envergadura.

Las metas del enrutamiento con IGRP son:

- Enrutamiento estable incluso en redes muy grandes y complejas.
- Rápida respuesta a cambios en la topología de la red.
- Pequeño overhead, IGRP no usa más ancho de banda de lo que necesita para su tarea.
- Reparte el tráfico entre rutas paralelas diferentes cuando son igual de buenas.
- Toma en cuenta la tasa de errores y el nivel de tráfico en diferentes caminos.

[*] http://www.cnice.mecd.es/tecnologica/experto/protocolos

- Manejo de múltiples "tipos de servicio" con un conjunto simple de información.

IGRP es un protocolo que permite a los *routers* construir las tablas de enrutamiento a partir del intercambio de información con otros *routers*. Un *router* comienza con entradas en sus tablas para todas las redes que están directamente conectadas a él y buscará una ruta que representa la mejor para llegar a cada red. Un camino se caracteriza por el próximo *router* al que deben ser enviados los paquetes, la interface de red que debe utilizarse e información de la métrica.

Para habilitar IGRP se pueden utilizar los siguientes comandos:

- El comando **router igrp** selecciona a IGRP como el protocolo de enrutamiento.
- El comando **network** especifica cualquier red conectada directamente que se desee incluir.

En el monitoreo de paquete IP se utilizan los siguientes comandos:

- El comando **show ip protocol** muestra parámetros, filtros e información de red acerca de todos los protocolos de enrutamiento en uso en el *router*.
- El comando **show ip** interfaces muestra el estado y los parámetros globales asociados con todas las interfaces IP.

- El comando **show ip route** muestra el contenido de una tabla de enrutamiento IP. La tabla contiene una lista de todas las redes y subredes conocidas y las métricas asociadas con cada entrada.

### 2.6.3 Protocolo de enrutamiento de gateway interior mejorado (EIGRP)

EIGRP es una versión avanzada de IGRP y suministra una eficiencia de operación superior combinando las ventajas de los protocolos de estado de enlace con las de los protocolos de vector distancia.

El algorítmo utilizado en EIGRP es el DUAL (*Distributed Update Algirithm*) y se aplica para obtener la computación de una ruta libre de bucles. Permite a todos los *routers* incluidos en un cambio en la topología sincronizarse al mismo tiempo. Los *routers* no afectados por este cambio, no están incluidos en el nuevo cálculo. EIGRP es extendido para ser un protocolo de capa de red independiente, permitiendo que DUAL pueda soportar otra serie de protocolos.

Los routers EIGRP descubren a sus vecinos e intercambian paquetes de saludo. Este protocolo envía paquetes de saludo cada 5 segundos. Si no llegan tres, se da por hecho que el *router* vecino está muerto y se utilizan rutas alternativas.

### 2.6.4 OSPF

OSPF significa "primero la ruta libre más corta". Este protocolo utiliza diferentes criterios para determinar cuál es la mejor ruta hacia un destino. Entre estos criterios se incluyen las métricas de costo, que influyen en elementos tales como velocidad, tráfico, confiabilidad y seguridad de la ruta. Cuando se creó este protocolo, se hizo para que cumpliera con los siguientes requerimientos:

- Ser abierto en el sentido de que no fuera propiedad de una compañía.
- Que pudiera varias métricas, entre ellas, la distancia física y el retardo.
- Que se adaptará rápida y automáticamente a los cambio de la topología.
- Ser capaz de realizar en encaminamiento dependiendo del tipo de servicio.
- Que pudiera equilibrar las cargas dividiendo la misma entre varias líneas.
- Que reconociera sistemas jerárquicos.
- Que implementara un mínimo de seguridad.

El protocolo OSPF se basa en el algorítmo SPF (*Link State)*[*] , y no tanto en el número menor de saltos.

OSPF encamina paquetes basados solo en la dirección IP destino del paquete y no se requiere además de eso ninguna encapsulación. Cada *router* mantiene una

[*] http://www.solont.com/z-net/ospf/ospf.htm

base de datos que describe al sistema autónomo, el cual consiste en entradas que describen cada estado local del *router*, por ejemplo sus interfaces disponibles y los vecinos alcanzables.

OSPF permite a las redes agruparse conjuntamente dentro de áreas haciendo que la topología interior del área sea invisible fuera de ella, y los routers que están dentro del área no tengan mayor información de la topología exterior.

El uso de áreas reduce el tráfico de enrutamiento comparado al que tiene el sistema autónomo completo como una única área. El enrutamiento entre áreas se efectúa vía backbone o troncal y, con ello, los *routers* se dividen en diferentes categorías dependiendo de su localización: r*outers* internos[*], de límite de área y de backbone. OSPF soporta los siguientes tipos de red física:

- **Punto a punto:** Los cuales unen un único par de *routers*. Por ejemplo, una línea en serie.
- **Broadcast:** Soporta muchos *routers*, con la capacidad de enviar un único mensaje a todos los dispositivos acoplados. Por ejemplo, Ethernet.
- **No broadcast:** Con múltiple acceso pero sin capacidad de *broadcast*. Por ejemplo, X.25.

[*] http://www.w10.org/~sjmudd/wireless/network-structure/html/x284.html

# 3. SEGURIDAD EN REDES

## 3.1 QUÉ ES SEGURIDAD?

La seguridad es la característica de cualquier sistema (informático o no) que indica que ese sistema está libre de todo peligro, daño o riesgo. Pero en informática es preferible utilizar el término “fiabilidad” dado que no existen sistemas ciento por ciento seguros. La fiabilidad hace referencia a la probabilidad de que un sistema se comporte tal y como se espera de él.

En un sistema que se considera fiable (seguro) se deben garantizar tres aspectos: confidencialidad, integridad y disponibilidad. La confidencialidad menciona que los objetos de un sistema deben ser accedidos únicamente por elementos autorizados a ello, provocando que la información no sea disponible para otras entidades; la integridad significa que los objetos sólo pueden ser modificados de manera controlada por elementos autorizados, y la disponibilidad indica que los objetos del sistema tienen que permanecer accesibles a elementos autorizados. Generalmente tienen que existir los tres aspectos descritos para que haya seguridad.

## 3.2 LISTAS DE CONTROL DE ACCESO: ACLs

Existen muchas maneras de controlar el acceso a la red, sin embargo, se deben buscar formas que permitan el acceso por parte del personal autorizado e impedir el acceso no autorizado a la red. Para ello, fueron creadas las listas de control de acceso, ACL (*Access Control Lists)*, las cuales consisten en un grupo de sentencias de permiso o rechazo que se aplican a direcciones o protocolos de capa superior.

Las ACL son listas de instrucciones que se aplican a una interfaz del *router* y le indican a éste qué tipos de paquetes debe aceptar y cuáles denegar. La aceptación y rechazo se basa en información específica como dirección origen, dirección destino y número de puerto.

Las ACL se pueden crear para todos los protocolos enrutados de red, como el Protocolo Internet (IP) y el Intercambio de paquetes de *internetwork* (IPX), para filtrar los paquetes a medida que pasan por un *router*.

Las ACLs proveen de un nivel adicional de seguridad a los ficheros extendiendo el esquema de permisos de usuarios habituales (propietario, grupo y resto). Las ACLs pueden asignar permisos a usuarios o grupos concretos; por ejemplo, se pueden otorgar ciertos permisos a dos usuarios sobre unos ficheros sin necesidad de incluirlos en el mismo grupo.

Los tipos* de ACL son:

- **Estándar:** Éste tipo de ACL usa cuando se desea bloquear todo el tráfico de una red, permitir todo el tráfico desde una red específica o denegar conjuntos de protocolo. Las ACL estándar comprueban las direcciones de origen de los paquetes que solicitan enrutamiento. Lo anterior permite o deniega el resultado para todo un conjunto de protocolos, según las direcciones de red, subred y *host*.
- **Extendidas:** Las ACL extendidas se usan para verificar condiciones ya que brindan más opciones de control que las ACL estándar. Las ACL extendidas comprueban tanto la dirección origen como la destino de cada paquete. También pueden verificar protocolos, números de puerto y otros parámetros específicos.
- **ACL de entrada (in):** los paquetes son procesados antes de que sean enrutados a una interfaz de salida.
- **ACL de salida (out):** los paquetes entrantes son enrutados a la interfaz de salida y luego son procesados por las listas de acceso antes de ser transmitidos.

La manera de aplicarlas es la siguiente:

---

*

http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054916637179372,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna3v2121001l,Engine=static/toc.html

- Para las listas de salida (out) permitir significa enviar al *buffer* de salida, y denegar significa descartar el paquete.
- Para las listas de entrada (in) permitir significa continuar el procesamiento del paquete (enlutarlo) y denegar significa descartar el paquete. Cuando se descarta se envía un mensaje ICMP que notifica al remitente que el destino ha sido inalcanzable.

Para acceder a determinados servicios de una máquina, es necesario definir permisos sobre el modo de acceso, el origen y los servicios a los que se permite acceder a esa máquina; esto se puede lograr mediante la orden **access-list:**

**access-list ID accion proto dir-origen pto-origen dir-destino pto-destino.**

Para habilitar un acceso HTTP desde cualquier lugar de Internet, y además acceso POP3 desde un segmento externo (por ejemplo, 196.33.22.128/25) a la máquina 158.42.22.41, se puede hacer mediante una ACL estándar:

**Router(config)# access-list [1-99] permit tcp any host 158.42.22.41 eq http**

**Router(config)# access-list [1-99] permit tcp 196.33.22.128 255.255.255.128 host 158.42.22.41 eq http**

Para que ningún equipo del exterior haga ping a la máquina 158.42.22.41, excepto los que vienen de la red 196.72.31.0/24, se define la siguiente ACL:

**Router(config)# access-list [1-99] permit icmp 196.72.31.0 255.255.255.0 host 158.42.22.41**

**Router(config)# access-list [1-99] deny icmp any any**

Con las órdenes anteriores se define la ACL ; esto no tiene ningún efecto sobre el funcionamiento del *firewall*, ya que para que lo tenga hay asociar esta lista a una interfaz de red: en concreto, a aquella de la que va a provenir el tráfico de entrada en cada caso. Para ello, se utiliza la orden **access-group**:

**Router(config-if)#{protocolo}access-group [1-99]{ in interface outside}**

Con este comando se asocia la lista de control a la interfaz especificada; si esta interfaz ya tenía asociada una lista de control, la nueva reemplaza a la antigua pero las conexiones no se pierden, ni siquiera las que estaban permitidas anteriormente pero que ahora se niegan. Esto es útil para poder añadir entradas intermedias a las listas de control sin que las conexiones establecidas por la interfaz a la que se desea asociarlas se pierdan: para ello, lo más rápido es copiar la lista en un editor de textos, realizar sobre el mismo las modificaciones necesarias, y grabarla de nuevo en el *firewall* con otro nombre; tras esto, se asocia a la interfaz correspondiente mediante **access-group**, y cuando todo funcione correctamente se graba en memoria mediante **write mem**. Si se desea añadir una entrada al final de la lista de control no es necesario todo esto: basta con ejecutar el **access-list** correspondiente para que la nueva entrada se añada a la lista, y automáticamente se aplique sobre la interfaz; si no se quiere añadir, sino eliminar

entradas de una ACL, se puede ejecutar directamente **no access-list**, orden que recibe como parámetro la entrada a eliminar:

**Router(config)# sh access-list [1-99]**

**access-list [1-99] permit tcp any host 158.42.22.41 eq smtp (hitcnt=0)**

**access-list [1-99] permit tcp any host 158.42.22.41 eq pop3 (hitcnt=0)**

**access-list [1-99] permit tcp any host 158.42.22.41 eq telnet (hitcnt=0)**

**Router(config)# no access-list [1-99] permit tcp any host 158.42.22.41 eq pop3**

**Router(config)# sh access-list [1-99]**

**access-list [1-99] permit tcp any host 158.42.22.41 eq smtp (hitcnt=0)**

**access-list [1-99] permit tcp any host 158.42.22.41 eq telnet (hitcnt=0)**

En cuanto a una ACL extendida, la forma completa del comando access-list es:

**Router(config)# access-list access-list-number {permit | deny}**

**protocol source [source-mask destination destination-mask operator operand] [established]**

El comando **ip access-group** une una ACL extendida existente a una interfaz. Sólo se permite una ACL por interfaz. El formato del comando corresponde a la primera línea; la segunda es un ejemplo de ACL extendida:

**Router(config-if)# ip access-group access-list-number {in | out}**

**Router(config)# access-list [100-199] permit icmp 196.72.31.0 255.255.255.0 host 158.42.22.41**

Según el lugar donde se ubique una ACL, se puede reducir el tráfico innecesario. En las ACL extendidas, hay que colocarlas lo más cerca posible del origen del tráfico denegado. Las ACL estándar no especifican direcciones destino, de manera que se deben colocar lo más cerca posible del destino.

Las ACL en routers firewall normalmente se sitúan entre la red interna y una red externa. El router firewall proporciona un punto de aislamiento, de manera que el resto de la estructura interna de la red no se vea afectada. También se pueden usar las ACL en un router situado entre dos partes de la red a fin de controlar el tráfico que entra o sale de una parte específica de la red interna.

Para aprovechar las ventajas de seguridad de las ACL, se deben configurar las ACL en los routers fronterizos, que están situados en las fronteras de la red. Esto brinda protección con respecto a la red externa, u otra parte menos controlada de la red. En estos routers fronterizos, se pueden crear ACL para cada protocolo de red configurado en las interfaces del router. Se pueden configurar las ACL para que el tráfico entrante, el tráfico saliente, o ambos, sean filtrados en una interfaz.

# 4. SOLUCIÓN A REDES

## 4.1 PRUEBAS BÁSICAS DE NETWORKING

### 4.1.1 Prueba de la capa de aplicación mediante telnet

Para tener información acerca de un *router* remoto se puede utilizar el protocolo conocido como Telnet. Este se define como un protocolo de terminal virtual que forma parte del conjunto de protocolos TCP/IP y permite que se realicen conexiones a los *hosts*. Se puede establecer una conexión entre un *route*r y un dispositivo conectado. También permite verificar el software de capa de aplicación entre las estaciones origen y destino. Es el mecanismo de prueba más completo disponible. Un *router* puede tener hasta cinco sesiones Telnet entrantes simultáneas.

Se puede usar Telnet para realizar una prueba que determine si se puede o no acceder a un *router* remoto. Una conexión exitosa de Telnet indica que la aplicación de capa superior y los servicios de las capas inferiores funcionan correctamente.

### 4.1.2 Prueba de la capa de red mediante el comando ping

Los protocolos de eco se utilizan para verificar si los paquetes de protocolo se están enrutando. El comando ping envía un paquete al *host* destino y luego espera un paquete de respuesta de ese host. Los resultados de este protocolo de eco pueden ayudar a evaluar la confiabilidad de ruta a host, las demoras en la ruta, si se puede acceder al *host* o si éste está funcionando.

### 4.1.3 Prueba de la capa de red con el comando trace

El comando trace es similar al comando ping, sólo que en lugar de probar la conectividad de extremo a extremo, trace prueba cada paso del proceso y es muy útil para averiguar a dónde se envían los datos en la red. Esta operación se puede realizar en los niveles EXEC usuario o privilegiado.

El comando trace aprovecha los mensajes de error generados por los *routers* cuando un paquete supera su valor de Tiempo de Existencia (TTL). El comando trace envía varios paquetes y muestra el tiempo de viaje de ida y vuelta para cada uno de ellos. La ventaja del comando trace es que indica cuál de los *routers* que aparecen en el camino fue el último al que se accedió. Esto se denomina aislamiento de fallas.

## 4.2 ARCHIVOS DE CONFIGURACIÓN DEL ROUTER

### 4.2.1 Trabajo con archivos de configuración de la versión 11.x

La información de configuración del *router* puede ser generada por varios medios. Se puede utilizar el comando configure del modo EXEC privilegiado para realizar la configuración desde una terminal virtual (remota), una conexión de módem o una terminal de consola. También se puede ingresar el comando configure del modo EXEC privilegiado para cargar una configuración desde un servidor de red TFTP, que permite mantener y guardar información de configuración en un sitio central. A continuación se muestran algunos de los comandos de configuración:

- **Configure terminal:** realiza la configuración desde la terminal de consola de forma manual.
- **Configure memory:** carga la información de configuración desde la NVRAM.
- **Copy tftp running-config:** carga la información de configuración desde un servidor de red TFTP en la RAM.
- **Show running-config:** muestra la configuración actual en la RAM.
- **Copy running-config startup-config:** almacena la configuración actual desde la RAM en la NVRAM.
- **Copy running-config tftp:** guarda la configuración actual de la RAM en un servidor de red TFTP.

- **Show startup-config:** muestra en pantalla la configuración guardada, que es el contenido de la NVRAM.
- **Erase startup-config:** borra el contenido de la NVRAM.

### 4.2.2 Uso de los comandos copy running-config tftp y copy tftp running-config

Se puede guardar una copia de la configuración actual en un servidor TFTP. Con el comando **copy running-config tftp** se puede guardar la configuración actual en la RAM, en un servidor de red TFTP. Para lograr lo anterior se deben seguir los siguientes pasos:

- Introducir el comando **copy running-config tftp.**
- Introducir la dirección IP del *host* que se desea utilizar para guardar el archivo de configuración.
- Introducir el nombre que se desea asignar al archivo de configuración.
- Confirmar las selecciones respondiendo *yes* (sí) cada vez que se solicite hacerlo.

Para configurar el *router* cargando el archivo de configuración que está guardado en uno de los servidores de red se deben realizar las siguientes tareas:

- Introducir el comando **copy tftp running-config.**
- Seleccionar un archivo de configuración de *host* o de red. El archivo de configuración de red contiene comandos que se aplican a todos los *routers* y servidores de terminal de la red. El archivo de configuración del *host* contiene comandos que se aplican a un *router* en particular.
- Introducir la dirección IP opcional del *host* remoto desde el cual se está recuperando el archivo de configuración.
- Introducir el nombre del archivo de configuración o aceptar el nombre por defecto. El nombre de archivo por defecto es **hostname-config** para el archivo *host* y **network-config** para el archivo de configuración de la red. En el entorno DOS, los nombres de archivo del servidor se limitan a ocho caracteres con una extensión de tres caracteres (por ejemplo, router.cfg).
- Confirmar el nombre del archivo de configuración y la dirección del servidor que suministra el sistema.

## 4.3 PROCEDIMIENTO DE RECUPERACIÓN DE CONTRASEÑA DEL ROUTER

Un procedimiento común que los técnicos realizan en los *routers* es el procedimiento de recuperación de contraseña. Este procedimiento se mostrará en la práctica de laboratorio correspondiente.

## 4.4 FUNCIONAMIENTO DE ARP

ARP se utiliza para resolver o asignar una dirección IP conocida a una dirección de subcapa MAC para permitir la comunicación a través de un medio de acceso múltiple como, por ejemplo, Ethernet. Para determinar una dirección MAC destino para un datagrama, se verifica una tabla denominada caché ARP. Si la dirección no figura en la tabla, ARP envía un *broadcast* que se recibe en cada estación de la red, buscando la estación destino.

El término "ARP local" se utiliza para describir la búsqueda de una dirección cuando el *host* que la solicita y el *host* destino comparten el mismo medio o cable. Antes de emitir el ARP, se debe consultar la máscara de subred. En este caso, la máscara determina que los nodos se encuentran en la misma subred.

## 4.5 DIAGNÓSTICO DE FALLAS DE LA RED

Las redes se establecen desde un punto de vista de seguridad y trabajo óptimo a cierto nivel que permita trabajar en ellas de manera confiable. Sin embargo, no se encuentran libres de posibles fallas que puedan afectar cualquier proceso que se esté llevando a cabo.

Los errores de Capa 1 incluyen:

- Cables rotos
- Cables desconectados
- Cables conectados a los puertos incorrectos
- Conexión de cable intermitente
- Cables incorrectos para la tarea
- Problemas del *transceiver*
- Problemas del cable DCE
- Problemas del cable DTE
- Dispositivos apagados

Entre los errores de Capa 2 se mencionan:

- Interfaces seriales incorrectamente configuradas
- Interfaces Ethernet incorrectamente configuradas
- Encapsulamiento incorrecto (HDLC es el encapsulamiento por defecto para las interfaces seriales)
- Configuraciones de temporización incorrectas en las interfaces seriales

Algunos de los errores de Capa 3 se definen a continuación:

- Protocolo de enrutamiento inhabilitado
- Protocolo de enrutamiento incorrecto habilitado
- Direcciones IP incorrectas

- Máscaras de subred incorrectas
- Enlaces DNS a IP incorrectos

## 4.6 ESTRATEGIAS DE DIAGNÓSTICO DE FALLAS DE LA RED

Para manejar el diagnóstico de fallas[*] se puede manipular cualquier método siempre y cuando exista algún tipo de proceso ordenado basado en los estándares de *networking* utilizados. El método propuesto por Cisco es el siguiente:

1. Obtener toda la información disponible y analizar los síntomas de la falla.
2. Localizar el problema dentro de un solo segmento de red, de un solo módulo o unidad completos o de un solo usuario.
3. Aislar la falla en un hardware o software específico dentro de la unidad, el módulo o la cuenta de red del usuario.
4. Localizar y corregir el error específico.
5. Verificar si el problema se ha resuelto.

[*] http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

# 5. TECNOLOGÍAS DE REDES DE ÁREA AMPLIA

## 5.1 GENERALIDADES

Al igual que las tecnologías de LAN (*Ethernet, Fast Ethernet, Gigabit Ethernet* y *Token Ring*), los protocolo de WAN funcionan también en la capa de enlace de datos del modelo de referencia OSI. Los protocolos de WAN trasladan los datos de una ubicación a otra a través de una interfaz serie asíncrona o síncrona.

Las transmisiones series síncronas son señales digitales que se transmiten con una temporización precisa de un dispositivo a otro. Por otra parte, la transmisión asíncrona no se realiza con temporización precisa y confía en la información de control (bits de inicio y finalización) que indica el inicio y la finalización de los datos.

El protocolo PPP fue diseñado originalmente para enlaces serie punto a punto, conectando un dispositivo con otro con un encapsulamiento y direccionamiento. El protocolo PPP ha evolucionado para trabajar en entornos tanto síncronos como asíncronos. Los protocolos X.25, *Frame Relay* y ATM no funcionan en un entorno estricto de enlace serie punto a punto, sino que utilizan circuitos virtuales para trasladar los datos.

Un circuito virtual (Virtual Circuit, VC) es un mecanismo de comunicación en el que se establece la ruta para el traslado de una información antes de que se envíen los datos, proceso conocido como colocar una llamada. Todos los paquetes de datos relacionados con la llamada siguen la misma ruta a través de la red, con lo que nos aseguramos de que los datos llegan al destino en el mismo orden que se enviaron. Al terminar la transferencia de datos, se finaliza la llamada. Los circuitos virtuales conmutados (*Switchet Virtual Circuits,* SVC) son los que se pueden establecer y suprimir según lo requiera la red. Los circuitos virtuales permanentes (*Permanent Virtual Circuit,* PVC) los establece la red de forma permanente y nunca se suprimen.

Los circuitos virtuales múltiples (SVC o PVC) pueden residir en una sola interfaz serie de un *router* Cisco. En este caso, cada uno de los circuitos virtuales puede tratarse como una interfaz separada, denominada subinterfaz. Las subinterfaces pueden implementarse para cualquier protocolo de WAN que utilice circuitos virtuales.

Los protocolos de WAN de Cisco que usan circuitos virtuales trasladan los datos de dos formas diferentes: *switching* de paquetes y *relay* de celda. El *switching* de paquetes es un método de transmisión de datos que envía los datos en unidades de longitud variable, también llamadas paquetes. El *switching* de paquetes en la capa de enlace de datos traslada los paquetes desde la capa de red y los encapsula con un direccionamiento de capa de enlace de datos específico. A

medida que los paquetes de enlace de datos atraviesan la red, cada nodo intermedio de *switching* de paquetes situado entre el origen y el destino lee la dirección de enlace de datos del paquete y lo reenvía. El paquete recorre la ruta del circuito virtual establecida previamente hasta que se alcanza la dirección de enlace de datos de destino. Frame Relay y X.25 utilizan *switching* de paquetes.

ATM, convierte los datos de los paquetes en celdas de longitud fija y realizan *relay* de celda. El *relay* de celda es un método de transmisión de datos que envía datos en pequeñas unidades de tamaño filo, también llamadas celdas, que puede procesar el hardware de una manera rápida y eficaz.

El funcionamiento del *relay* de celda es similar al *switching* de paquetes, solo que los datos del sistema de origen se convierten primero en celdas de longitud fija en vez de paquetes.

## 5.2 PROTOCOLO PUNTO A PUNTO

A fines de la década del ´80, el Protocolo Internet de enlace serial (SLIP) representaba una limitación para el crecimiento de Internet. PPP se creó para solucionar los problemas de conectividad remota de Internet. Además, PPP era necesario para poder asignar direcciones IP de forma dinámica y permitir el uso de

múltiples protocolos. PPP suministra conexiones de *router* a *router* y de *host* a red a través de circuitos síncronos y asíncronos.

PPP[*] es el protocolo WAN más popular y más ampliamente utilizado porque ofrece todas estas funciones:

- Control de la configuración del enlace de datos
- Proporciona asignación dinámica de direcciones IP
- Multiplexión de protocolo de red
- Configuración de enlace y verificación de la calidad del enlace
- Detección de errores
- Opciones de negociación para destrezas tales como negociación de la dirección de capa de red y negociaciones de compresión de datos.

### 5.2.1 Componentes de PPP

PPP busca resolver los problemas de conectividad de Internet mediante tres componentes básicos:

[*] LEINWAND, Allan y PINSKY, Bruce. Configuración de Routers Cisco. Madrid: Cisco Press, 2001. Págs 66-67.

- Un método para encapsular datagramas a través de enlaces seriales. PPP utiliza el Control de enlace de datos de alto nivel (HDLC) como base para encapsular datagramas a través de enlaces punto a punto.
- Un Protocolo de control de enlace (LCP) para establecer, configurar y probar la conexión de enlace de datos.
- Una familia de Protocolos de control de red (NCP) para establecer y configurar distintos protocolos de capa de red. PPP está diseñado para permitir el uso simultáneo de múltiples protocolos de capa de red. En la actualidad, PPP soporta otros protocolos además de IP, incluyendo Intercambio de paquetes de *internetworking* (IPX) y *Apple talk*. PPP utiliza su componente de NCP para encapsular múltiples protocolos.

### 5.2.2 Subcomandos de configuración de la interfaz de PPP

Se puede usar el subcomando de configuración de interfaz de IOS **encapsulation ppp** para activar PPP síncrono en una interfaz serie. En el siguiente ejemplo se configura PPP síncrono en la interfaz serial 1/1 del router Lab_a.

Lab_a **# configure terminal**
Lab_a (config ) **# interface serial 1/1**
Lab_a (config-if ) **# encapsulation ppp**
Lab_a (config-if) **# ^ z**

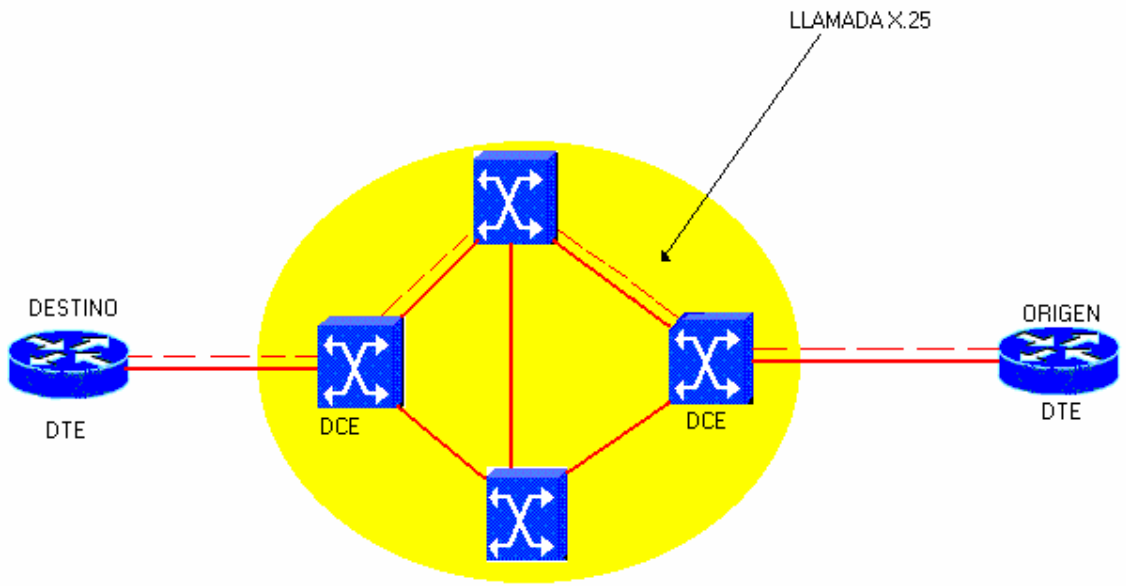
## 5.3 X.25

X.25 es un protocolo de *switching* de paquetes que admite tanto SVC como PVC y que fue desarrollado por primera vez en los años setenta. La Unión Internacional de las Telecomunicaciones (ITU) es una agencia de los Estados Unidos que administra el protocolo X.25. Debido a la gran aceptación internacional de X.25, es posible que sea el protocolo de WAN que más se utiliza en el mundo hoy en día.

Como todos los protocolos de *switching* de paquetes, X.25 fundamentalmente define una red para las comunicaciones de datos similar a la de la red telefónica y traslada los datos mediante circuitos virtuales. La comunicación entre dos dispositivos comienza con la llamada de un dispositivo a otro a fin de establecer un SVC o PVC, sigue la transferencia de los datos y posteriormente acaba con la finalización de la llamada. El protocolo X.25 define una comunicación punto a punto entre el equipo terminal de datos (*Data Terminal Equipment*, DTE) y el equipo de terminación del circuito de datos (*Data Terminating Equipament*, DCE). Los DTE (como los *router* Cisco) se conectan con los DCE (como los *módems*), que se conecta a su vez con uno o más *switches* WAN X.25 y en ultimo término con otro DTE.

Una llamada a través de una red X.25 se inicia cuando el DTE* de origen analiza una llamada al DCE al que está conectado. Los switches X.25 de la red decide como enrutar la llamada del origen al destino. Todos los datos se conmutan entonces desde el DTE de origen al DTE de destino a través de la red X.25, como se ilustra en la figura 10.

**Figura 10: Una Red X.25**




* http://www.linti.unlp.edu.ar/trabajos/tesisDeGrado/tutorial/redes/servicio.htm

El protocolo X.25 utiliza un esquema de direcciones denominado X.121. La recomendación de ITU-T X.121 especifica los formatos de la dirección de origen y de destino para el protocolo X.25 de la capa de enlace de datos. Los *switches* X.25 enrutan las llamadas por la ruta de un circuito virtual basándose en las direcciones X.121 de origen y destino.

En cuanto a la configuración, el primer paso para utilizar X.25 en una interfaz serie Cisco es configurar la interfaz mediante el comando **encapsulation x25** para que pueda utilizar la encapsulación X.25.

Las direcciones X.121 del enlace de datos X.25 no se graban en la ROM como las direcciones LAN. Esto significa que el administrador de la red ha de comunicarle a un *router* Cisco la dirección local X.121 de una interfaz serie X.25, lo que se realiza con el subcomando de configuración de interfaz x25 *address*. Con los *switches* X.25 de algunos fabricantes es necesario establecer un tamaño máximo de paquetes de entrada y de salida (el valor predeterminado es de 128 bytes). Es posible que también haya que que configurar el *router* Cisco con el tamaño de paquetes de entrada (ips,*input paccket size*) y el tamaño de paquetes de salida (ops, *output packet size*) adecuados en la interfaz serie con los comandos x25 ips y x25 ops a fin de funcionar correctamente en la red X.25.

Las redes X.25 tienen un tamaño de ventana de entrada y salida predeterminado para los paquetes que usan los mecanismos de control de flujo. Es posible que

sea necesario configurar el tamaño predeterminado de las ventanas de entrada (win) y de salida (wout) para que la red X.25 funcione correctamente, al igual que tal vez haga también falta definir un tamaño máximo de los paquetes.

En el ejemplo siguiente se configura el router Lab_a con encapulación X.25 y una dirección de enlace de datos X.121 de 537000000001. Se especifica un tamaño de paquetes de entrada y salida de 256 bytes. También se el tamaño de la ventana de salida y entrada en siete paquetes.

Lab_a **# configure terminal**

Lab_a(config) **# interface serial 1**

Lab_a (config-if) **# encapsulation x25**

Lab_a (config-if) **# x25 address 53700000001**

Lab_a (config-if) **# x25 ips 256**

Lab_a (config-if) **# x25 ops 256**

Lab_a (config-if) **# x25 win 7**

Lab_a (config-if) **# x25 wout 7**

Lab_a (config-if) **# ^z**

## 5.4 FRAME RELAY

*Frame Relay* es un estándar del Comité Consultivo Internacional Telegráfico y Telefónico (CCITT) y del Instituto Nacional Americano de Normalización (ANSI) que define un proceso para el envío de datos a través de una red de datos públicos (PDN). Es una tecnología de datos eficiente, de elevado desempeño, utilizada en redes de todo el mundo. *Frame Relay* es una forma de enviar información a través de una WAN dividiendo los datos en paquetes. Cada paquete viaja a través de una serie de *switches* en una red *Frame Relay* para alcanzar su destino. Opera en las capas física y de enlace de datos del modelo de referencia OSI, pero depende de los protocolos de capa superior como TCP para la corrección de errores. *Frame Relay* se planteó originariamente como un protocolo destinado a utilizarse con las interfaces RDSI. Actualmente, *Frame Relay* es un protocolo de capa de enlace de datos conmutado de estándar industrial, que maneja múltiples circuitos virtuales mediante el encapsulamiento de Control de enlace de datos de alto nivel (HDLC) entre dispositivos conectados. *Frame Relay* utiliza circuitos virtuales para realizar conexiones a través de un servicio orientado a conexión.

La red que proporciona la interfaz *Frame Relay* puede ser una red pública proporcionada por una portadora o una red de equipos privados, que sirven a una misma empresa. Una red *Frame Relay* puede componerse de computadores, servidores, etc. en el extremo del usuario y por dispositivos de red *Frame Relay*

como *switches, routers*, CSU/DSU, o multiplexores. Con frecuencia se hace referencia a los dispositivos del usuario como Equipo terminal de datos (DTE), mientras que el equipo de red que hace interfaz con el DTE se conoce a menudo como Equipo de transmisión de datos (DCE).

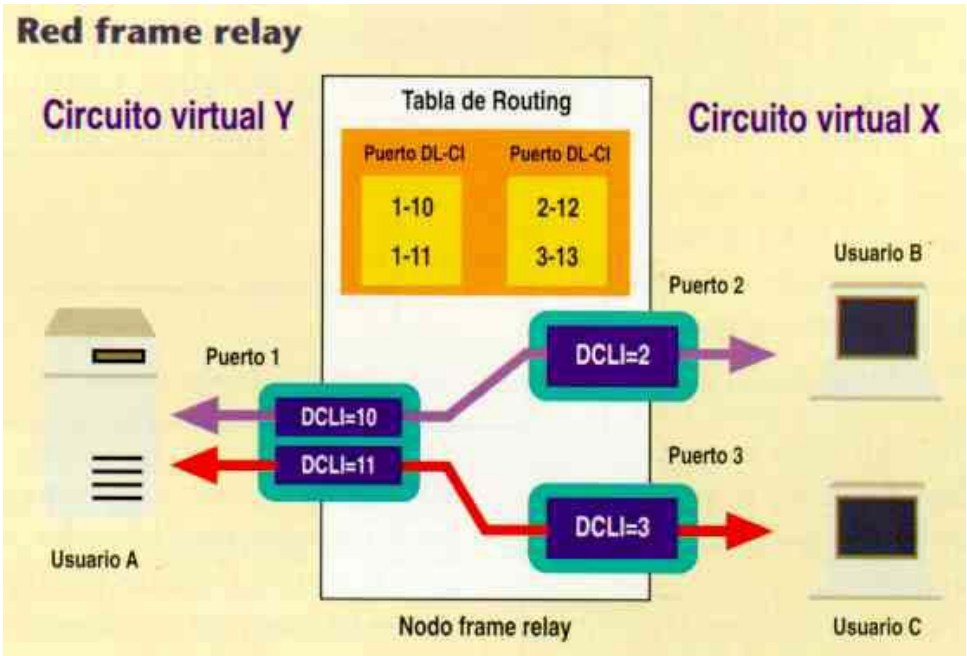
Como interfaz entre el equipo del usuario y de red, *Frame Relay* proporciona un medio para realizar la multiplexión de varias conversaciones de datos lógicas, llamadas circuitos virtuales, a través de un medio físico compartido asignando DLCI (Identificadores de Conexión de enlace de datos, *Data-link Connection Identifiers*) a cada par de dispositivos DTE/DCE.

Los estándares *Frame Relay* direccionan circuitos virtuales permanentes (PVC) que se encuentran administrativamente configurados y administrados en una red *Frame Relay*. Los PVC de *Frame Relay* son identificados por los DLCI. Los DLCI de *Frame Relay* tienen importancia local. Es decir que los valores en sí no son únicos en la WAN *Frame Relay*. Dos dispositivos DTE conectados por un circuito virtual podrían utilizar un valor DLCI distinto para referirse a la misma conexión.

*Frame Relay* proporciona un medio para realizar la multiplexión de varias conversaciones de datos lógicas. El equipo de conmutación del proveedor de servicios genera una tabla asignando los valores DLCI a puertos salientes. Cuando se recibe la trama, el dispositivo de conmutación analiza el identificador de conexión y entrega la trama al puerto saliente asociado. La ruta completa al

destino se establece antes de enviar la primera trama como se muestra en la figura 11.

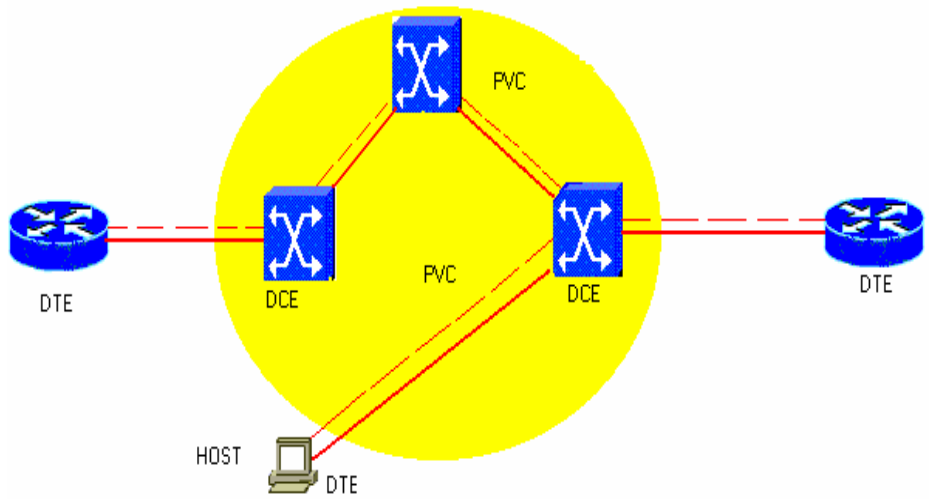
**Figura 11:Identificación de los PVC por los DLCI**




El espacio de direccionamiento DLCI se limita a 10 bits. Esto permite crear 1024 direcciones DLCI posibles. La porción utilizable de estas direcciones es determinada por el tipo de LMI (Interfaz de gestión local, *Local Management Interface*) utilizada. El tipo LMI Cisco soporta un intervalo de direcciones DLCI desde DLCI 16-1007 para el transporte de datos de usuario. El tipo LMI ANSI/UIT soporta un intervalo de direcciones desde DLCI 16-992 para el transporte de datos

de usuario. Las direcciones DLCI restantes se reservan para que el distribuidor las pueda implementar. Esto incluye mensajes LMI y direcciones *multicast.* Una red *Frame Relay* con PVC se muestra en la figura 12.

**Figura 12: una red Frame Relay con PVC**




Para configurar Frame Relay en una interfaz serie Cisco, debemos empezar por usar el subcomando de interfaz encapsulation frame-relay. Posteriormente se puede utilizar el subcomando frame-relay interface-dlci para establecer el DLCI de la interfaz. Los dispositivos Cisco usan de forma predeterminada el LMI de Cisco en las interfaces Frame Relay. Es posible establecer el tipo de LMI utilizando el subcomando de interfaz frame-relay lmi-type. Ejemplo:

Lab_a # **configure terminal**

Lab_a (config) **# interface serial 0**

Lab_a (config-if) **# encapsulation frame**

Lab_a (config-if) **# frame-relay interface-dlci 100**

Lab_a (config-if) **# frame-relay lmi-type ansi**

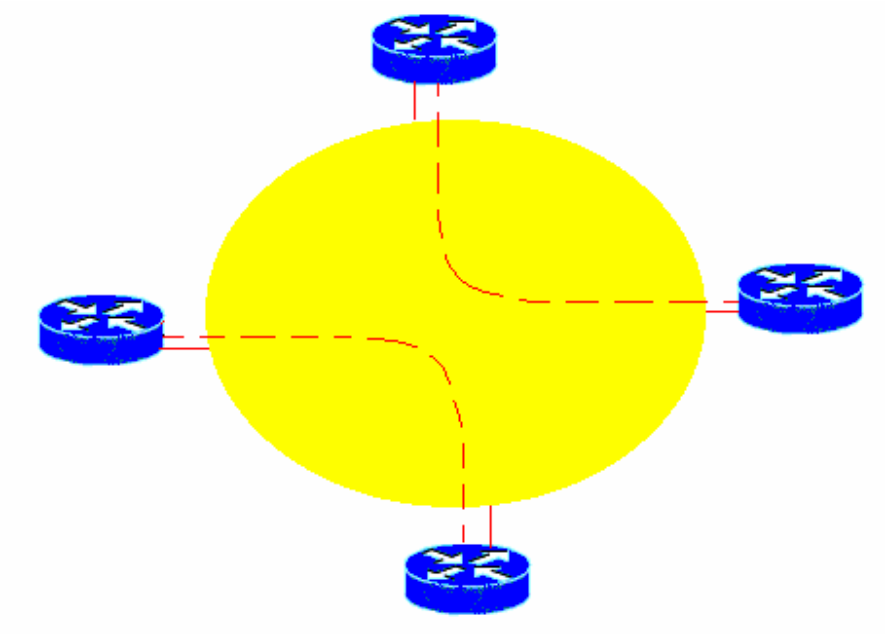
Lab_a (config-if) **# ^z**

La configuración *Frame Relay* anterior es la básica para un solo circuito virtual en una interfaz serie Cisco. También se puede contar con varios circuitos virtuales en una sola interfaz serie y tratar a cada uno de ellos como una interfaz separada, que se llama subinterfaz. Hay que considerar a una subinterfaz como una interfaz de hardware definida por el software IOS.

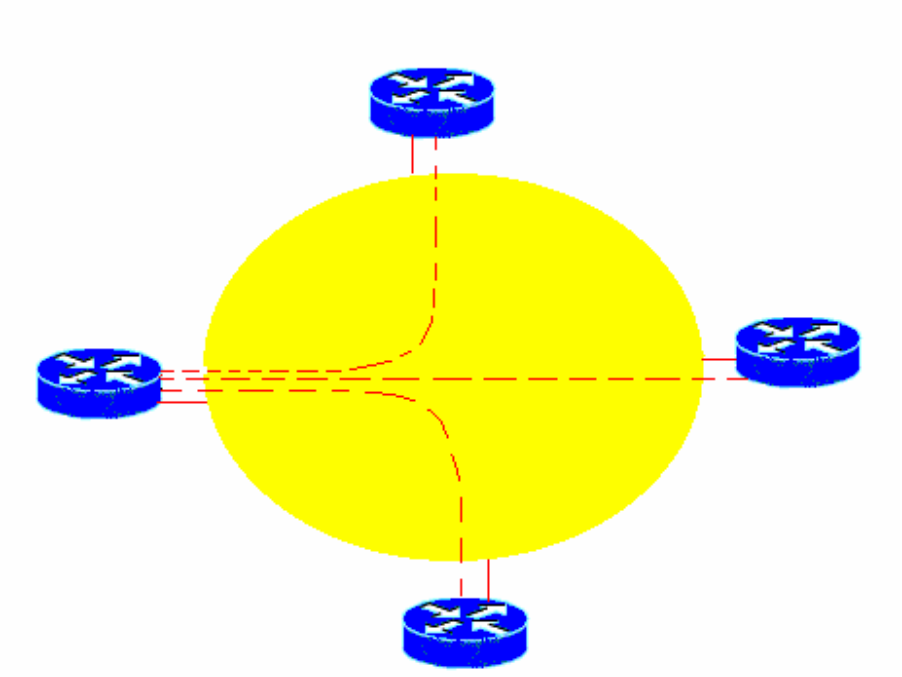
Los dos tipos de subinterfaces son punto a punto y multipunto. Las interfaces punto a punto se utilizan cuando un solo circuito virtual conecta un *router* con otro (ver figura 13.a). Un subinterfaz punto a punto es como un circuito virtual que emula un enlace serie dedicado.

La subinterfaces multipunto se utilizan cuando el router es el centro de una estrella de circuitos virtuales, como se ilustra en la figura 13.b.

**Figura 13: Redes Frame Relay Punto a Punto (a) y Multipunto (b)**



(a)



**(b)**

Es posible definir un número limitado de subinterfaces en una interfaz física determinada (la única excepción es la memoria del router). En el ejemplo siguiente, se define la interfaz serial 0.100 en el router Lab_a.

Lab_a **# configure terminal**

Lab_a (config) **# interface serial 0**

Lab_a (config-if) **# encapsulation frame**

Lab_a (config-if) **# interface serial 0.100 point-to-point**

Lab_a (config-subif) **# frame-relay interface-dlci 100**

Lab_a (config-subif) **# frame-relay lmi-type ansi**

Lab_a (config-subif) **# ^z**

## 5.5 MODO DE TRANSFERENCIA ASÍNCRONA

### 5.5.1 Qué es una red ATM

El *Asynchronous Mode Transfer* (ATM) o Modo de Transferencia Asíncrona es una tecnología de última generación que permite el transporte de distintas señales -datos, audio e imagen de alta calidad- en forma simultánea y asíncrona, es decir, de una forma que asume espontáneamente las distintas señales que son generadas periódicamente por el emisor para organizarlas eficientemente en especies de cápsulas o paquetes que son transferidos a gran velocidad por

canales virtuales. Esto implica que tanto el emisor como el receptor no tienen que estar sincronizados para la transmisión de datos, ya que el conjunto o paquete de datos trae la identificación sobre el inicio y término de la transmisión.

### 5.5.2 Cómo se transmiten los datos?

La alta velocidad que alcanza ATM se basa en la premisa de que para una mejor transmisión de datos, lo óptimo es simplificar los procedimientos. En términos sencillos, lo que hace ATM es mandar para las distintos señales, un solo tipo de paquete de información, de tal modo que los datos se mandan en unas celdas que almacenan bits, que luego llegan a los conmutadores para que éstos los distribuyan. En definitiva, el ahorro de tiempo se consigue al disminuir el trabajo de procesamiento de la información. Con respecto a su reconocimiento mundial, la tecnología ATM, que fue propuesta originalmente por la Industria de las Telecomunicaciones, es recomendada en la actualidad como solución universal para redes de banda ancha por los más importantes organismos de las industrias de comunicaciones y computadores.

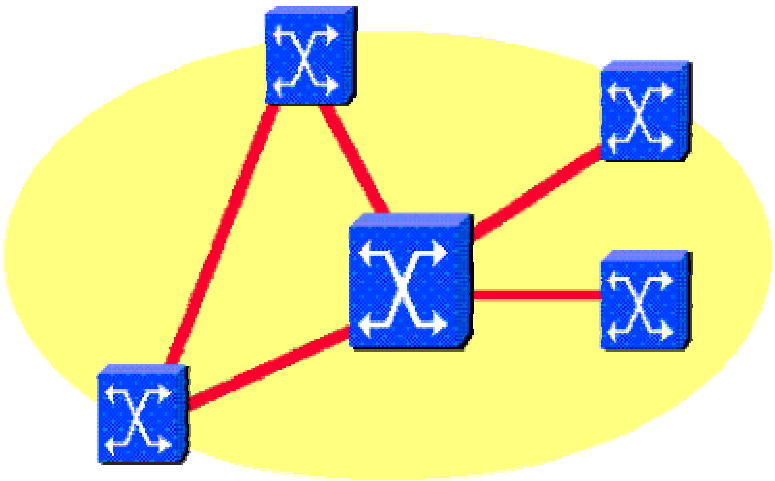
### 5.5.3 Principios de las redes ATM

Una red ATM (ver figura 14) muestra gran capacidad de integración de diversos tipos de tráfico. También presenta otras características, como:

- La asignación dinámica y flexible del ancho de banda.
- La optimización del compromiso entre caudal y latencia.
- La ganancia estadística, es decir, su capacidad de optimizar la relación entre la suma de las velocidades de las fuentes y la velocidad del enlace.

Al usar *relay* de celda, ATM está diseñado para manejar varios tipos de servicios de red, entre los que se incluyen voz, video y datos. Una red ATM consta de *switches* ATM (dispositivo DCE) y puntos finales ATM (dispositivos DTE). Los puntos finales envían información a los *switches* ATM, que segmentan la información en celdas y conmutan las celdas a través de la red. Este proceso es el mismo para los tres tipos de tráfico que maneja la red ATM.

**Figura 14: Una red ATM**



ATM proporciona servicio tanto orientado a conexión (PVC Y SVC) como sin conexión mediante canales virtuales. Un canal virtual es similar a un circuito virtual en X.25 o *Frame Relay*.

La red ATM define las conexiones a través de la red ATM como una rutas virtuales, que se identifican mediante números de identificador de ruta virtual (*virtual path identifier*, VPI).

Una ruta virtual es un paquetes de canales virtuales que están conmutados a través de la red ATM basándose en el mismo VPI. También podemos considerar una ruta virtual como un mecanismo de agrupamiento para definir la ruta de una serie de canales virtuales.

Una red virtual se identifica mediante la combinación de un VPI y un identificador de canal virtual VCI. El VPI define la ruta que recorre el canal virtual a través de la red, mientras que el VCI es exclusivo para cada conexión del VPI. Los números VPI y VCI sólo tienen importancia local, al igual que los números DLCI para *Frame Relay* suelen tener importancia local. Los *switches* ATM asignan los números VPI/VCI a través de un enlace particular con el siguiente dispositivo de la conexión (en la dirección de destino).

Las capas de adaptación ATM (AAL) son protocolo que forman parte del modelo de referencia OSI en la parte superior de la capa de enlace de datos. Estas capas,

cada una de las cuales se denomina AAL, son las responsables de proporcionar los diferentes servicios ATM a los protocolos de la capa de red[*].

### 5.5.4 Subcomandos de configuración de la interfaz de ATM

Las interfaces de AMT de Cisco son procesadores dedicados de la interfaz (o adaptadores de una tarjeta VIP).

Esto implica que no es necesario especificar el subcomando de interfaz encapsulation para la interfaces ATM; la encapsulación ATM es lo único que admite el hardware. No hay que especificar los circuitos virtuales que existen en una interfaz determinada utilizando el comando de interfaz **atm pvc**. La siguiente salida muestra la configuración de PVC 1 usando VPI 0 y VCI 100 para un canal virtual AAL5.

Router # **configure terminal**
Router(config)# **interface atm2/0**
Router(config-if)# **atm pvc 1 0 100 aal5snap**
Router(config-if)# **^z**

[*] http://webepcc.unex.es/jlgs/Art/ponencia10.htm

El estado de una interfaz ATM[*] se puede examinar mediante el comando show interfaces.

[*] LEINWAND, Allan y PINSKY, Bruce. Configuración de Routers Cisco. Madrid: Cisco Press, 2001. Págs 74-76

# 6. CONCLUSIONES

Para el amplio conocimiento de las redes se requiere conocer muchos aspectos acerca de ellas. Básicamente el conocimiento del modelo OSI que incluye el estudio de las funciones de cada capa, el direccionamiento IP, enrutamiento, dispositivos de trabajo, conmutación y tecnologías utilizadas. Todo esto para comprender el funcionamiento de las redes hoy día y de los múltiples procesos que en ellas se realizan. Desde una red sencilla hasta la más compleja comprenden los mismos conocimientos básicos.

Entere estos conceptos básicos es de gran importancia el estudio del router y de las diferentes operaciones que en él se realizan, no sin antes mencionar que es precisamente este dispositivo el que hace posible la comunicación entre redes más sencillas que se encuentran a gran distancia. Dicho comunicación establece el concepto de las WAN, en las cuales el router desempeña un papel importante debido a la labor de enrutamiento que en el se lleva a cabo.

También es de mencionar que una red por sí sola no siempre va a registrar una labor libre de errores y de posibles inconvenientes para los cuales hay que estar preparado. Por ello, además de conocer las características de las redes y su funcionamiento, es de vital importancia mantener su operación y monitoreo

continuo para resolver fallas y protegerlas de cualquier ataque. Por lo cual, se debe estudiar lo concerniente a la seguridad de la red y mantenerse en continuo proceso de actualización de las distintas alternativas que se proponen para ello. Como también el establecimiento de un plan de trabajo que permita resolver cualquier inconveniente de la manera más óptima posible para, así, no alterar la labor de comunicación que se este manejando ya que los inconvenientes en la red de una empresa u organización podrían traer como consecuencia la pérdida de capital, información confidencial o el retraso del resto de procesos que dependan de la red.

# RECOMENDACIONES

En este trabajo, el lector ha encontrado un conjunto de conceptos de red tanto a nivel de LAN (Red de área local) como a nivel de WAN (Red de área amplia) que fundamentan cualquier estudio referente a temas más avanzados en las redes implementadas actualmente.

El énfasis hecho en la configuración del router es otro de los temas básicos de redes que pretendió mostrar, por medio de las prácticas de laboratorio, sus distintas funciones con las cuales es posible lograr el intercambio de información en un área geográfica amplia.

Dichas prácticas deben ser implementadas para adquirir mayor conocimiento y destreza en la labor de configuración del router, para las cuales, se necesita un conjunto de equipos mínimo para lograr su realización, tales como: routers, concentradores, PC's, cables UTP cat. 6, cable de consola, cable WAN y contar con el manejo del Hyperterminal.

Las prácticas de laboratorio pueden mejorarse a través de la configuración de switches, con el fin de crear redes de alta velocidad a nivel de WAN con las tecnologías expuestas en esta monografía (PPP, X.25, Frame Relay y ATM). También se debería montar una práctica de las ACLs con el protocolo de enrutamiento IPX para un futuro, ya que actualmente el laboratorio no posee los equipos necesarios y lo único que se puede hacer es el montaje con el protocolo IP.

# BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

Curriculum CCNA (Cisco certified network associate curriculum) Semester 3 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054916637179372,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna3v2121001l,Engine=static/toc.html

CHOMYCZ, Bob. Instalaciones de fibra óptica: Fundamentos, técnicas y aplicaciones. Madrid: McGraw-Hill, 1998.

GARZÓN, Gonzalo. Módulo de Informática básica. Minor en comunicaciones y redes de computadores. Cartagena: Corporación Universitaria Tecnológica de Bolívar (CUTB), 2002.

LEINWAND, Allan y PINSKY, Bruce. Configuración de Routers Cisco. 2ª. Edición. Madrid: Cisco Press, 2001.

Organización de las Redes Wireless [online]. Madrid: Simon Mudd y Madrid Wireless, 2001. Ultima actualización: 2002. Disponible en Internet: www.wl0.org/~sjmudd/wireless/network-structure/html/x284.html

Protocolo de Encaminamiento OSPF [online]. Madrid, España: Juan Ignacio Jiménez Cuesta, 2000. En Internet: www.solont.com/z-net/ospf/ospf.htm

Protocolos de Encaminamiento [online]. España: Ministerio de Educación, cultura y deporte. Centro Nacional de Información y Comunicación Educativa Madrid CNICE, 2001. Última actualización: 2003. Disponible en Internet: www.cnice.mecd.es/tecnologica/experto/protocolos/

Revisión y Clasificación de Protocolos para Redes de Tecnología ATM [online]. Boletín de red iris: Ponencia 10. José Luis González-Sánchez y Jordi Domingo-Pascual. Escuela Politécnica de Cáceres. Disponible en Internet: http://webepcc.unex.es/jlgs/Art/ponencia10.htm

X.25 [online]. Tutorial sobre servicios en internet. Buenos Aires: Andrea Suárez y Eugenia Losinno, 1998. Ultima modificación: 30/08/1999. Disponible en internet: http://www.linti.unlp.edu.ar/trabajos/tesisDeGrado/tutorial/redes/servicio.htm

# ANEXOS

# ANEXO A. LABORATORIO 1: CARACTERÍSTICAS GENERALES DEL ROUTER

## 1. GUÍA DE LABORATORIO

### 1. 1 OBJETIVOS:

- Determinar el número de modelo de un router Cisco y cuáles son sus interfaces físicas (puertos).
- Identificar los cables conectados al router y a qué parte se conectan.
- Manejar los parámetros de configuración de HyperTerminal.
- Conectarse a la consola del router utilizando el programa de PC HyperTerminal.
- Determinar la versión de IOS y el nombre de archivo.
- Determinar el tipo de CPU, la cantidad de memoria RAM, NVRAM y Flash.

### 1.2 EQUIPO UTILIZADO:

- Windows PC c/ HyperTerminal.
- Router Cisco (modelo 16xx o 25xx)

- Cable de consola (rollover) que conecta el puerto serial del PC con el puerto de consola del router
- Cable Ethernet CAT 6 conectado a un puerto Ethernet
- Hub o switch Ethernet
- Cable WAN conectado a un puerto serial

## 1.3. MARCO TEÓRICO

Un router es un equipo que en su interior tiene una Unidad de procesamiento central (CPU), un sistema operativo (Cisco IOS), RAM y ROM. Se diferencia de un computador porque no tiene unidad de disco, teclado ni monitor. Una de las formas de configurar el router es conectarse directamente a él a través de un PC o una terminal no inteligente. El PC le suministra al router un monitor y un teclado, que constituyen su "consola". De esta manera, se pueden introducir comandos y establecer comunicación directa con el router. Para ello, se utilizará el programa Windows HyperTerminal (emulación de terminal) que permitirá que un PC funcione como la consola del router y configurará los parámetros adecuados de puerto serial del PC para conectarse y comunicarse con él.

## 1.4. PROCEDIMIENTO

- Se debe implementar la red mostrada en la figura 15 verificando que el cableado este correcto.
- Ahora, se examinará al router. Para ello, se identificará el número de modelo del router, el puerto de la terminal de consola al cual se encuentra conectado y el tipo de cable que define al “cable de consola” (rollover, de conexión cruzada o de conexión directa).
- Luego, se deben registrar todas las interfaces (o conectores de puerto) del router y cualquier cable conectado: Esto indica que si el puerto tiene un cable conectado, debe identificarse el tipo de cable, el conector y el dispositivo conectado al otro extremo. Anotar los siguientes datos en la siguiente tabla:

**Tabla 1.**

| | |
|---|---|
| **Interfaz del router** | |
| **Identificador de puerto** | |
| **Tipo de cable** | |
| **Conector** | |
| **Dispositivo conectado al cable** | |
| **Puerto conectado al cable** | |

- Ahora, se debe revisar la configuración HyperTerminal de la estación de trabajo: Para ello, deben seguir los siguientes pasos:

1. Hacer clic en **Inicio/Programas/Accesorios/Comunicaciones** y luego en **HyperTerminal**.
2. Hacer clic con el botón derecho del ratón en el icono que se ha definido para el acceso por consola al router Cisco.
3. Hacer clic en **Propiedades**. El nombre del icono es de la forma xxxx.ht. Si no existe ningún icono, se puede crear utilizando los parámetros que aparecen en las respuestas de la planilla de trabajo. En la pantalla **Propiedades**, se hace clic en la ficha **Número de teléfono** y luego haga clic en el botón **Configurar**.

Luego de efectuar los pasos anteriores, se debe completar la siguiente tabla:

**Tabla 2.**

| **Opción de configuración**<br>**Configuración(es) actual(es)** | |
|---|---|
| **Puerto COM** | |
| **Bits por segundo** | |
| **Bits de datos** | |
| **Paridad** | |
| **Bits de parada** | |
| **Control de flujo** | |

- Conectarse al puerto de consola en el router y escribir el comando **show version**. El propósito de esto es mostrar la versión IOS y cualquier otra información importante relacionada con la memoria RAM, NVRAM y Flash. Luego de aplicar el comando **show versión**, se obtendrá la información mencionada, con la cual, se debe completar la siguiente tabla:

**Tabla 3.**

| | |
|---|---|
| **Versión de IOS** | |
| **Nombre del archivo de imagen de IOS** | |
| **Tipo de procesador (CPU)** | |
| **Cantidad de RAM del router** | |
| **Número de interfaces Ethernet** | |
| **Número de interfaces seriales** | |
| **Cantidad de NVRAM** | |
| **Cantidad de memoria Flash** | |

## 1.5. ANÁLISIS DE RESULTADOS

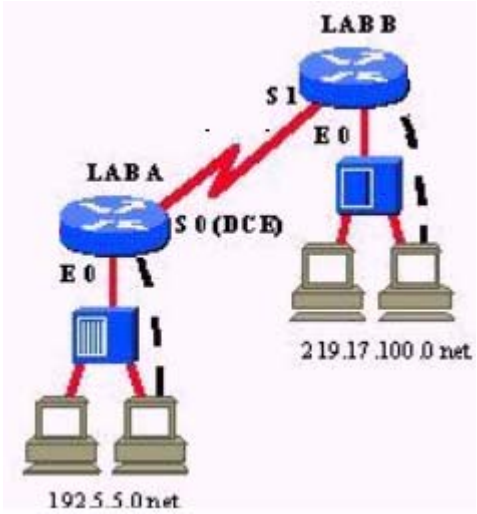
## 1.6. RECOMENDACIONES

## 1.7. CONCLUSIONES

## 1.8. BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

**Figura 15. Conexión entre dos redes LAN**



# ANEXO B. LABORATORIO 2: CONFIGURACIÓN DE LA TOPOLOGÍA DEL SEMESTRE DOS DE CISCO

## 1. GUÍA DE LABORATORIO

### 1.1 OBJETIVOS:

- Configurar el equipo de laboratorio de Cisco de acuerdo con el diagrama de topología del Semestre 2 o analizar las conexiones físicas de una configuración de laboratorio existente.
- Documentar el cableado y las conexiones entre los dispositivos.
- Analizar los routers en una configuración de laboratorio existente y documentar la configuración de IOS.
- Utilizar el comando show running-config en cada router para determinar los números de red IP conectados, las interfaces, las direcciones IP y la información de la máscara de subred para las redes de área local (LAN) y las redes de área amplia (WAN) que están en uso.
- Utilizar el icono del Panel de control / Red o la utilidad winipcfg.exe en cada estación de trabajo para determinar las configuraciones 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.

## 1.2 EQUIPO UTILIZADO

- 5 estaciones de trabajo de PC 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 seriales 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 CAT 6 de conexión directa para conectar los routers y estaciones de trabajo con hubs y switches.

## 1.3 MARCO TEÓRICO

Esta práctica de laboratorio muestra la forma en que los routers de laboratorio de Cisco se configuran y conectan para la topología del Semestre 2 (ver figura 16).

Dicha configuración está 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. Luego, en la segunda parte, se realizará la configuración de routers y estaciones de trabajo para cumplir con la topología mostrada en la figura 16. Se utilizarán los comandos de IOS para examinar y documentar las configuraciones de red IP de cada router. También verificará la configuración IP de cada estación de trabajo para asegurarse de que existe conectividad entre todos los nodos en la configuración de laboratorio.

La topología de laboratorio del Semestre 2 muestra una WAN corporativa para una empresa de tamaño mediano con filiales en todo el mundo. No se encuentra conectada a Internet: es la red privada de la empresa. Esta topología no es redundante: si falla cualquier router dentro de la cadena, la red dejará de funcionar. Esta red que se encuentra bajo una administración común (la empresa) se denomina sistema autónomo.

El protocolo enrutado es el conocido IP. El protocolo de enrutamiento es el Protocolo de Gateway Fronterizo (BGP) usado ampliamente entre los routers de Internet.

Cada uno de los routers se conecta a una LAN de oficina o campus. Las conexiones desde A-B, B-C y C-D son líneas T1 arrendadas conectadas a las interfaces seriales del router.

Cada router tiene una LAN Ethernet conectada a él. En cada LAN aparecen hosts junto con sus cables de consola para permitir la configuración y visualización del contenido de los routers.

## 1.4 PROCEDIMIENTO

### 1.4.1 Implementación de la topología del segundo semestre.

- Implementar la red mostrada en la figura 16. El equipo se debe colocar de modo tal que todas las interfaces estén orientadas en la misma dirección y que se pueda acceder con facilidad al cableado y a las conexiones. Si la configuración de routers se realiza sobre mesas o escritorios, se deben colocar los routers en orden uno al lado del otro. Se puede colocar los switches y hubs sobre los respectivos routers para evitar confusiones.

- Ahora, se deben 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 terminación de circuito 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 extremos y un conector DB60 en el otro extremo, que se conecta a la interfaz serial del router.

- Ahora, se deben examinar los cables y las conexiones de los routers y completar la siguiente tabla:

**Tabla 1.**

| **Desde** | **Interfaz** | **Hacia: Nombre del router** | **Interfaz** |
|---|---|---|---|
| Lab_A | | | |
| Lab_B | | | |
| Lab_C | | | |
| Lab_D | | | |
| Lab_E | | | |

- A continuación, se debe conectar el cableado Ethernet como indoica la figura 16. Completar en la siguiente tabla cuáles son las interfaces Ethernet del router que están en uso y a qué hub (o switch) están conectadas:

**Tabla 2.**

| Desde | Interfaz del router | Hacia qué dispositivo Ethernet |
|---|---|---|
| Lab_A | | |
| Lab_B | | |
| Lab_C | | |
| Lab_D | | |
| Lab_E | | |

- Ahora, debe realizarse el cableado Ethernet de cada estación de trabajo. Se debe conectar al menos una estación de trabajo a cada hub o switch y en la tabla indicada se debe registrar el dispositivo al que se conecta cada PC:

**Tabla 3.**

| Desde la estación de trabajo | Hacia qué dispositivo Ethernet |
|---|---|
| PC1 | |
| PC2 | |
| PC3 | |
| PC4 | |
| PC5 | |
| PC6 | |
| PC/ | |
| PC8 | |
| PC9 | |
| PC10 | |

- El paso siguiente es realizar la conexión de las estaciones de trabajo de consola con los routers. Para ello, se debe conectar uno de los extremos de los cables rollover desde las estaciones de trabajo asignadas a la interfaz de consola de los routers Lab-A, B, C, D y E. Luego, conectar el otro extremo de cada uno de los cables rollover a un conector serial RJ-45-a-DB-9. Después, se debe conectar el conector serial a los puertos seriales de las 5 estaciones de trabajo. Finalmente, se conectan los cables de alimentación a todos los dispositivos y se encienden los equipos verificando que todos estén activados observando las luces indicadoras.

### 1.4.2 Configuración de la topología del segundo semestre

- Primero, se deben examinar y documentar las configuraciones del router.
- Luego, hay que conectarse al primer router Lab-A. Iniciando el programa HyperTerminal **(Inicio/Programas/Accesorios/Comunicación)**. Se escribe la contraseña **cisco** si se debe entrar al modo usuario. El indicador debe ser **Lab-A>**
- Después, se entra al modo Exec privilegiado. Se escribe **enable** cuando aparezca el indicador del router. Luego, se escribe la contraseña class o la que se haya asignado anteriormente. Ahora el indicador debe ser Lab-A# C.
- Tomar nota de de las interfaces (E0, S0 etc.) que aparecen. Ahora, se escribe el comando **show running-config** para obtener información. El router

responde mostrando el archivo de configuración activo ubicado actualmente en la RAM. Se debe completar la siguiente tabla con la información de interfaz IP para cada uno de los cinco routers.

**Tabla 4.**

| **Nombre del router** | **Lab_A** | **Lab_B** | **Lab_C** | **Lab_D** | **Lab_E** |
|---|---|---|---|---|---|
| **Número del modelo** | | | | | |
| **Dirección IP de la interfaz EO** | | | | | |
| **Máscara de subred de la interfaz EO** | | | | | |
| **Dirección IP de la interfaz E1** | | | | | |
| **Máscara de subred de la interfaz E1** | | | | | |
| **Máscara de subred de la interfaz S0** | | | | | |
| **Velocidad de temporización de la interfaz S0** | | | | | |
| **Dirección IP de la interfaz S1** | | | | | |
| **Máscara de subred de la interfaz S1** | | | | | |
| **Otra(s) interfaz (interfaces)** | | | | | |

- Con la información obtenida mediante el comando show running-config en el router Lab-A, se deben contestar las siguientes preguntas:

  a. ¿Cuál es el protocolo de enrutamiento utilizado?
  b. ¿Cuáles son las redes que están conectadas directamente a las interfaces?
  c. ¿Cuál es la velocidad de temporización de la interfaz S0 en el router Lab-A?
  d. ¿Cuál es la contraseña para las líneas Telnet VTY 0 a 4?

- El siguiente paso es examinar y documentar las configuraciones de las estaciones de trabajo. Para ello, se siguen los siguientes pasos:

  1. Verificar la configuración IP de la estación de trabajo haciendo clic en **Inicio/Configuración** y seleccionando **Panel de control**.
  2. Hacer doble clic en el icono **Red**.
  3. Escoger el protocolo TCP/IP y hacer clic en el botón **Propiedades.**
  4. Para cada estación de trabajo, se debe hacer clic en la ficha Dirección IP y registrar los valores actuales para la dirección IP y máscara de subred en la tabla 5.
  5. Hacer clic en la ficha **Gateway** y registre la dirección IP del gateway por defecto en la tabla: (debe ser la dirección IP de la interfaz del router E0 a la que está conectado el hub para cada estación de trabajo). También se

puede ejecutar la utilidad winipcfg.exe del indicador de comando de DOS para verificar la configuración de cada estación de trabajo.

- Con la información que se obtuvo de cada estación de trabajo, completar la configuración IP.

**Tabla 5.**

| Nro. de estación de trabajo | Dirección IP de la estación de trabajo | Máscara de subred | Dirección IP del gateway por defecto |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

- Ahora, es necesario probar la conectividad de los routers del laboratorio. Para ello, se utiliza el comando ping. Se comenzará con router Lab-A utilizando la conexión de la estación de trabajo de consola para ello. Se debe inciar el programa HyperTerminal y hacer ping a la interfaz S1 del router Lab-B. Esto permite verificar si el enlace WAN entre Lab-A y Lab-B es correcto. Luego, se hará ping a las interfaces seriales de los demás routers. Verificar si el ping realizado tuvo éxito.
- Finalmente, se hará ping de una estación de trabajo al router. Para lograrlo, se debe hacer clic en **Inicio/Programas/MS-DOS** y hacer 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. Terminar la práctica de laboratorio haciendo ping en las interfaces seriales de los demás routers y verificando si hubo éxito en este último paso.

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

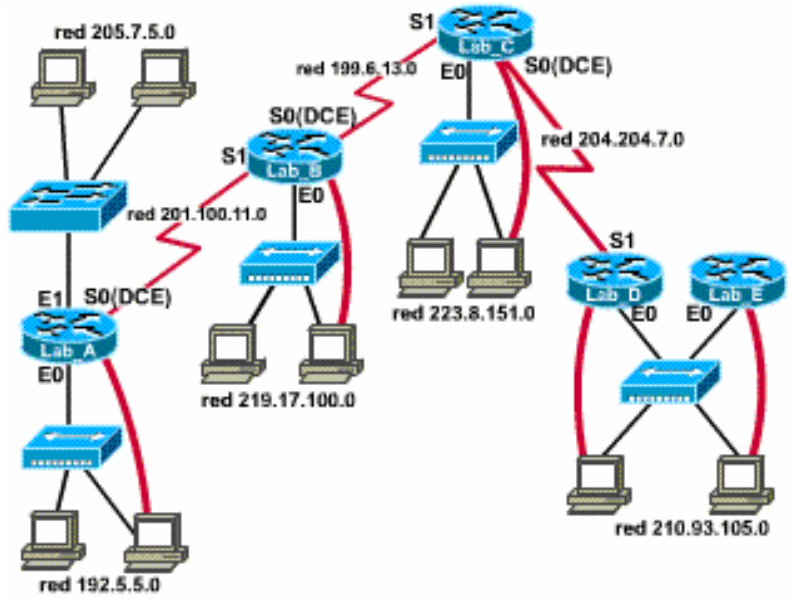
## 1.7CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

**Figura 16. Topología del Segundo Semestre de Cisco. Red a implementar(a) e información de la topología (b)**

**(a)**




**(b)**

| Router | E0 | E1 | S0 | S1 |
|---|---|---|---|---|
| Lab_A | 192.5.5.1 | 205.7.5.1 | 201.100.11.1 | ---------- |
| Lab_B | 219.17.100.1 | ---------- | 199.6.13.1 | 201.100.11.2 |
| Lab_C | 223.5.151.1 | ---------- | 204.204.7.1 | 199.6.13.2 |
| Lab_D | 210.93.105.1 | ---------- | ---------- | 204.204.7.2 |
| Lab_E | 210.93.105.2 | ---------- | ---------- | ---------- |

Enable password para los routers: **class**

Vty password para los routers: **cisco**

SM para los routers: **255.255.255.0**

# ANEXO C. LABORATORIO 3: INTERFAZ DEL USUARIO DEL ROUTER

## 1. GUÍA DE LABORATORIO

### 1.1 OBJETIVOS

- Conectarse al router en modo usuario y en modo privilegiado.
- Utilizar varios comandos básicos del router para determinar cómo se configura el router.
- Familiarizarse con la función HELP del router.
- Usar las funciones de historial de comandos y de edición
- Desconectarse del router.

### 1.2 EQUIPO UTILIZADO

- PC con monitor, teclado, ratón y cables de alimentación.
- Sistema operativo Windows (Win 95, 98, NT o 2000) instalado en el PC.
- Programa HyperTerminal configurado para acceder a la consola del router.
- PC conectado al puerto de consola del router mediante un cable rollover.

## 1.3 MARCO TEÓRICO

Esta práctica de laboratorio presenta la interfaz del usuario de línea de comando del Sistema Operativo de Internetwork (IOS) de Cisco. A través de ello, se iniciará el proceso de conexión al router y utilización de diferentes niveles de acceso para introducir comandos en "Modo usuario" y "Modo privilegiado". También se usará la función HELP, de historial y de edición. La interfaz de comandos del IOS es el método más común para configurar un router de Cisco. Allí se podrán observar ua gran variedad de comandos disponibles, especialmente en el modo privilegiado.

## 1.4 PROCEDIMIENTO

- Primero, hay que conectarse al router e introducir la contraseña cisco si se solicita. Anotar el indicador del router y su significado.
- Ahora, se debe introducir el comando help (ayuda) escribiendo (?) en el indicador del router. Alli se muestran todos los comandos disponibles para el Modo Usuario. Escribir ocho (8) comandos disponibles que aparecen en la respuesta del router.
- Luego, en el modo EXEC usuario, se debe entrar al modo privilegiado utilizando el comando **enable.** Ahora, se digita la contraseña enable (class) para entrar al modo privilegiado. Anotar el indicador del router y su significado.

- Ahora, se debe introducir el comando help escribiendo (?) en el indicador del router. Alli se muestran todos los comandos disponibles para el Modo Privilegiado. Anotar diez (10) comandos disponibles que aparecen en la respuesta del router.
- Luego, se observarán los comandos show introduciendo la palabra **show** seguida de un espacio y luego un signo (?). Aquí se verán los subcomandos disponibles para el comando show. ¿El comando "running-config" es uno de los comandos disponibles para este nivel de usuario?
- El paso siguiente es observar la configuración actual del router. Para ello, se debe introducir el comando **show running-config** en el indicador del router. Aquí se visualiza el archivo de configuración activo para el router que se guarda en la RAM. Anotar los 6 datos claves que se pueden obtener a través de este comando.
- Si aparece la palabra **more** (más), se debe presionar la barra espaciadora para que el router siga mostrando la siguiente página de información.
- Ahora se verificará el historial de comandos. Se debe presionar la tecla flecha arriba o (Control-P). Con ello, se puede revisar el historial de comandos. ¿Qué sucedió en el indicador del router?
- Finalmente, se debe introducir el comando **exit** (salir) en el indicador del router para terminar.

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

# ANEXO D. LABORATORIO 4: MODOS DE LA INTERFAZ DE USUARIO DEL ROUTER

## 1. GUÍA DE LABORATORIO

### 1.1 OBJETIVOS

- Identificar los seis modos de router básicos y los dos modos de router opcionales
- Familiarizarse con el indicador del router para cada modo
- Utilizar varios comandos para entrar en modos específicos

### 1.3 EQUIPO UTILIZADO

- PC con monitor, teclado, ratón y cables de alimentación, etc.
- Sistema operativo Windows (Win 95, 98, NT o 2000) instalado en el PC
- Programa HyperTerminal PE configurado para acceder a la consola del router
- PC conectado al puerto de consola del router mediante un cable rollover

## 1.3 MARCO TEÓRICO

Al utilizar sistemas operativos del router, como Cisco IOS, es necesario conocer cada uno de los distintos modos usuario de un router y cuál es la función de cada uno de ellos. Existen seis modos principales disponibles para la mayoría de los routers:

- Modo EXEC usuario
- Modo EXEC privilegiado (también denominado modo Enable)
- Modo de configuración global
- Modo de configuración del router
- Modo de configuración de interfaz
- Modo de configuración de subinterfaz

Los otros dos modos que se utilizan menos frecuentemente son modo RXBoot y modo de configuración inicial (setup). RXBoot es un modo de mantenimiento que se puede utilizar para la recuperación de contraseñas. El modo de configuración inicial (setup) presenta un diálogo interactivo basado en indicadores que ayuda al nuevo usuario a crear una configuración básica inicial.

Cada vez que el router muestra un modo, el indicador es distinto. Según el modo en que se encuentra el router, algunos comandos pueden estar disponibles o no.

Para saber cuáles de los comandos se pueden utilizar se escribe un signo de interrogación (?).

## 1.4 PROCEDIMIENTO

- Para empezar la práctica se debe tratar de averiguar cuáles son los modos y qué función cumple cada uno de ellos. Se debe tomar nota del aspecto que tienen los indicadores del router en cada uno de los modos y completar la tabla escribiendo el indicador adecuado seleccionándolo en la lista de opciones que se suministra a continuación:

**Tabla 1.**

| Descripción del modo | Indicadores del modo |
|---|---|
| 1. Modo EXEC usuario . | |
| 2. Modo EXEC privilegiado | |
| 3. Modo de configuración global | |
| 4. Modo de configuración del router | |
| 5. Modo de configuración de interfaz | |

A. Router #

B. Router>

C. Router(config-if) #

D. Router(config-router) #

E. Router(config) #

- Ahora se debe indicar la función de cada uno de los modos del router completando la siguiente tabla escribiendo la letra correspondiente a la opción correcta que se suministra a continuación:

**Tabla 2.**

| Descripción del modo | Indicadores del modo |
|---|---|
| 1. Modo EXEC usuario . | |
| 2. Modo EXEC privilegiado | |
| 3. Modo de configuración global | |
| 4. Modo de configuración del router | |
| 5. Modo de configuración de interfaz | |

A. Examen detallado del router, depuración y prueba. Acceso remoto.

B. Configuración de las direcciones IP y máscaras de subred.

C. Comandos de configuración simple.

D. Examen limitado del router. Acceso remoto.

E. Protocolos de enrutamiento.

- A continuación, se debe escribir un comando que permita entrar al modo que se solicita, después del indicador correspondiente:

**Tabla 3.**

| Modo deseado | Indicador actual | Comando | Explicación |
|---|---|---|---|
| **Modo EXEC privilegiado** | **Router>** | | |
| **Modo de configuración global** | **Router#** | | |
| **Modo de configuración de interfaz** | **Router (config.)#** | | |
| **Modo de configuración del router** | **Router (config.)#** | | |

- Finalmente, se debe describir cuál es la función general de los siguientes modos:

1. Configuración de interfaz
2. Modo Enable

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

# ANEXO E. LABORATORIO 5: ACCESO A TELNET REMOTO

## 1. GUÍA DE LABORATORIO

### 1.1 OBJETIVOS:

- Utilizar el comando telnet para acceder a otros routers de forma remota.
- Verificar que la capa de aplicación entre el origen y el destino funcione correctamente.
- Recuperar información acerca de routers remotos utilizando los comandos show del router.

### 1.2 EQUIPO UTILIZADO

- PC con el sistema operativo Windows e HyperTerminal instalados.
- Router conectado al PC mediante un cable rollover de consola
- Por lo menos 3 routers interconectados mediante cables de simulación de WAN o Ethernet

### 1.3 MARCO TEÓRICO

La función telnet (terminal remota) se utiliza para acceder a los routers de forma remota. En esta práctica, se hará telnet desde el router local hasta otro router "remoto" para simular que está en la consola del router remoto. Este procedimiento utilizará el software de cliente Telnet del router y el software de servidor Telnet del router remoto. También se puede hacer "telnet" desde la estación de trabajo como cliente hacia cualquier router conectado con la red. Además, puede se puede hacer telnet a los switches Ethernet de Cisco. Sin embargo, no se puede hacer telnet desde un router o una estación de trabajo hacia otro servidor o cliente Windows porque el sistema operativo Windows no reconoce el daemon de servidor Telnet. Un daemon es un término de UNIX que se refiere a un programa que se ejecuta en un servidor que acepta peticiones de servicios. Usted puede decidir si permite que las otras personas hagan telnet hacia su router o puede solicitar una contraseña para las sesiones Telnet entrantes. Las conexiones Telnet se denominan line VTY 0 4 en el archivo de configuración del router. El router admite hasta 5 sesiones Telnet entrantes simultáneas (0 a 4).

Telnet es una buena herramienta de diagnóstico de fallas porque se puede utilizar para acceder a los routers remotos para obtener información cuando existen problemas o cuando es necesario realizar cambios en la configuración. También prueba la capa de aplicación OSI del host origen hacia la capa física y luego a través de la red y de nuevo hacia las capas superiores de la pila de protocolo del

router destino. Esto le permite verificar el software de capa de aplicación entre los hosts origen y destino.

## 1.4 PROCEDIMIENTO

- Conectarse al router introducir la contraseña si se solicita. ¿Qué indicador mostró el router?
- Luego, se debe introducir telnet en el indicador del router. Aquí, el router muestra la ayuda del comando telnet. ¿Cuál fue la respuesta del router?
- Ahora, se introduce telnet "nombre del router" o dirección IP en el indicador del router para conectarse a un router remoto. En este momento, el router pide la Verificación de acceso de usuario del router al que accede de forma remota. Introducir la contraseña cisco. ¿Qué indicador mostró el router?
- Introducir el comando **show interface** en el indicador del router para ver información acerca de las interfaces. Anotar en la siguiente tabla las interfaces, su dirección IP y su máscara de subred.

**Tabla 1.**

| Interfaz | Dirección IP | Máscara de subred |
|---|---|---|
| | | |
| | | |

- Introducir el comando **show protocols** en el indicador del router para observar el estado global y específico para la interfaz de cualquiera de los protocolos configurados de capa 3. Anotar la interfaz y responder las siguientes preguntas basándose en la información obtenida por el router al que se accede de forma remota:

    1. Hay una señal de detección de portadora?
    2. Se reciben los mensajes de actividad?

- Entrar al modo privilegiado con telnet mientras se mantiene conexión con el router remoto. Luego, colocar enable para entrar al modo EXEC privilegiado y escribir la contraseña class. ¿Qué indicador mostró el router? ¿En qué modo está el router?
- Introducir el comando **show running-config** en el indicador del router remoto para observar la información sobre la configuración actual. ¿Cuál es el archivo que se visualiza en el router remoto? ¿Dónde está guardado el archivo?
- Introducir el comando **show startup-config** en el indicador del router con el fin de ver la información sobre la copia de respaldo del archivo de configuración almacenada en la NVRAM. Responder las siguientes preguntas:

    1. ¿Cuál es el archivo que se visualiza en el router remoto? ¿Dónde está guardado el archivo?

2. ¿Cuál es la información que se visualiza con respecto a las conexiones VTY de línea?

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

# ANEXO F. LABORATORIO 6: COMANDO PING

## 1. GUÍA DE LABORATORIO

### 1.1 OBJETIVOS

- Usar el comando ping para enviar datagramas ICMP al host objetivo.
- Verificar que la capa de red entre el origen y el destino funcione correctamente.
- Capturar información para evaluar la confiabilidad de la ruta hacia el host.
- Determinar los retardos a lo largo de la ruta y si el host se puede alcanzar o si está en funcionamiento.

### 1.2 EQUIPO UTILIZADO

- PC con el sistema operativo Windows e HyperTerminal instalados.
- Router conectado al PC mediante un cable rollover de consola
- Por lo menos 3 routers interconectados mediante cables de simulación de WAN o Ethernet

## 1.3 MARCO TEÓRICO

Protocolo de Mensajes de Control de Internet (ICMP) le otorga al router la capacidad para diagnosticar la conectividad de red básica. Al usar ping xxx.xxx.xxx.xxx se envía un paquete ICMP al host especificado y luego se espera un paquete de respuesta de ese host. Se puede hacer ping al nombre de host de un router pero se debe tener una tabla de consulta de hosts estática en el router o en el servidor DNS para la resolución de nombres a direcciones IP.

Ping es una excelente herramienta para diagnosticar las fallas de la capa 1 a 3 del modelo OSI. Si no es posible conectarse a un computador host (tal como un servidor) se puede hacer ping a la dirección IP del servidor, entonces el problema probablemente no se relacione con las conexiones de cableado físico, las NIC o los routers que se encuentran entre la terminal y el servidor. A través de esta práctica de laboratorio se podrán notar las diferencias que existen entre el uso del comando ping desde un router y desde una estación de trabajo.

## 1.4 PROCEDIMIENTO

- Conectarse al router e introducir la contraseña cisco si se solicita. ¿Qué indicador mostró el router? ¿Qué significa?

- Introducir el comando **show host** en el indicador del router para observar la información acerca de asignaciones de hosts a direcciones de capa 3 (IP), de qué manera esta información se adquirió y la antigüedad de la entrada? Enumerar cuatro (4) nombres de host y la primera dirección IP que corresponde a cada uno de estos nombres de host.

**Tabla 1.**

| Nombre de host | Dirección IP |
|---|---|
| | |
| | |
| | |
| | |

- Introducir el comando ping xxx.xxx.xxx.xxx donde xxx.xxx.xxx.xxx es la dirección IP de uno de los demás hosts enumerados anteriormente. Se debe repetir el proceso con todas las direcciones IP enumeradas. En este paso, el router envía un paquete ICMP para verificar la conexión de hardware y la dirección de la capa de red. Como el PC está actuando como consola del router, está haciendo ping de un router a otro. Enumerar cuatro (4) datos importantes que se hayan recibido de vuelta tras la emisión del comando ping .
- Observar el ejemplo del ejemplo del comando ping generado por un router.

lab-b#ping 210.93.105.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echoes to 210.93.105.1, timeout is 2 seconds: !!!.!

Success rate is 80 percent (4/5), round-trip min/avg/max = 68/68/168 ms

1. ¿Qué indica el signo de exclamación (!)?
2. ¿Qué indica el punto (.)?
3. ¿Qué prueba el comando ping ?

- Hacer click en **Inicio/Programas/MS DOS** desde una estación de trabajo. Esto abrirá una ventana de indicadores de comando, en la cual, se puede hacer ping a los routers y probar que la pila TCP/IP y el gateway por defecto de la estación de trabajo están configurados y funcionan correctamente.
- Introducir ping y la dirección IP del gateway por defecto de la estación de trabajo en el indicador de comando. El gateway por defecto es la dirección IP de la interfaz del router más cercano. Al hacer ping al gateway por defecto se podrá controlar si puede enviar con éxito paquetes desde y hacia el router que se encuentra directamente conectado a la red LAN.
- Introducir ping y la dirección IP del router remoto en el indicador de comando. Esto permite probar la conectividad de capa 3 entre la estación de trabajo y el router remoto. ¿El resultado del comando ping desde la estación de trabajo es el mismo que el del comando ping desde un router?
- Introducir ping y la dirección IP de otro router remoto en el indicador de comando. Esto permite probar la conectividad de capa 3 entre la estación de

trabajo y los otros routers remotos. Enumerar las diferencias que existen entre el comando ping del router y el comando ping de la estación de trabajo.

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7 CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

# ANEXO G. LABORATORIO 7: COMANDO TRACEROUTE

## 1. GUÍA DE LABORATORIO

### 1.1 OBJETIVOS

- Usar el comando traceroute de Cisco IOS desde el router origen al router destino.
- Usar el comando tracert del Sistema Operativo de Windows desde la estación de trabajo origen al router destino.
- Usar el comando show ip route para mostrar la tabla de enrutamiento del router.
- 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.

## 1.2 EQUIPO UTILIZADO

- PC con monitor, teclado, ratón y cables de alimentación, etc.
- Sistema operativo Windows (Win 95, 98, NT o 2000) instalado en el PC
- Programa HyperTerminal
- Acceso a múltiples routers

## 1.3 MARCO TEÓRICO

El comando traceroute utiliza paquetes ICMP y el mensaje de error generado por los routers cuando el paquete supera su Tiempo de Existencia (TTL). Al iniciar el comando trace 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 envía entonces un mensaje de tiempo excedido ICMP de vuelta al origen. El router origen envía entonces un paquete de petición de eco ICMP con el TTL establecido en dos (2). El primer router recibe la petición de eco de 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 cero (0) luego, envía un mensaje de tiempo excedido ICMP de vuelta al origen. El origen envía entonces una petición de 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 de 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 diagnóstico de fallas denominada aislamiento de fallas.

## 1.4 PROCEDIMIENTO

- Conectarse al router e introducir la contraseña cisco si se solicita. ¿Qué indicador mostró el router? ¿Qué significa?
- Introducir el comando trace en el indicador del router. ¿Cuál fue la respuesta del router? Una vez se ha introducido el comando trace, se debe presionar <intro> dos veces para volver a la línea de comando.
- Introducir el comando trace ? en el indicador del router. ¿Cuál fue la respuesta del router?
- Introducir el comando trace ip ? en el indicador del router. ¿Cuál fue la respuesta del router?
- Introducir el comando trace ip xxx.xxx.xxx.xxx donde xxx.xxx.xxx.xxx es la dirección IP del destino objetivo. Esto se realiza para averiguar a dónde se envían los datos en la red. Se recomienda realizar esta práctica de laboratorio utilizando uno de los routers extremos y hacer trace IP al otro router extremo. (ip es la opción por defecto). Enumerar los nombres de host y direcciones IP de los routers a través de los cuales se enrutó el paquete ICMP.

**Tabla 1.**

| Nombre de host | Dirección IP |
|---|---|
| | |
| | |
| | |

- Repitir el paso anterior con todos los demás routers de la red.
- Ahora, hacer click en Inicio/Programas/MS DOS desde la estación de trabajo de la consola. Alli, se abre una ventana de indicador de comando MS-DOS. Al usar esta ventana se estará usando la pila TCP/IP de la estación de trabajo para empezar el rastreo hacia el destino. El primer salto será el gateway por defecto o la interfaz del router más cercana en la LAN a la cual está conectada la estación de trabajo.
- Introducir tracert y la misma dirección IP que utilizó en el primer router. Indicar en la siguiente tabla el nombre de host y dirección IP del router a través del cual se enrutó el paquete ICMP.

**Tabla 2.**

| Nombre de host | Dirección IP |
|---|---|
| | |
| | |
| | |

¿Por qué existe una entrada más en el resultado del comando tracert cuando se realiza el rastreo desde el indicador de comando del computador al host objetivo?

- Hacer click en Inicio/Programas/MS DOS desde una estación de trabajo que tenga acceso a Internet. Allí, se abre una ventana de comandos de MS-DOS. Introducir tracert www.cisco.com. Responder las siguientes preguntas:

  1. ¿Cuál es la dirección IP de www.cisco.com?
  2. ¿Cuantos saltos hacen falta para llegar a www.cisco.com? Si un paquete pasa a través de un router esto se considera como un (1) salto y el TTL del paquete decrece de a uno (1).

- Introducir show ip route desde el indicador del router. Esto mostrará la tabla de enrutamiento del router. Indicar las direcciones con número de red IP directamente conectadas al equipo.

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7 CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

# ANEXO H. LABORATORIO 8: CONFIGURACIÓN DEL ROUTER CON HYPERTERMINAL

## 1. GUÍA DE LABORATORIO

### 1.1 OBJETIVOS

- Capturar la configuración activa de un router en un archivo de texto ASCII, utilizando HyperTerminal
- Editar o modificar el archivo de texto capturado con un editor de texto tal como el Bloc de notas de Windows
- Cargar el archivo de texto para configurar otro router usando HyperTerminal

### 1.2 EQUIPO UTILIZADO

- PC con monitor, teclado, ratón y cables de alimentación, etc.
- Sistema operativo Windows (Win 95, 98, NT o 2000) instalado en el PC
- Programa HyperTerminal PE configurado para acceder a la consola del router
- PC conectada al puerto de consola del router mediante un cable rollover

## 1.3 MARCO TEÓRICO

HyperTerminal es utilizado para capturar y cargar una configuración del router como un archivo de texto ASCII. Esta copia guardada se puede usar como copia de respaldo para el router actual o como base para la configuración de un nuevo router. Cuando se agrega un nuevo router a una red, resulta útil basar la nueva configuración en una ya existente.

Se prefiere el uso del Bloc de notas de Windows para editar el texto. WordPad y otros procesadores de texto que poseen funciones de texto enriquecido necesitan que utilice la función 'guardar como', con la opción 'documento de texto'. Esto NO es necesario si usa el Bloc de notas debido a que NO adjunta encabezados de formateo, mientras que la mayoría de los demás procesadores de texto lo hacen. La adición de estos encabezados daña el archivo de configuración. Como cada router puede tener distintas interfaces, debe analizar la configuración del router capturado y modificarlo para que se adecue a la nueva configuración. Además, las direcciones IP asignadas a las interfaces en el nuevo router deben ser distintas de las del router original.

## 1.4 PROCEDIMIENTO

- Conectarse al router e introducir la contraseña cisco si se solicita.

- Desde el modo EXEC usuario, entrar al modo EXEC privilegiado utilizando el comando enable. introducir la contraseña enable class. Luego, digitar el comando **show running-config.** Aquí se muestra el archivo de configuración activo para el router que se encuentra almacenado en la RAM. Enumerar todas las interfaces del router.
- Iniciar el proceso de copia de la configuración del router en un archivo de texto con ayuda de HyperTerminal. Aquí se captura todo el texto que aparece en la pantalla en un archivo de texto. Estando en HyperTerminal, hacer clic en la opción del menú **Transfer** (Transferencia), luego hacer clic en **Capture text** (Capturar texto). Cuando se solicite, proporcionar la ruta y el nombre de la ubicación donde se debe capturar la configuración. Usar el nombre del router como nombre de archivo y usar .txt como extensión.
- Introducir el comando **show running-config** en el indicador de comando. Este comando muestra el archivo de configuración activo para el router que se encuentra almacenado en la RAM.
- Detener la captura del archivo de la configuración del router en un archivo de texto. En este instate, HyperTerminal dejará de capturar el texto que aparece en pantalla. En HyperTerminal, hacer clic en la opción del menú **Transfer** (Transferencia), luego hacer clic en **Capture text** (Capturar texto). Aparece un nuevo menú. Hacer clic en **Stop** (Detener).
- Eliminar cualquier información innecesaria de la configuración capturada. Como, por ejemplo, los indicadores **more**. Luego, hacer clic en el botón **Inicio**

de Windows, hacer clic en **Ejecutar** y escriba **Notepad** y presione la tecla **Intro**. En el Bloc de notas, hacer clic en **Archivo/Abrir**. Buscar el archivo que se indicó en el paso anterior y hacer clic en **Abrir**. Borre las líneas innecesarias. Guardar la versión limpia de la configuración haciendo clic en **Archivo/Guardar**. Cerrar Bloc de notas (**Archivo/Cerrar**) y vuelver a HyperTerminal.

- Entrar el comando **erase startup-config** en el indicador del router. Esto es para eliminar el archivo de configuración en la NVRAM.
- Introducir el comando **show startup-config** en el indicador del router. Este paso muestra que la configuración inicial del router no estará disponible al reiniciar el router. ¿Qué muestra el router al introducir este comando?
- Entrar el comando **reload** en el indicador del router. Dicho comando reiniciará al router. Cuando se solicite continuar con la recarga, digitar **Y** y presionar la tecla **Intro**. Se puede notar que el router muestra el mensaje: "Notice: NVRAM invalid, possibly due to write erase." Cuando se solicite entrar al diálogo de configuración inicial, se debe escribir **N** y presionar **Intro**. Cuando se solicite terminar la instalación automática escribir **Y** y presionar **Intro**. Presionar Intro nuevamente. ¿Qué aspecto tiene el indicador?
- Utilizar el comando **send file** en HyperTerminal para copiar la nueva configuración en el área de la memoria denominada portapapeles. En HyperTerminal, se escribe el comando **enable** para pasar al modo EXEC privilegiado. ¿Por qué no se necesita contraseña?

- Entrar al modo de configuración global introduciendo el **comando configure terminal**. Hacer clic en **Transfer/Send/Text File** (Transferencia/Enviar/Archivo de Texto). Seleccionar el archivo que guardó previamente. Responder las siguientes preguntas:

  1. ¿Qué cambió en el indicador del router?
  2. ¿Qué comando cambia el indicador del router?

- Presionar y mantener presionada la tecla **Control** luego presionar la **tecla Z** para salir del modo de configuración global.
- Usar el comando **copy running-config startup-config** para guardar la configuración creada del router. Este comando copia la configuración activa del router desde la RAM en la NVRAM.
- Verificar que la configuración sea correcta utilizando el comando **show running-config**. Introducir el comando **copy start run** en el indicador del router.
- Utilizar el comando **reload** para reiniciar el router. Aquí se verificará que la nueva configuración se haya guardado en la NVRAM reiniciando el router. Cuando se solicite que confirmar se presiona **Y**, para reiniciar el router. Una vez que el router reinicie, presionar nuevamente la tecla **Intro**.

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7 CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

# ANEXO I. LABORATORIO 9: CONFIGURACIÓN DEL ROUTER USANDO TFTP

## 1. GUÍA DE LABORATTORIO

### 1.1 OBJETIVOS

- Copiar un archivo de configuración del router en un servidor TFTP.
- Configurar un router desde un servidor TFTP.

### 1.2 EQUIPO UTILIZADO

- PC con monitor, teclado, ratón y cables de alimentación, etc.
- Sistema operativo Windows (Win 95, 98, NT o 2000) instalado en el PC
- Programa HyperTerminal configurado para acceder a la consola del router
- PC conectado al puerto de consola del router mediante un cable rollover
- TFTP instalado y operativo en una estación de trabajo accesible desde el router en el cual está trabajando.

## 1.3 MARCO TEÓRICO

Un servidor TFTP (Protocolo trivial de transferencia de archivos) se utiliza para guardar una copia del archivo de configuración del router. También se puede configurar el router desde el servidor TFTP. El uso de un servidor TFTP es una excelente forma de mantener copias de seguridad de archivos de configuración para routers y otros equipos de red, tales como los switches. Además, las imágenes del IOS se pueden almacenar en un servidor TFTP. Este servidor es más sencillo de utilizar que un servidor FTP estándar. TFTP no necesita que el usuario tenga una contraseña o que navegue entre directorios. Por esta razón, es importante que el servidor TFTP sea seguro (es decir, no disponible al público en general). TFTP usa UDP en lugar de TCP como cualquier servidor FTP estándar. TFTP es una utilidad de transferencia de archivos muy básica y no requiere servicios de entrega garantizada de TCP. El "servidor" TFTP puede ser un servidor de archivos, una estación de trabajo o incluso un router Cisco y debe tener la utilidad TFTP instalada y operativa.

## 1.4 PROCEDIMIENTO

- Conectarse al router. Introducir la contraseña cisco si se solicita.
- Entrar al modo privilegiado utilizando el comando **enable.** Introducir la contraseña **enable class.**

- Verificar la conectividad al servidor TFTP entrando ping xxx.xxx.xxx.xxx (la dirección IP de la estación de trabajo que ejecuta el servidor TFTP). Esto es para saber que se puede alcanzar el servidor TFTP desde el router.
- Si no se logró hacerlo, habrá que verificar las conexiones y luego verificar las configuraciones de los routers en el laboratorio para asegurarse de que se pueda alcanzar el servidor TFTP. Verificar que la estación de trabajo tenga el servidor TFTP instalado y que esté operando.
- Introducir el comando **copy running-config tftp** e iniciar el proceso de copia de la configuración actual del router en el servidor TFTP. Cuando se solicite el host remoto, introducir la dirección IP que se verificó anteriormente y presionar **Intro**. Cuando se solicite el archivo de configuración que se debe leer, la opción por defecto es el nombre del router, seguido por un guión y la palabra confg (por ej., LAB-A-confg). Aceptar este nombre presionando **Intro**, o escribir un nuevo nombre y presionar **Intro**. ¿Cuál es el nombre del archivo de configuración que se está escribiendo en el servidor TFTP?
- Confirmar la escritura del archivo de configuración en el servidor TFTP presionando **Intro**. Alli aparecen signos de exclamación en la pantalla, que muestran la marcha del proceso de copia de archivos TFTP.
- Introducir el comando **erase startup-config** en el indicador del router para eliminar el contenido de la NVRAM .

- Introducir el comando **show startup-config** en el indicador del router y confirmar que la configuración inicial del router no estará disponible al reiniciar el router. ¿Qué muestra el router al introducir este comando?
- Reiniciar el router con el comando **reload.** Cuando se solicite continuar con la recarga, introducir **Y** y presione la tecla **Intro**. Alli el router muestra el mensaje: "Notice: NVRAM invalid, possibly due to write erase". Cuando se solicite entrar al diálogo de configuración inicial, escribir **N** y presione **Intro**. Cuando se solicite terminar con la instalación automática escriba **Y** y presione **Intro**. Presionar **Intro** nuevamente.
- Entrar al modo privilegiado utilizando el comando **enable.** Aquí se puede ver que la configuración ha sido borrada y que no se requiere contraseña.
- Reconfigurar manualmente la dirección IP y la máscara de subred de la interfaz (E0 o E1) que se utiliza para transferir el archivo de configuración de respaldo desde el servidor TFTP. Esto es porque el router perdió el archivo de configuración cuando se borró y se volvió a cargar la NVRAM. La configuración de la interfaz es necesaria para volver a establecer una conexión con el servidor TFTP.
- Copiar la copia de respaldo del archivo de configuración del servidor TFTP entrando el comando **copy tftp running-config.** Cuando se solicite el host remoto, introducir la dirección IP que se verificó anteriormente y presionar **Intro**. Cuando se solicite el archivo de configuración que se debe leer, la opción por defecto es el nombre del router, seguido por un guión y la palabra

confg (por ej., LAB-A-confg). Aceptar ese nombre presionando **Intro,** o escribir un nuevo nombre y presionar **Intro** o escribir el nombre que usó anteriormente. Confirmar que se desea copiar el archivo de configuración del servidor TFTP presionando **Intro**. Una vez que se completa el proceso, el router indica la cantidad de la RAM utilizada para el archivo de configuración y la cantidad total de RAM disponibles en el router.

- Guardar el nuevo archivo de configuración utilizabdo el comando **copy running-config startup-config.** Este comando copia la configuración activa del router desde la RAM en la NVRAM como copia de respaldo. Introducir el comando **copy start run** en el indicador del router.

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7 CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet:

http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

# ANEXO J. LABORATORIO 10: MODO DE CONFIGURACIÓN GLOBAL DEL ROUTER

## 1. GUÍA DE LABORATORIO

### 1.1 OBJETIVOS

- Usar el modo de configuración del router para configurar el protocolo de enrutamiento.
- Configurar la identificación del router (nombre).
- Configurar un título con un mensaje del día (motd).
- Usar el modo de configuración de interfaz para introducir una descripción de interfaz.

### 1.2 EQUIPO UTILIZADO

- PC con monitor, teclado, ratón y cables de alimentación, etc.
- Sistema operativo Windows (Win 95, 98, NT o 2000) instalado en el PC
- Programa HyperTerminal PE configurado para acceder a la consola del router
- PC conectado al puerto de consola del router mediante un cable rollover

## 1.3 MARCO TEÓRICO

El indicador del router en el modo de configuración global es: "Router-name(config)#". Se utilizarán otros modos de configuración para múltiples líneas de comando y configuraciones detalladas como en la configuración de interfaces. Al trabajar con las interfaces, el aspecto del indicador del router es "Router-name(config-if)#". También se podrá configurar un título con un mensaje del día mediante el comando banner motd en el modo de configuración global e introducir descripciones para las interfaces en el router en el modo de configuración de interfaz.

## 1.4 PROCEDIMIENTO

- Conectarse al router E introducir la contraseña cisco si se solicita.
- Entrar al modo privilegiado colocando **enable e** introducir la contraseña class. ¿Cuál es el comando del router que se utiliza para visualizar la configuración actual?
- Introducir el comando **show running-config** para ver la información acerca de la configuración actual desde el archivo cargado en la RAM (Memoria de acceso aleatorio). Comparar el nombre de host en la configuración actual con el indicador del router. ¿Son iguales?

- Introducir el comando **show startup-config** para ver información sobre la copia de respaldo del archivo de configuración almacenada en la NVRAM (RAM no volátil). ¿El nombre del host es igual que el del indicador del router?
- Introducir el comando **configure terminal** para entrar al modo de configuración global. ¿Qué aspecto tiene el indicador del router?
- Escribir el comando **help** escribiendo (?) en el indicador del router. Con ello, el router responde con todos los comandos disponibles para el modo de configuración global. ¿Hostname es una de las opciones del comando?
- Escribir el comando **help** para hostname introduciendo hostname ? en el indicador del router para obtener una ayuda con respecto a este comando. ¿Cómo respondió el router?
- Introducir **hostname** y un nombre en el indicador del router. Este comando reemplazará el nombre de host del router por el nombre indicado. ¿El indicador del router cambió al nuevo nombre de host?
- Escribir **exit** en el indicador del router para volver al indicador de modo privilegiado. Introducir **show running-config** para verificar la configuración activa. El cambio de configuración realizado (nombre de host) sólo será efectivo cuando el router se reinicie o se recargue. ¿Cuál es el nombre de host del router?
- Escribir **show startup-config** para ver información sobre la copia de respaldo del archivo de configuración almacenada en la NVRAM. ¿El nombre del host es igual que el del indicador del router?

- Entrar el comando **configure terminal** y entrar al modo de configuración global. Escribir **banner motd #Este es el mensaje del día#** en el indicador del router. Aquí, se está creando un título con el mensaje del día que aparece cuando alguien se conecta al router. El mensaje se encuentra rodeado por signos # que indican al router el inicio y el final del mensaje.
- Introducir **exit** en el indicador del router. Escribir **show running-config** para verificar la configuración activa. El cambio de configuración que se acaba de realizar será efectivo hasta que el router se reinicie o se recargue. ¿Cuál es el mensaje del día mostrado por el router?
- Escribir **exit** en el indicador del router para salir del router; también se puede usar **logout** .
- Conectarse al router. Introducir la contraseña cisco si se solicita. Entrar al modo privilegiado utilizando el comando **enable**. Introducir la contraseña enable class.
- Escribir el comando **show running-config** para ver información sobre la configuración actual. ¿Existe un nombre para describir la interfaz serial0?
- Introducir **configure terminal** en el indicador del router para entrar al modo de configuración global.
- Escribir el comando **interface serial0** en el indicador de configuración global para cambiar la configuración de serial0. ¿Cuál es el aspecto del indicador de router en el modo de configuración de interfaz?

- Introducir el comando **help** (?) en el indicador del router para obtener una lista de comandos disponibles para configurar la interfaz serial0. Luego, escribir **description ?** en el indicador del router.
- Introducir en **description** el texto que se desee (hasta 80 caracteres) en el indicador del router. Esto mostrará una descripción para la interface serial0.
- Escribir **exit** en el modo de configuración de interfaz. Luego, **exit** en el modo de configuración global. Observar cómo el indicador del router ha cambiado después de utilizar cada comando exit.
- Entrar el comando **show running-config** para ver información sobre la configuración actual. ¿Cuál es la descripción para la interface serial0?
- Introducir el comando **show startup-config** en el indicador del router para observar información sobre la copia de respaldo del archivo de configuración almacenada en la NVRAM. ¿La descripción de la interfaz serial0 es la misma que la anterior?
- Escribir el comando **reload.** Cuando se solicita guardar los cambios contestar que **NO**. esto es porque todos los cambios realizados al router eran efectivos en la configuración activa, una vez que se recarga el router, éste se recarga a partir de la copia de respaldo del archivo de configuración. Si se hubiesen conservado los cambios se hubiera usado un comando para copiar la configuración actual en la copia de respaldo del archivo de configuración. ¿Cuál es el comando que se utiliza para copiar la configuración actual en la copia de respaldo de la configuración (de inicio)?

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7 CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

# ANEXO K. LABORATORIO 11: MODO DE CONFIGURACIÓN DE LA INTERFAZ DEL ROUTER

## 1.GUÍA DE LABORATORIO

### 1.1 OBJETIVOS

- Utilizar el modo de configuración de interfaz para configurar las interfaces.
- Configurar las asignaciones de dirección IP a las interfaces del router.
- Configurar las asignaciones de máscara de subred a las interfaces del router.
- Copiar la configuración activa en la copia de respaldo de la configuración.

### 1.2 EQUIPO UTILIZADO

- PC con monitor, teclado, ratón y cables de alimentación, etc.
- Sistema operativo Windows (Win 95, 98, NT o 2000) instalado en el PC
- Programa HyperTerminal PE configurado para acceder a la consola del router
- PC conectado al puerto de consola del router mediante un cable rollover

## 1.3 MARCO TEÓRICO

El modo de configuración de la interfaz del router se utiliza para configurar una dirección IP y una máscara de subred para cada interfaz del router. Aquí se debe verificar que la conectividad de la capa 3 sea correcta usando el comando ping. El comando show running-config servirá para asegurarse de que los cambios que han realizado sean los deseados. Luego se guarda la configuración activa en la copia de respaldo de la configuración.

## 1.4 PROCEDIMIENTO

- Conectarse al router e introducir la contraseña cisco si se solicita. Entrar al modo privilegiado con el comando **enable.** Introducir la contraseña class.
- Escribir el comando **show running-config** para ver información sobre la configuración actual. Anotar los datos de interfaz, dirección IP y máscara de subred parta cada router.
- Escribir el comando **configure terminal**. Esto es para configurar en el modo de configuración global. ¿Qué aspecto tiene el indicador del router?
- Entrar el comando **interface serial0** en el indicador de configuración global. Con esto, se puede cambiar la configuración de serial0. ¿Qué aspecto tiene el indicador del router?

- Escribir IP address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy en el indicador del modo de interfaz del router. xxx.xxxx.xxx.xxx es la dirección IP y yyy.yyy.yyy.yyy es la máscara de subred para Serial0. Utilizar la dirección IP y la máscara de subred de la configuración de laboratorio del segundo semestre (remitirse a la figura 16, página 137), Con este comando se establece la IP y la máscara de subred para serial0
- Entrar el comando **clock rate 56000** para establecer la velocidad del reloj DCE para el enlace WAN. Esta velocidad del reloj se debe establecer en la conexión DCE (hembra).
- Introducir **exit** en el indicador del router. Para volver a un indicador de configuración global. ¿Qué aspecto tiene el indicador del router?
- Teclear **exit** o presionar **control y la tecla z (Control-z)** al mismo tiempo para entrar al modo privilegiado. ¿Qué aspecto tiene el indicador del router?
- Escribir el comando **show running-config** en el indicador del router para obtener información sobre la configuración actual. Aquí, aparecerá cualquier cambio que haya introducido. ¿Cuál fue la dirección IP y la máscara de subred que asignó el router para serial0?
- Introducir ping xxx.xxx.xxx.xxx donde xxx.xxx.xxx.xxx es una dirección IP de serial0 en el indicador de router. En este instante, se puede probar la serial0 y asegurarse de que esté funcionando. (Nota: Si el otro extremo del enlace serial de la WAN (el router siguiente) no está configurado correctamente o si el otro router no está activado es posible que el resultado de ping no sea exitoso).

- Entrar el comando **copy running-config startup-config** en el indicador del router. Esto es para que la configuración activa se copie en la copia de respaldo de la configuración. La próxima vez que el router se active o recargue, cargará desde la copia de respaldo de la configuración.
- Repetir todos los pasos con todas las interfaces identificadas (la velocidad del reloj se establece solamente en S0). ¿Qué comandos informarán cuántas y qué tipo de interfaces se encuentran en el router?
- Entrar el comando **reload** en el indicador del router para recergar el router desde la copia de respaldo de la configuración.
- Escribir el comando **show running-config** en el indicador del router para obtener información sobre la configuración actual.
- Salir del router

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7 CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

# ANEXO L. LABORATORIO 12: CISCO CONFIGMAKER

## 1. GUÍA DE LABORATORIO

### 1.1 OBJETIVOS

- Usar Cisco ConfigMaker para configurar un router.
- Trazar un mapa de red utilizando Cisco ConfigMaker.
- Imprimir un archivo de configuración creado por ConfigMaker.

### 1.2 EQUIPO UTILIZADO

- Estación de trabajo de PC con el sistema operativo Windows e HyperTerminal instalados.
- Cisco ConfigMaker (versión más reciente) - IOS versión 11.2 o posterior.
- Dos routers de Cisco - modelo de serie 1600 o serie 2500 cada uno con 1 interfaz serial y 1 interfaz Ethernet.
- Un router Cisco - modelo de serie 1600 o serie 2500 con 2 interfaces seriales y 1 interfaz Ethernet.

- Dos hubs Ethernet - 10BASE-T, de 4 a 8 puertos (Use tres hubs si el switch no está disponible).
- Un switch Ethernet (Cisco Catalyst 1900 u otro similar).
- Tres cables de consola para conectar la estación de trabajo directamente al puerto de consola del router.
- Tres conjuntos de cables seriales V.35 WAN (macho/ hembra) para conectar de router a router.
- Seis cables Ethernet CAT6 de conexión directa.

## 1.3 MARCO TEÓRICO

Cisco ConfigMaker es una aplicación de Windows 95/98/NT que permite configurar routers, switches, hubs y otros dispositivos Cisco. Mediante una interfaz de usuario gráfica, se puede trazar la red y luego Cisco ConfigMaker crea los archivos de configuración Cisco IOS para los dispositivos de la red. Además, se puede usar Cisco ConfigMaker como herramienta fuera de línea. Se puede trazar y configurar una red completa sin tener los dispositivos a mano hasta que esté listo para entregarles los archivos de configuración.

## 1.4 PROCEDIMIENTO

- Descargar desde www.cisco.com e instalar Cisco ConfigMaker.

- Hacer doble clic en el icono Cisco ConfigMaker para abrir el programa ConfigMaker e iniciar el tutorial automáticamente. También se puede ejecutar el tutorial después haciendo clic en el icono tutorial de la barra de herramientas.
- En Devices (Dispositivos), hacer clic en la carpeta **Routers** y agregue los routers a la configuración de laboratorio. Una vez que ha seleccionado el número de modelo correcto del router que va a agregar, colocar el router en el lugar deseado dentro del área del diagrama de red arrastrándolo al área del Diagrama de red. Se pedirá que información de configuración. ¿Que otras series de routers se pueden configurar con ConfigMaker?
- Para configurar el router, se debe dar nombre al router. Teclear Lab-A y hacer clic en **siguiente.** Luego se deben asignar asignar las contraseñas de conexión y enable secret del router. Introducir cisco como contraseña y class como enable, luego hacer clic en siguiente. Luego, hay que comunicar al router qué protocolo usará: seleccionar TCP/IP, hacer clic en siguiente y luego salir.
- Repetir los pasos anteriores para agregar otros routers al diagrama de red.
- Para agregar conexiones a los routers, hacer click en **HDLC** en la ventana **conexiones** y luego en Lab-A, luego en el dispositivo con el cual se va a conectar (Lab-B). Después de agregar la conexión HDLC del Lab-A al Lab-B, se abre el asistente HDLC. Hacer clic en **siguiente**. Ahora se formula la pregunta sobre qué interfaz serial se desea utilizar para esta conexión. Utilizar **Serial0,** luego hacer clic en **siguiente**. Luego se solicitará información de

direccionamiento para esta interfaz. Introducir la dirección IP y la máscara de subred, luego hacer clic en **siguiente**. ConfigMaker pedirá que se suministre información acerca del router al cual está conectado (Lab-B). Seleccionar **interface Serial1** para el Lab-B e introducir la dirección IP, luego hacer clic en **siguiente**. Ahora se puede crear una copia de respaldo de la conexión. Para esta práctica de laboratorio seleccionar **no backup** (sin copia de respaldo) luego hacer clic en **siguiente** y salir. ¿Qué otras conexiones puede configurar con ConfigMaker?

- Repetir los pasos anteriores para los demás routers.
- Para agregar o cambiar la configuración del router, se hace doble clic en el router Lab-A en el diagrama de red. Hacer clic en la ficha **IOS Configuration**. ¿Qué comando faltaba de la configuración de IOS de ConfigMaker para la interfaz S0?
- Para agregar comandos de configuración, colocarse en **Lab-A Properties** (Propiedades de Lab-A) en la ficha **IOS Configuration** haga clic en el botón **Add / Modify IOS commands.** Esta ventana permitirá introducir comandos adicionales para el router. ¿Qué comandos hay que agregar al router para colocar temporización a la interfaz S0?
- Para entregar los comandos IOS al router, resaltar el router en el que se desea cargar la configuración IOS y hacer clic en el botón **Deliver** (Entregar). Aquí, ConfigMaker intentará cargar la configuración del IOS. Si existe un problema o

error ConfigMaker se comunicará y se podrá corregir el problema y luego hacer clic en **Deliver** para intentar entregar nuevamente la configuración IOS.

- Para imprimir el diagrama de red y la configuración del router, se debe hacer clic en el menú **File** (Archivo) y luego hacer clic en **Print Network** (Imprimir red) o **Print All** (Imprimir todo). También se puede hacer clic en **Print Preview** (Vista preliminar) para ver cómo quedó antes de imprimir. **Print All** (Imprimir todo) imprimirá el diagrama de red y un listado del archivo de configuración para cada router.
- Para guardar la configuración del router en un archivo de texto, se debe hacer clic con el botón derecho del ratón en el router, hacer clic en **IOS Configuration** y luego hacer clic en **File/Save As** (Archivo/Guardar como). Se le puede otorgar un nombre al archivo, que tendrá la extensión .CFG. Se puede editar con el Bloc de notas de Windows. También se puede imprimir el archivo de configuración desde aquí o enviarlo a un router

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7 CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

# ANEXO M. LABORATORIO 13: CONFIGURACIÓN DEL ROUTER DESDE UN NAVEGADOR WEB

## 1. GUÍA DE LABORATORIO

### 1.1 OBJETIVOS

- Configurar un router como servidor HTTP para aceptar peticiones de configuración a través de un navegador de Web.
- Aprender los valores del router que se pueden configurar a través de un navegador de Web.

### 1.2 EQUIPO UTILIZADO

- PC con monitor, teclado, ratón y cables de alimentación, etc.
- Sistema operativo Windows (Win 95, 98, NT o 2000) instalado en el PC
- Programa HyperTerminal PE configurado para acceder a la consola del router
- PC conectado al puerto de consola del router mediante un cable rollover
- PC conectado al mismo hub o switch que el router

- Un navegador de web (Internet Explorer o Netscape Navigator) instalado en la estación de trabajo.

## 1.3 MARCO TEÓRICO

El comando IP HTTP server permite que el router actúe como servidor Web HTTP (Protocolo de transferencia de hipertexto) limitado. No existen gráficos sino una serie de pantallas de texto en color que permiten al administrador modificar la configuración y consultar información acerca del router. La interfaz del navegador hacia el router soporta el control del ratón y hace que resulte más fácil realizar ciertas tareas sin que sea necesario conocer muy bien la interfaz de línea de comando. La interfaz de línea de comando está disponible una vez que se encuentra en modo navegador. Es posible usar una interfaz de navegador al acceder a los switches y routers de Cisco

Es más probable que un navegador de web esté disponible en un computador cliente que un programa de Telnet. Puede resultar más fácil en algunos casos verificar el estado de un router y realizar configuraciones menores desde un navegador de web.

## 1.4 PROCEDIMIENTO

- Conectarse al router. Introducir la contraseña cisco si se solicita. Entrar al modo EXEC privilegiado con el comando **enable**. Entrar la contraseña enable de class.
- Entrar al modo de configuración global y teclear el comando **configure terminal** para cambiar valores de configuración que afectan al router.
- Para activar la función del servidor HTTP, se escribe el comando **IP HTTP server**. Esto permite al router actuar como servidor HTTP limitado en el puerto HTTP por defecto (80). Presionar y mantener presionada la tecla **Control** luego presionar la **tecla Z** para salir del modo de configuración global.
- Para acceder al router a través del navegador de red se debe activar el navegador de web en la estación de trabajo e introducir la dirección IP del puerto Ethernet del router en la ventana de direcciones del navegador. Cuando se entra la dirección IP de la interfaz Ethernet del router, éste se conectará como cliente HTTP y el servidor HTTP que se activó previamente en el router responderá a las peticiones del navegador. Responder las siguientes preguntas:

  1. ¿Cuál es la dirección IP del puerto Ethernet?
  2. ¿Qué opciones hay disponibles?

Cuando se solicita un nombre de usuario y contraseña, el campo de nombre de usuario se puede dejar en blanco: Introducir class como contraseña.

Para observar las opciones disponibles, se debe hacer clic en cada una de las opciones y tomar nota de lo obtenido. Aquí aparecen recursos de ayuda en la mitad inferior de la página de presentación del router. ¿Qué opción de la página de presentación del router tiene la mayor cantidad de subopciones?

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7 CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

# ANEXO N. LABORATORIO 14: RECUPERACIÓN DE LA CONTRASEÑA DEL ROUTER

## 1. GUÍA DE LABORATORIO

### 1.1 OBJETIVO

Aprender el procedimiento para recuperar la contraseña en caso de olvido.

### 1.2 EQUIPO UTILIZADO

- PC conectada al puerto de consola del router mediante un cable rollover
- Sistema operativo Windows (Win 95, 98, NT o 2000) instalado en el PC
- Programa HyperTerminal PE configurado para acceder a la consola del router

### 1.3 MARCO TEÓRICO

Habrán circunstancias en las cuales la contraseña para un router deberá reemplazarse. También es posible que se haya olvidado la contraseña o que el

administrador de red no trabaje más en la empresa. El procedimiento de recuperación de contraseña requiere acceso físico al router debido a que se utiliza un cable de consola directamente conectado. Como los métodos de recuperación de contraseña se publican en Internet y en libros, los routers necesitan estar en una ubicación segura con acceso físico restringido al personal autorizado.

## 1.4 PROCEDIMIENTO

- Antes de iniciar la práctica, se debe borrar la información contenida en la NVRAM.
- Ahora, hay que conectarse al router e introducir la contraseña cisco si se solicita.
- Introducir el comando **show version**. Aquí se muestran los valores de registro de la configuración actual junto con información adicional. ¿Cuáles es el valor del registro de configuración actual?
- Apagar el router durante unos segundos y encenderlo nuevamente. Cuando el router está reiniciando, la secuencia de arranque se puede interrumpir.
- Dentro de los primeros 60 segundos después de encender el router, presionar y mantener presionada la tecla **Control**, luego presionar la tecla **Pausa**. Esto se hace para interrumpir la secuencia de arranque.
- Introducir los comandos para cambiar el registro de configuración. El registro de configuración se cambia para pedir al router que ignore el archivo de

configuración en la NVRAM en el siguiente inicio. El procedimiento varía según el modelo del router.

- Router serie 2500: El indicador es >, sin nombre de router. Escribir o/r 0x42 y presionar **Intro.** Luego, se escribe i y se presiona **Intro** para recargar el router. Hay que espera a que el router reinicie. Luego, se escribe n cuando se solicite entrar a la configuración inicial. Presionar **Intro** para ver el indicador router>.
- Router serie 1600: El indicador es rommon 1>. Se debe escribir **config** y **Y** cuando se solicite cambiar la configuración. Escribir N para todas las preguntas menos **ignore system config info**. Luego de responder las preguntas, se solicitará cambiar la configuración nuevamente. Escribir N, luego escribir **reset** para recargar el router. Esperar hasta que el router reinicie. Escribir N cuando se solicite entrar a la configuración inicial. Presionar **Intro** para ver el indicador router>.

- Entrar al modo EXEC privilegiado. Utilizando el comando **enable**. ¿Por qué no se requiere ninguna contraseña?
- Examinar la configuración que el router está utilizando a través del comando **show running-config**. Como los registros de la configuración se establecieron para ignorar el archivo de configuración, el router posee una configuración mínima.

- Escribir el comando **copy startup-config running-config** para que el archivo de configuración se cargue desde la NVRAM en la RAM . Esto permitirá visualizar y/o modificar las contraseñas del router. ¿Cuál es el cambio que se presenta en el indicador del router?
- Entrar el comando **show running-config**. Las contraseñas que se han cifrado con el comando enable secret aparecen como una serie de letras, números y símbolos. Las contraseñas no cifradas aparecen en forma de texto simple. ¿Qué contraseñas se pueden ver?
- Introducir los comandos para cambiar las contraseñas apropiadas. Las contraseñas que se establecen con el comando **enable secret** no se pueden descifrar. La única opción es cambiar la contraseña a otro valor. Se debe ir al modo de configuración global y teclear el comando **configure terminal** y luego el comando **enable secret nuevacontraseña**. Presionar y mantener presionada la tecla **Control** y presionar **Z** para salir del modo de configuración global. Escribir el comando **show running-config.** ¿Qué contraseñas se pueden ver ahora? ¿El valor de la contraseña cifrada cambió con respecto al paso anterior?
- Examinar el estado actual del registro de configuración y cambiarlo nuevamente a su valor original ya que el registro de configuración sigue programado para que ignore la configuración inicial contenida en la NVRAM. Introducir el comando **show version**. ¿Cuál es el valor del registro de configuración?

- Entrar al modo de configuración global introduciendo el comando **config terminal.** Escribir el comando **config-register 0x2102**. (Nota: usar el valor original que se guardó en el paso 2). Presionar **Control Z** para salir del modo de configuración global. Introducir comando **show version** para ver el nuevo valor del registro de configuración. ¿Cuál es el nuevo valor del registro de configuración?
- Teclear el comando **reload**. Luego se debe introducir **Y** si se indica que hay que guardar la nueva configuración y que se procederá con la carga. Todo esto para verificar la nueva contraseña. Se debe entrar al modo EXEC privilegiado con el comando **enable** y luego introducir la contraseña class. Si se establece correctamente la contraseña de habilitación, el indicador del router cambiará. Para ver el estado del registro de configuración se debe digitar el comando **show version .**

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7 CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

# ANEXO O. LABORATORIO 15: CONFIGURACIÓN INDIVIDUAL DEL ROUTER

## 1. GUÍA DE LABORATORIO

### 1.1 OBJETIVOS

- Configurar un router basándose en la configuración de la topología del segundo semestre de Cisco.
- Configurar el router utilizando solamente la Interfaz de línea de comando (CLI)
- Configurar los parámetros de la dirección IP de la estación de trabajo para comunicarse con el router a través de Ethernet

### 1.2 EQUIPO UTILIZADO

- PC conectada al puerto de consola del router mediante un cable rollover
- Sistema operativo Windows (Win 95, 98, NT o 2000) instalado en el PC
- Programa HyperTerminal PE configurado para acceder a la consola del router

## 1.3 MARCO TEÓRICO

Para esta experiencia de laboratorio se configurará individualmente uno de los cinco routers del laboratorio mediante la interfaz de línea de comando, sin utilizar notas, solamente con la topología de red (ver figura 16, página 137). Se puede usar la función de ayuda del router y el diagrama del router. La idea es configurar el router tan rápidamente como sea posible, sin cometer errores. También se deben configurar los parámetros IP para una de las estaciones de trabajo Ethernet conectadas.

## 1.4 PROCEDIMIENTO

- Acceder al router a través de la consola. Verificar que tenga una buena conexión de consola y que el programa HyperTerminal esté configurado adecuadamente. El router se debe arrancar sin archivos de configuración de inicio en la NVRAM.
- Identificar la información de dirección Ipy completar la siguiente tabla:

**Tabla 1.**

| Nombre del router | Lab_A | Lab_B | Lab_C | Lab_D | Lab_E |
|---|---|---|---|---|---|
| Número del modelo | | | | | |
| Dirección IP de la interfaz E0 | | | | | |
| Máscara de subred de la interfaz E0 | | | | | |
| Dirección IP de la interfaz | | | | | |
| Máscara de subred de la interfaz | | | | | |
| Dirección IP de la interfaz S0 | | | | | |
| Máscara de subred de la interfaz SO | | | | | |
| Velocidad de temporización de la interfaz SO | | | | | |
| Dirección IP de la interfaz SI | | | | | |
| Máscara de subred de la interfaz SI | | | | | |
| Otra(s) interfaz (interfaces) | | | | | |

- Ahora, debe realizarse la configuración del router a través de la conexión de consola. Para esto se debe seleccionar un router y configurar la siguiente información para cada router: Nombre de host, contraseñas, direcciones IP de las interfaces, protocolo de enrutamiento y números de red asociados, tabla de consulta de host IP. Repetir el mismo procedimiento con los demás routers.

Asegurarse de copiar la configuración actual en la configuración de inicio una vez que se haya terminado o se perderá la configuración en el siguiente rearranque.

- Configurar los parámetros IP de la estación de trabajo utilizando **Panel de Control/ Red.** Se debe configurar la dirección IP, la máscara de subred y el gateway por defecto para que sean compatibles con el router.
- Probar la configuración utilizando los comandos ping y telnet, desde el indicador DOS del PC.
- A continuación, se presentan los resultados del comando **show running-config** para los cinco routers de la configuración de la topología del semestre dos. Si existe algún inconveniente al configurar algunos de los routers, se pueden consultar los siguientes datos:

**Router: LAB-A**

LAB-A#show run

Building configuration...

Current configuration:

version 11.1

service udp-small-servers

service tcp-small-servers

hostname LAB-A

enable secret 5 $1$xT7v$9EC3X5IBHLwq2RehHNvWc0

```
interface Ethernet0
ip address 192.5.5.1 255.255.255.0
interface Ethernet1
ip address 205.7.5.1 255.255.255.0
interface Serial0
ip address 201.100.11.1 255.255.255.0
clock rate 56000
interface Serial1
no ip address
shutdown
router rip
network 192.5.5.0
network 205.7.5.0
network 201.100.11.0
ip host LAB-B 201.100.11.2 219.17.100.1 199.6.13.1
ip host LAB-C 199.6.13.2 223.8.151.1 204.204.7.1
ip host LAB-D 204.204.7.2 210.93.105.1
ip host LAB-E 210.93.105.2
ip host LAB-A 192.5.5.1 205.7.5.1 201.100.11.1
no ip classless
line con 0
password cisco
login
```

line aux 0

line vty 0 4

password cisco

login

!end

**Router: LAB-B**

LAB-B#show run

Building configuration...

Current configuration:

version 11.1

service udp-small-servers

service tcp-small-servers

hostname LAB-B

enable secret 5 $1$xT7v$9EC3X5lBHLwq2RehHNvWc0

interface Ethernet0

ip address 219.17.100.1 255.255.255.0

no mop enabled

interface Serial0

ip address 199.6.13.1 255.255.255.0

clock rate 56000

interface Serial1

ip address 201.100.11.2 255.255.255.0

```
interface BRI0
no ip address
shutdown
router rip
network 219.17.100.0
network 199.6.13.0
network 201.100.11.0
ip host LAB-B 201.100.11.2 219.17.100.1 199.6.13.1
ip host LAB-C 199.6.13.2 223.8.151.1 204.204.7.1
ip host LAB-D 204.204.7.2 210.93.105.1
ip host LAB-E 210.93.105.2
ip host LAB-A 192.5.5.1 205.7.5.1 201.100.11.1
no ip classless
snmp-server community public RO
line con 0
password cisco
login
line aux 0
line vty 0 4
password cisco
login
```

**Router: LAB-C**

```
LAB-C#show run
Building configuration...
Current configuration:
version 11.1
service udp-small-servers
service tcp-small-servers
hostname LAB-C
enable secret 5 $1$xT7v$9EC3X5IBHLwq2RehHNvWc0
interface Ethernet0
ip address 223.8.151.1 255.255.255.0
interface Serial0
ip address 204.204.7.1 255.255.255.0
clock rate 56000
interface Serial1
ip address 199.6.13.2 255.255.255.0
interface BRI0
no ip address
shutdown
router rip
network 223.8.151.0
network 199.6.13.0
network 204.204.7.0
```

ip host LAB-A 192.5.5.1 205.7.5.1 201.100.11.1

ip host LAB-B 201.100.11.2 219.17.100.1 199.6.13.1

ip host LAB-C 199.6.13.2 223.8.151.1 204.204.7.1

ip host LAB-D 204.204.7.2 210.93.105.1

ip host LAB-E 210.93.105.2

no ip classless

line con 0

password cisco

login

line aux 0

line vty 0 4

password cisco

login

!

**Router: LAB-D**

LAB-D#show run

Building configuration...

Current configuration:

version 11.1

service udp-small-servers

service tcp-small-servers

hostname LAB-D

```
enable secret 5 $1$xT7v$9EC3X5IBHLwq2RehHNvWc0
interface Ethernet0
ip address 210.93.105.1 255.255.255.0
no ip mroute-cache
no ip route-cache
interface Serial0
no ip address
no ip mroute-cache
no ip route-cache
shutdown
interface Serial1
ip address 204.204.7.2 255.255.255.0
no ip mroute-cache
no ip route-cache
router rip
network 204.204.7.0
network 210.93.105.0
ip host LAB-A 102.5.5.1 205.7.5.1 201.100.11.1
ip host LAB-B 201.100.11.2 219.17.100.1 199.6.13.1
ip host LAB-C 199.6.13.2 223.8.151.1 204.204.7.1
ip host LAB-D 204.204.7.2 210.93.105.1
ip host LAB-E 210.93.105.2
no ip classless
```

line con 0

password cisco

login

line aux 0

line vty 0 4

password cisco

login

**Router: LAB-E**

LAB-E#show run

Building configuration...

Current configuration:

version 11.1

service udp-small-servers

service tcp-small-servers

hostname LAB-E

enable secret 5 $1$q/QJ$EA8tfOg1/Rxn/28FSrLgJ/

interface Ethernet0

ip address 210.93.105.2 255.255.255.0

interface Serial0

no ip address

shutdown

interface Serial1

```
no ip address
shutdown
router rip
network 210.93.105.0
ip host LAB-A 192.5.5.1 205.7.5.1 201.100.11.1
ip host LAB-B 201.100.11.2 219.17.100.1 199.6.13.1
ip host LAB-C 199.6.13.2 223.8.151.1 204.204.7.1
ip host LAB-D 204.204.7.2 210.93.105.1
ip host LAB-E 210.93.105.2
no ip classless
line con 0
password cisco
login
line aux 0
line vty 0 4
password cisco
login
!
```

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7 CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

# ANEXO P. LABORATORIO 16: FUNCIONAMIENTO DE ARP

## 1. GUÍA DE LABORATORIO

### 1.1. OBJETIVOS

- Familiarizarse con el comando show ARP del router.
- Familiarizarse con el comando clear ARP del router.

### 1.2 EQUIPO UTILIZADO

- PC conectada al puerto de consola del router mediante un cable rollover
- Sistema operativo Windows (Win 95, 98, NT o 2000) instalado en una PC
- Programa HyperTerminal configurado para acceder a la consola del router
- PC conectada al puerto de consola del router mediante un cable rollover

### 1.3 MARCO TEÓRICO

Los comandos show ARP y clear ARP son muy importantes para diagnosticar un problema de red. El router mantiene información sumamente detallada acerca de

la dirección MAC y las direcciones IP asociadas. De vez en cuando, la información puede dañarse y causar problemas en la entrega de paquetes. Cuando esto ocurre, la tabla ARP del router se debe despejar y reconstruir.

## 1.4 PROCEDIMIENTO

- Conectarse al router y escribir la contraseña cisco si se solicita.
- Escribir el comando **show arp** en el indicador del router. Aquí, el router responde con la tabla ARP que muestra la dirección IP y la dirección MAC de cada interfaz. Cuáles son las tres (3) informaciones importantes que se pueden ver?
- Entrar al modo privilegiado con el comando **enable**. Teclear la contraseña class.
- Escribir el comando **help** (ayuda) escribiendo **(?)** en el indicador del router. Aquí, el router muestra todos los comandos disponibles en el Modo Privilegiado. ¿El comando clear aparece como una opción?
- Introducir el comando **clear arp** en el indicador del router. En este instante, el router despeja la tabla arp.
- Introducir **show arp** en el indicador del router. El router responde con la tabla ARP. ¿Hay alguna entrada en la tabla ARP? Si observa la dirección IP de las entradas ARP, ¿para qué se utilizan las entradas?

- Hacer ping a todas las interfaces de la red. Esto es para generar tráfico de red entre los routers.
- Escribir el comando **show arp** para observar la tabla ARP. ¿Hay alguna entrada nueva en la tabla ARP?
- Abrir un indicador de comandos de MS-DOS **(Inicio/Programas/MS DOS)**. Hacer ping a todas las estaciones de trabajo en la red de laboratorio. Hay que observar que las estaciones de trabajo tengan un direccionamiento IP adecuado para la red con la que están conectadas y un gateway por defecto. Esto produce tráfico de red desde una estación de trabajo hacia otra.
- Introducir el comando **show arp** para observar la tabla ARP. ¿Hay alguna entrada nueva en la tabla ARP? Explicar por qué.
- Salir del router.

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7 CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

# ANEXO Q. LABORATORIO 17: CONFIGURACIÓN DE RUTAS ESTÁTICAS

## 1. GUÍA DE LABORATORIO

### 1.1 OBJETIVOS

- Configurar una ruta estática entre routers vecinos directos usando el comando ip route.
- Copiar la configuración activa en la configuración de inicio.

### 1.2 EQUIPO UTILIZADO

- 5 estaciones de trabajo de PC 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 seriales 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 CAT 6 de conexión directa para conectar los routers y estaciones de trabajo con hubs y switches.

## 1.3 MARCO TEÓRICO

Las rutas estáticas son rutas que hacen que los paquetes se desplacen entre un origen y un destino a través de una ruta determinada. Generalmente son definidas manualmente por un administrador de red. Las actualizaciones de enrutamiento no se envían a través de un enlace si sólo se encuentran definidas por una ruta estática, por lo tanto, conservan el ancho de banda. Otra aplicación para una ruta estática es la seguridad ya que el enrutamiento dinámico tiende a revelar todo lo que conoce acerca de una red. A veces, las rutas estáticas se utilizan para sitios remotos y para probar un enlace determinado o una serie de routers de la internetwork.

## 1.4 PROCEDIMIENTO

- Conectarse al router. Introducir la contraseña cisco si se solicita.

- Escribir ping xxx.xxx.xxx.xxx. Esta dirección IP corresponde a uno de los routers vecinos. ¿Alguna de las interfaces del router respondió con un ping exitoso?
- Entrar al modo privilegiado con el comando **enable**. Escribir la contraseña class.
- Introducir **show startup-config.** Aquí, el router mostrará información sobre la copia de respaldo del archivo de configuración almacenada en la NVRAM. ¿Qué protocolos de enrutamiento o rutas estáticas se han definido, de haberlos?
- Escribir el comando **configure terminal.** ¿Qué aspecto tiene el indicador del router?
- Introducir **IP route ?** en el indicador del router. En este momento, el router responde mostrando la descripción disponible para la ruta IP. ¿Cuál fue la respuesta del router?
- Escribir **IP route xxx.xxx.xxx.xxx ?** en el indicador del router. xxx.xxx.xxx.xxx es la dirección de red para la cual se desea una ruta estática. ¿Cuál fue la respuesta del router?
- Digitar **IP route xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy** en el indicador del router. La dirección xxx.xxx.xxx.xxx. corresponde a la dirección de red de la red destino mientras yyy.yyy.yyy.yyy es la máscara de subred de la red destino. ¿Cuál fue la respuesta del router?

- Introducir **IP route xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy zzz.zzz.zzz.zzz** en el indicador del router. La dirección xxx.xxx.xxx.xxx. corresponde a la dirección de red de la red destino; yyy.yyy.yyy.yyy es la máscara de subred de la red destino y zzz.zzz.zzz.zzz es la dirección IP de la interfaz vecina directa.
- Salir del modo de configuración global del router escribiendo **exit** en el indicador del router. ¿Qué aspecto tiene el indicador del router?
- Teclear el comando **show running-config** para que el router muestre el archivo de configuración activo. ¿Había una ruta IP con la ruta estática que se configuró en el archivo de configuración activo?
- Introducir el comando **copy running-config startup-config** en el indicador del router para registrar permanentemente los cambios de configuración en la memoria.
- Entrar el comando **ping xxx.xxx.xxx.xxx** en el indicador del router. La dirección xxx.xxx.xxx.xxx. corresponde al router vecino al que se le configuró una ruta estática. ¿Se pudo alcanzar la interfaz del router?
- Salir del router

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7 CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

Protocolos de Encaminamiento [online]. España: Ministerio de Educación, cultura y deporte. Centro Nacional de Información y Comunicación Educativa Madrid CNICE, 2001. Última actualización: 2003. Disponible en Internet: www.cnice.mecd.es/tecnologica/experto/protocolos/

# ANEXO R. LABORATORIO 18: CONFIGURACIÓN DE RIP E IGRP

## 1. GUÍA DE LABORATORIO

### 1.1 OBJETIVOS

- Configurar la red de la topología del semestre 2 por medio de los protocolos de enrutamiento RIP e IGRP.
- Analizar el comportamiento de los protocolos dinámicos RIP e IGRP.
- Estudiar la métrica de RIP e IGRP.

### 1.2 EQUIPOS UTILIZADOS

- 5 estaciones de trabajo de PC 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 seriales 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 CAT 6 de conexión directa para conectar los routers y estaciones de trabajo con hubs y switches.

## 1.3 MARCO TEÓRICO

El enrutamiento dinámico, se produce cuando los routers se envían entre sí mensajes periódicos de actualización de enrutamiento. Cada vez que un router recibe un mensaje que contiene nueva información, vuelve a calcular una nueva mejor ruta y envía esta nueva información actualizada a los demás *routers*. Los protocolos RIP e IGRP son ejemplos de protocolos de enrutamiento dinámico.

RIP es el protocolo más común para transferir información de enrutamiento entre *routers* ubicados en la misma red y se encarga de calcular las distancias hacia un destino. RIP permite que el *router* determine cuál es la ruta que usará para enviar datos, basándose en un concepto que se conoce como vector-distancia. Siempre que se transportan datos en un *router* y, por lo tanto, a través de un nuevo número de red, se considera que han realizado un salto. Si existen varias rutas hacia un destino, el *router* selecciona la ruta que tiene el menor número de saltos y este

resulta ser su único método utilizado como métrica de enrutamiento para averiguar la mejor ruta. El máximo número de saltos es 15. Si el destino se encuentra a más de 15 salto, se le considera inalcanzable.

IGRP es un protocolo desarrollado por Cisco Systems y fue creado para darle solución a problemas como el enrutamiento en grandes redes en donde era complicado manejar otro tipo de protocolos como el RIP. IGRP también es un protocolo de vector distancia, sin embargo, al determinar cuál es la mejor ruta también tiene en cuenta elementos como, por ejemplo, el ancho de banda, la carga, el retardo y la confiabilidad.

## 1.4 PROCEDIMIENTO

### 1.4 1. Configuración IGRP

- Antes de empezar la práctica del protocolo de enrutamiento IGRP, hay que asegurarse que el router no tenga ninguna configuración previa. Por medio del puerto de consola eliminar IGRP con el comando **no igrp xxx** y las rutas estáticas con **no ip route xxx.xxx.xxx.xxx**.
- Ejecutar el siguiente paso utilizando uno de los cinco router de la figura 16 (remitirse a la página 137). Cuando se va a configurar el router, él por defecto

toma el nombre “**Router**”, Pero se le puede asignar un nuevo nombre con host name (Lab_A o Lab_B ect..).

- Primero, hay que entrar al modo usuario para hacer Ping a todas las interfaces IP del router y todas las interfaces que se encuentran directamente conectadas a los routers vecinos. Qué interfaces del router responden con éxito a un ping?
- Mostrar los protocolos de enrutamiento usando el siguiente comando **Router> show ip protocols.** Está algún protocolo de enrutamiento definido?
- Entrar al modo privilegiado con **class password** usando el siguiente comando:

  **Router> enable**

  **Password: class**
- Mostrar la configuración que corre en la **RAM** con el comando **Router# show running-config.** Están definidas las rutas estáticas ?
- Entrar al modo de configuración con el comando **router#config term.**
- Habilitar IGRP en el router con el comando **router(config) # router igrp 100.** Qué cambio hubo en el router?
- Definir cuáles de las redes van a utilizar IGRP a través del siguiente comando **Router(config-router) # network xxx.xxx.xxx.xxx.** Qué respuesta arrojó el router?
- Repetir anterior con todas las redes conectadas al router directamente.
- Colocar Exit
- Colocar **CNCTL-Z**

- Mostrar los archivos de configuración del router en la RAM con el comando **router#show running-config.** Aparecen el protocolo IGRP y las redes definidas?
- Colocar el comando **router# copy run start** desde el modo privilegiado. Qué hace este comando?
- Mostrar el protocolo de enrutamiento establecido con el comando **router#show ip protocols.** Qué protocolo de enrutamiento aparece?
- Mostrar las tablas de enrutamiento IP que muestran las redes cuáles redes son conocidas por el router a través del comando **router# show ip route.** Qué redes aparecen en la lista?
- Mostrar las interfaces del router y sus estadísticas con el comando **router#show ip interface.** Qué interfaces están en uso?
- Habilitar **IGRP debugging** con el comando **router# debug ip igrp transactions.** Qué efecto tiene este comando?
- Revisar las características por defecto para los timers con el comando **router#show ip protocol.** Cuáles son las características básicas para los cuatro timers?: Update (actualizar), Invalid (invalidar), Hold Down (mantener bajo) y Flushed (nivelado)
- Reiniciar los timers de la red IGRP con los comandos:

  **Router# config term**

  **Router(config)# router igrp 100**

  **Router(config-router)# no timers basic**

Cuál es el propósito de este comando?

- Ajustar los timers de la red usando los siguientes comandos:

  **router# config term**

  **Router(config)# router igrp 100**

  **Router(config-router)# timer basic**

- Forzar la red para que cumpla con una distancia máxima de 2 saltos con los siguientes comandos:

  **Router# config term**

  **Router(config)# router igrp 100**

  **Router(config-router)# metric maximum-hosp 2**

- Desactivar el protocolo **IP debugging** con el comando **router#no debug ip igrp transactions.**

### 1.4.2 Configuración RIP

- Conectarse al router y colocar el login. Entrar password cisco.
- Probar conectividad de la capa 3 colocando **ping xxx.xxx.xxx.xxx** a todas las interfaces del router y los router vecinos. Todas las interfaces respondieron con éxito el ping?

- Colocar **show ip route** en el router. Aquí, el router responde con esta tabla de enrutamiento. Hay algún protocolo definido?
- Colocarse en el modo privilegiado con el comando **enable.** Colocar el **password class.**
- Colocar **show running-config** en el indicador del router. Aquí, se muestra información sobre los archivos de configuración activos. Existe rutas estáticas definidas?
- Colocarse en modo de configuración global con el comando **configure terminal.** Esto es para poder configurar al router.
- Habilitar el protocolo de enrutamiento RIP con el comando **router rip**. Qué cambios hay en el router?
- Habilitar RIP en una red ip particular. Colocar **network xxx.xxx.xxx.xxx**. en el router. La anterior es la dirección de la red en la que se quiere habilitar RIP.
- Repetir el paso anterior con todas las redes conectadas al router.
- Salir del modo de configuración del router con **exit.** Aquí, el router saldrá del modo de configuración y estará en el modo de configuración global. Teclear **exit** y salir del modo configuración global.
- Escribir el comando **show running-config** para ver el archivo de configuración activo. Pueden observarse el protocolo RIP y las redes definidas?
- Copiar la configuración activaa la configuración de backup con el comando **copy running-config startup-config.** Qué hace este comando?

- Escribir **show IP protocols** para observar los valores acerca de los timers y de la información asociada a la red con el router. Cuando es la próxima actualización debida?
- Escribir show IP route para observar la tabla de enrutamiento. Cuántas rutas fueron descubiertas por RIP?
- Introducir **show IP interfaces** para ver el estado y los parámetros asociados con una interface. Qué información se obtuvo de este comando?
- Salir del router con **exit.**

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7 CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet:

http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

Protocolos de Encaminamiento [online]. España: Ministerio de Educación, cultura y deporte. Centro Nacional de Información y Comunicación Educativa Madrid CNICE, 2001. Última actualización: 2003. Disponible en Internet: www.cnice.mecd.es/tecnologica/experto/protocolos/

# ANEXO S. LABORATORIO 19: DIAGNÓSTICO DE FALLAS

## 1. GUÍA DE LABORATORIO

### 1.1 OBJETIVOS

- Diagnosticar las fallas en la red de laboratorio de 5 routers.
- Documentar los problemas detectados y las medidas correctivas que se han tomado.

### 1.2 EQUIPO UTILIZADO

- 5 estaciones de trabajo de PC 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 seriales 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 CAT 6 de conexión directa para conectar los routers y estaciones de trabajo con hubs y switches.

## 1.3 MARCO TEÓRICO

Las redes se establecen desde un punto de vista de seguridad y trabajo óptimo a cierto nivel que permita trabajar en ellas de manera confiable. Sin embargo, no se encuentran libres de posibles fallas que puedan afectar cualquier proceso que se esté llevando a cabo.

Los errores de Capa 1 incluyen:

- Cables rotos
- Cables desconectados
- Cables conectados a los puertos incorrectos
- Conexión de cable intermitente
- Cables incorrectos para la tarea
- Problemas del *transceiver*
- Problemas del cable DCE
- Problemas del cable DTE

- Dispositivos apagados

Entre los errores de Capa 2 se mencionan:

- Interfaces seriales incorrectamente configuradas
- Interfaces Ethernet incorrectamente configuradas
- Encapsulamiento incorrecto (HDLC es el encapsulamiento por defecto para las interfaces seriales)
- Configuraciones de temporización incorrectas en las interfaces seriales

Algunos de los errores de Capa 3 se definen a continuación:

- Protocolo de enrutamiento inhabilitado
- Protocolo de enrutamiento incorrecto habilitado
- Direcciones IP incorrectas
- Máscaras de subred incorrectas
- Enlaces DNS a IP incorrectos

Las herramientas que se pueden utilizar para el software (IOS) incluyen ping, trace, ip route, telnet, y show arp. Con ellas se puede examinar la red y establecer las fallas que se presentan.

## 1.4 PROCEDIMIENTO

- Implementar y revisar las conexiones físicas en la configuración de laboratorio estándar (ver figura 16, página 137).
- Diagnosticar los problemas de red inducidos. Los problemas básicos son los siguientes:

    1. No se puede hacer ping a un host en la red de LAB-E desde un host en la red de LAB-A.
    2. No se puede hacer telnet desde un router al nombre de host de otro router.

- Se causarán algunas fallas a propósito para luego examinar dichos problemas
- Anotar los problemas a medida que se vayan detectando y luego se debe indicar la solución a ellos. Luego de hacer ping desde una estación de trabajo en la red de Lab-A hacia una estación de trabajo en la red de Lab-E y hacer telnet desde un router al nombre de host de otro router, verificar si realmente se han solucionado todos los problemas.

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7 CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 2 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054163264868331,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna2v2121001l,Engine=static/toc.html

# ANEXO T. LABORATORIO 20: CONFIGURACIÓN PPP

## 1. GUÍA DE LABORATORIO

### 1.1 OBJETIVOS

- Comprender como afecta el encapsulamiento WAN de tipo serie síncrono.
- Analizar la conversión desde HDLC para el encapsulamiento PPP en una WAN.

### 1.2 EQUIPO UTILIZADO

- 2 routers para crear una WAN y encapsular HDLC para crear una conexión entre los routers.
- Cable de consola para configurar el router.

### 1.3 MARCO TEÓRICO

Los protocolos de WAN trasladan los datos de una ubicación a otra a través de una interfaz serie asíncrona o síncrona. Las transmisiones series síncronas son

señales digitales que se transmiten con una temporización precisa de un dispositivo a otro. Por otra parte, la transmisión asíncrona no se realiza con temporización precisa y confía en la información de control (bits de inicio y finalización) que indica el inicio y la finalización de los datos.

PPP se creó para solucionar los problemas de conectividad remota de Internet. Además, PPP era necesario para poder asignar direcciones IP de forma dinámica y permitir el uso de múltiples protocolos. PPP suministra conexiones de *router* a *router* y de *host* a red a través de circuitos síncronos y asíncronos.

PPP es el protocolo WAN más popular y más ampliamente utilizado porque ofrece todas estas funciones:

- Control de la configuración del enlace de datos
- Proporciona asignación dinámica de direcciones IP
- Multiplexión de protocolo de red
- Configuración de enlace y verificación de la calidad del enlace
- Detección de errores
- Opciones de negociación para destrezas tales como negociación de la dirección de capa de red y negociaciones de compresión de datos.

## 1.4 PROCEDIMIENTO

- Observar la figura 15 (remitirse a la página 124), y usar el comando **Lab_A#show running-config** para responder las siguientes preguntas:

    1. Cuál es la interface serial usada por la WAN?
    2. Cuál es la dirección IP de esta interface?
    3. Cuál es la máscara de subred de esta interface?
    4. Esta interface es una conexión DCE o DTE?
    5. Cómo se identifica una conexión DCE y DTE?
    6. Cuál es la rata de reloj establecida por esta interface?
    7. De cuánto es el ancho de banda establecido por esta interface?

- Examinar los cables WAN que están conectados al router Lab_A y responder las siguientes preguntas:

    1. Cuál es la interface que está conectada al router Lab_A?
    2. Qué tipo de conector está en la conexión física del puerto serial del router?
    3. Qué tipo de conector físico está al otro lado del cable?

- Introducir el comando **Lab_A#show interface serial 0** y responder las siguientes preguntas:

1. Cuál es el estado de la interface y la línea de protocolos?
2. Cuál es la dirección IP y la máscara de subred mostrados?
3. Qué es la unidad de transmisión máxima (MTU)?
4. Cuánto es el ancho de banda establecido?
5. Cuál es el propósito de encapsular?

- Cambiar el ancho de banda establecido del serial S0 con los siguientes comandos:

**Lab_A#config t**

**Lab_A(config)#int s0**

**Lab_A(config-if)#no bandwidth**

Utilizar el comando show interface S0 otra vez. Cuál es el ancho de banda establecido ahora?

Por qué sucede esto?

- Cambiar nuevamente el ancho de banda a 56Kbits con los siguientes comandos:

**Lab_A#config t**

**Lab_A(config)#int s0**

**Lab_A(config-if)#bandwidth 56**

Usar el comando **show interface s0** para verificar el ancho de banda.

- Mirar la configuración de la interface WAN del router Lab_B. Para ello, se debe hacer telnet desde el router Lab_A a Lab_B y usar el comando **show running-config** para responder las siguientes preguntas:

1. Cuál es la interface serial usada por la WAN?
2. Cuál es la dirección IP de esta interface?
3. Cuál es la máscara de subred de esta interface?
4. Esta interface es una conexión DCE o DTE?
5. Cómo se identifica una conexión DCE y DTE?
6. Cuál es la rata de reloj establecida por esta interface?
7. De cuánto es el ancho de banda establecido por esta interface?

- Examinar los cables WAN que están conectados al router Lab_B y responder las siguientes preguntas:

1. Cuál es la interface que está conectada al router Lab_B?
2. Qué tipo de conector está en la conexión física del puerto serial del router?

3. Qué tipo de conector físico está al otro lado del cable?

- Introducir el comando **Lab_B#show interface serial 1** y responder las siguientes preguntas:

1. Cuál es el estado de la interface y la línea de protocolos?
2. Cuál es la dirección IP y la máscara de subred mostrados?
3. Qué es la unidad de transmisión máxima (MTU)?
4. Cuánto es el ancho de banda establecido?
5. Cuál es el propósito de encapsular?

- Cambiar la encapsulación WAN de HDLC a PPP en el router Lab_A. Conectar el PC con el router Lab_A por el puerto de consola y usar los comandos para cambiar la encapsulación WAN en la interface serial 0 del router Lab_A:

**Lab_A(config)#interface serial 0**

**Lab_A(config-if)#encapsulation ppp**

Responder las siguientes preguntas:

1. Al utilizar el comando **show interface s0**, cuál es el estado de la interface y la línea de protocolo ahora?

2. Cuál era la encapsulación de antes?
3. Cual es el encapsulamiento establecido ahora?
4. Se puede hacer ping o telnet del router Lab_A al router Lab_B? Por qué?

- Cambiar la encapsulación WAN de HDLC a PPP en el router Lab_B. Conectar el PC con el router Lab_B por el puerto de consola y usar los comandos para cambiar la encapsulación WAN en la interface serial 1 del router Lab_B:

**Lab_B#config t**

**Lab_B(config)#interface serial 1**

**Lab_B(config-if)#encapsulation ppp**

Responder las siguientes preguntas:

1. Al utilizar el comando **show interface s1**, cuál es el estado de la interface y la línea de protocolo ahora?
2. Cuál era la encapsulación de antes?
3. Cual es el encapsulamiento establecido ahora?
4. Se puede hacer ping o telnet del router Lab_A al router Lab_B? Por qué?

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7CONCLUSIONES

## BIBLIOGRAFÍA

LEINWAND, Allan y PINSKY, Bruce. Configuración de Routers Cisco. 2ª. Edición. Madrid: Cisco Press, 2001.

# ANEXO U. LABORATORIO 21: CONFIGURACIÓN FRAME RELAY

## 1. GUÍA DE LABORATORIO

### 1.1 OBJETIVOS

- Estudiar la tecnología Frame Relay de la familia WAN
- Comprender los requerimientos y opciones de la comunicación Frame Relay
- Simular la configuración de una red Frame Relay conmutada entre dos routers.

### 1.2 EQUIPO UTILIZADO

- 3 routers Cisco con el IOS 11.2 o el más reciente.
- Cable WAN
- Hub y/o switches unidos al router
- Cable de consola
- Estaciones de trabajo

## 1.3 MARCO TEÓRICO

*Frame Relay* es una forma de enviar información a través de una WAN dividiendo los datos en paquetes. Cada paquete viaja a través de una serie de *switches* en una red *Frame Relay* para alcanzar su destino. Opera en las capas física y de enlace de datos del modelo de referencia OSI, pero depende de los protocolos de capa superior como TCP para la corrección de errores. *Frame Relay* se planteó originariamente como un protocolo destinado a utilizarse con las interfaces RDSI. Actualmente, *Frame Relay* es un protocolo de capa de enlace de datos conmutado de estándar industrial, que maneja múltiples circuitos virtuales mediante el encapsulamiento de Control de enlace de datos de alto nivel (HDLC) entre dispositivos conectados. *Frame Relay* utiliza circuitos virtuales para realizar conexiones a través de un servicio orientado a conexión.

## 1.4 PROCEDIMIENTO

En esta práctica de laboratorio no se implementará un circuito Frame Relay sino que se presentará una simulación de laboratorio. Esto se debe a que en la vida real la unión entre los routers es una nube. El propósito de esta práctica es presentar el proceso de configuración del router conectado a una Frame Relay de una conexión WAN.

Para llevar a cabo esta experiencia, se debe seleccionar 3 routers que tengan serial WAN. Conectarlos entre ellos. El router del centro simula una frame relay conmutada. Aquí se pretende simular que los routers se encuentran separados geográficamente. Se configurarán los routers Lab_A y Lab_C como remotos y el del medio (Lab_B) como Frame Relay.

- Para la configuración de la parte física de los 3 routers, entrar el comando **show controller S0** para la conexión DCE/DTE. Qué indica este comando?
- Revisar la interface WAN en router remoto Lab_A y responder las siguientes preguntas:
  1. Cuál es la dirección IP y número de bits de la subred de esta interface?
  2. Cuál es el estado de la interface y la línea de protocolo?
  3. Cuál es el encapsulamiento que presenta actualmente?
- Configurar la interface serial en Lab_A para una conexión Frame Relay. Para ello, se debe conectar la estación de trabajo al router Lab_A por medio del puerto de consola y utilizar los comandos de Frame relay en la **interface serial 0.**

  **Lab_A#config t**

  **Lab_A(config)#interface serial 0**

  **Lab_A(config-if)#ip address 201.100.11.1 255.255.255.0**

  **Lab_A(config-if)#encapsulation frame-relay**

  **Lab_A(config-if)#no shutdown**

**exit**

La configuración para la interfece E0 es la siguiente:

**Lab_A(config)#interface Etherneth0**

**Lab_A(config-if)#ip address 192.5.5.1 255.255.255.0**

**Lab_A(config-if)#no shutdown**

**exit**

La configuración del protocolo de enrutamiento IGRP es la siguiente:

**Lab_A(config)#router igrp 100**

**Lab_A(config-router)#network 201.100.11.0**

**Lab_A(config-router)#network 192.5.5.0**

**<controlz> y copy run start**

- Usar el comando **show running-config** para verificar la configuración de la interface de s0. Qué información se obtuvo de la interface s0 de Lab_A?
- Revisar la interface WAN en el router remoto Lab_C. para ello, se debe conectar la estación de trabajo con el router Lab_C por el puerto de consola y usar el comando show interface y responder las siguientes preguntas:
  1. Cuál es la dirección IP y número de bits de la subred de esta interface?
  2. Cuál es el estado de la interface y la línea de protocolo?
  3. Cuál es el encapsulamiento que presenta actualmente?
- Configurar la interface serial en Lab_C para una conexión Frame Relay. Para ello, se debe conectar la estación de trabajo al router Lab_C por medio del

puerto de consola y utilizar los comandos de Frame relay en la **interface serial 1.**

**Lab_C#config t**

**Lab_C(config)#interface serial 1**

**Lab_C(config-if)#ip address 201.100.11.2 255.255.255.0**

**Lab_C(config-if)#encapsulation frame-relay**

**Lab_C(config-if)#no shutdown**

**exit**

La configuración para la interface E0 es la siguiente:

**Lab_C(config)#interface Etherneth0**

**Lab_C(config-if)#ip address 223.8.151.1  255.255.255.0**

**Lab_C(config-if)#no shutdown**

**exit**

La configuración del protocolo de enrutamiento IGRP es la siguiente:

**Lab_C(config)#router igrp 100**

**Lab_C(config-router)#network 201.100.11.0**

**Lab_C(config-router)#network 223.8.151.0**

**<controlz> y copy run start**

- Usar el comando **show running-config** para verificar la configuración de la interface s1.  Qué información muestra la interface serial s1 de Lab_C?
- Configurar Lab_B como un switche Frame Relay.  Para ello, se debe conectar la estación de trabajo al router Lab_B por medio del puerto de consola y utilizar

los comandos para habilitar el switcheo Frame Relay y definir las **interfaces serial 0 y serial 1** como DCE. La configuración del switch frame relay se muestra a continuación:

**Lab_B#config t**

**Lab_B(config)#frame-relay switching**

La configuración de la interface s0 es así:

**Lab_B(config)#interface serial0**

**Lab_B(config-if)#no ip address**

**Lab_B(config-if)#encapsulation frame-relay**

**Lab_B(config-if)#clock rate 56000**

**Lab_B(config-if)#frame-relay intf-type dce**

**Lab_B(config-if)#frame-relay route 21 interface serial 1 20**

**Lab_B(config-if)#no shutdown**

La configuración para la interface S1 es la siguiente:

**Lab_B(config)#interface serial1**

**Lab_B(config-if)#no ip address**

**Lab_B(config-if)#encapsulation frame-relay**

**Lab_B(config-if)#clock rate 56000**

**Lab_B(config-if)#frame-relay intf-type dce**

**Lab_B(config-if)#frame-relay route 20 interface serial 0 21**

**Lab_B(config-if)#no shutdown**

**Control z y copy run start**

- Utilizar el comando **show running-config** para verificar la configuración de s0 y s1. Qué información muestra la interface s0 de Lab_B? Qué información muestra la interface s1 de Lab_B?
- Confirmar que la línea se encuentra activada utilizando el comando **show interface serial 0.** Cuál es el estado del link de trama serial?Cuántos mensajes LMI se han enviado? Cuántos se han recibido? A que tipo de LMI corresponde?
- Verificar el estado PVC de Frame Relay para el router Lab_A a través del comando **Lab_A#show frame pvc.** Cuál es el número DLCI de la conexión? Cuál es el estado del PVC?
- Revisar el mapa de Frame relay del router Lab_A con el comando **Lab_A#show frame map.** Cuál es el número de interface local, dirección IP de la interface conmutada y el DLCI de la conexión?
- Mirar el estado del LMI del router Lab_A con el comando **Lab_A#show frame lmi.** Cuál es el número de la interface local? Es DCE o DTE?
- Verificar el estado del PVC de frame relay del router Lab_B con el comando **Lab_B#show frame pvc.** Cuál es el número del DLCI de la conexión? Cuál es el estado de los PVCs?
- Verificar las tablas de enrutamiento de frame relay del router Lab_B con el comando **Lab_B# show frame route.** Qué clase de información se muestra? Input, intf,input DLCI, output intf, output DLCI y estado.

- Verificar el estado PVC de frame relay para el router Lab_B (el switch) con el comando **Lab_A#ping 201.100.11.2.** Cuál fue el resultado de esto?

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7 CONCLUSIONES

## BIBLIOGRAFÍA

LEINWAND, Allan y PINSKY, Bruce. Configuración de Routers Cisco. 2ª. Edición. Madrid: Cisco Press, 2001.

# ANEXO V. LABORATORIO 22: LISTAS DE CONTROL DE ACCESO ACL

## 1. GUIA DE LABORATORIO

### 1.1 OBJETIVOS

- Revisar las características y capacidades de las ACL estándar y extendidas.
- Construir una ACL estándar que permita o niegue tráfico específico.
- Construir una ACL extendida que permita o niegue tráfico específico.
- Aplicar una ACL estándar a una interface del router.
- Aplicar una ACL extendida a la interfaz de un router.
- Probar la ACL estándar para determinar si fueron archivados los resultados deseados.
- Probar la ACL extendida para determinar si fueron archivados los resultados deseados.

### 1.2 EQUIPO UTILIZADO

- 5 routers con hubs y switches (ver topología del semestre 2, página 137).
- Estación de trabajo conectada al router por el puerto de consola.

## 1.3 MARCO TEÓRICO

Existen muchas maneras de controlar el acceso a la red, sin embargo, se deben buscar formas que permitan el acceso por parte del personal autorizado e impedir el acceso no autorizado a la red. Para ello, fueron creadas las listas de control de acceso, ACL (*Access Control Lists)*, las cuales consisten en un grupo de sentencias de permiso o rechazo que se aplican a direcciones o protocolos de capa superior.

Las ACL son listas de instrucciones que se aplican a una interfaz del *router* y le indican a éste qué tipos de paquetes debe aceptar y cuáles denegar. La aceptación y rechazo se basa en información específica como dirección origen, dirección destino y número de puerto.

Los tipos de ACL son:

- **Estándar:** Éste tipo de ACL usa cuando se desea bloquear todo el tráfico de una red, permitir todo el tráfico desde una red específica o denegar conjuntos de protocolo. Las ACL estándar comprueban las direcciones de origen de los paquetes que solicitan enrutamiento. Lo anterior permite o deniega el resultado para todo un conjunto de protocolos, según las direcciones de red, subred y *host*.

- **Extendidas:** Las ACL extendidas se usan para verificar condiciones ya que brindan más opciones de control que las ACL estándar. Las ACL extendidas comprueban tanto la dirección origen como la destino de cada paquete. También pueden verificar protocolos, números de puerto y otros parámetros específicos.

## 1.4 PROCEDIMIENTO

### 1.4.1 Aplicación de una ACL Estándar

Para empezar, se realizarán dos ejercicios para luego, aplicarlos en el transcurso de la práctica.

- **Ejercicio A.** En la ACL1, se impedirá el tráfico IP de un host específico (estación de trabajo con la dirección IP 192.5.5.2) conectado al hub de la interface E0 de Lab_A, del alcance de una red completa (210.93.105.0, la red entre Lab_D y Lab_E).
- **Ejercicio B.** En la ACL2, se impedirá el tráfico IP de todos los host de unared específica, 219.17.100.0 (red fuera de lab_B) del alcance de una red completa (223.8.151.0, red fuera de Lab_C). Este ejercicio es opcional.

- Construir la ACL. Para esto, se define la ACL en el modo roter(config)# ya sea para impedir el paso a un host o a una red completa: **access_list#[permit/deny] source IP address [máscara][log].**

  El número [#] está entre 1-99 para una ACL estándar. Responder las siguientes preguntas:

  1. Cuál es el propósito de un cero en una máscara?
  2. Cuántos números de bits representa un cero en una máscara?
  3. Cuál es el propósito del 255 en una máscara?
  4. Cuántos números de bits representa el 255?
- Verificar la ACL con el comando **show access-list 1.** Si se va a corregir algún error, se debe borrar la ACL y empezar de nuevo. Al borrarla, se repite la parte del comando **access-list#** con la palabra **NO** enfrente. Cuántas características tiene la ACL?
- Aplicar la ACL a una interface del router. Aquí se aplicará la ACL1 en la interface s1 del router Lab_D y la ACL2 se aplicará en la interfaz E0 de Lab_C. Escoger si se va a denegar un host o una red completa. Utilizar los comandos:

  **Router(config)#interface serial 1**

  **Router(config-if)#ip access-group 1 in**
- Verificar el funcionamiento de la ACL con el comando **show running-config.**

### 1.4.2 Aplicación de una ACL extendida

Para empezar, se plantearán dos ejercicios que se aplicarán en la práctica:

- **Ejercicio A.** Impedir el tráfico telnet de un host específico, 192.5.5.2 (estación fuera de Lab_A) del alcance de la red completa 210.93.105.0 (red entre lab_D y Lab_E).
- **Ejercicio B.** Impedir el tráfico telnet de un host específico, 210.93.105.2 (estación fuera de Lab_E) del alcance de la red completa 192.5.5.0 (fuera de Lab_A).
- Construir la ACL. Para esto, se define la ACL en el modo roter(config)# ya sea para impedir el paso a un host o a una red completa: **access_list#[permit/deny] [protocol] source IP wildcard mask [port] dest. IP wildcard mask [port] [established] [log] [other options]address [máscara][log].**

  El número [#] está entre 100-199 para una ACL extendida. Responder las siguientes preguntas:

  1. Cuál es la máscara del encabezado fuente dado como 0.0.0.0?
  2. Cuál es la máscara del encabezado de destino dado como 0.0.0.255?
  3. Qué se revisa con el comando **eq telnet**?
- Verificar la ACL con el comando **show access-list 101.** Si se va a corregir algún error, se debe borrar la ACL y empezar de nuevo. Al borrarla, se repite la parte del comando **access-list#** con la palabra **NO** enfrente. Cuántas características tiene la ACL?

- Aplicar la ACL a una interface del router. En cualquier router, sea Lab_B o Lab_D, se podría aplicar un filtro que impida el paso de paquetes telnet del router Lab_A de ser transmitido a la LAN D/E (red 210.93.105.0)? En qué interfaz está aplicada la lista ? Completar los comandos:

  **Router(config)#**

  **Router(config-if)#**

  En cualquier router, sea Lab_B o Lab_D, se podría aplicar un filtro que impida el paso de paquetes telnet del router Lab_E de ser transmitido a la LAN D/E (red 201.100.11.0)? En qué interfaz está aplicada la lista? Completar los comandos:

  **Router(config)#**

  **Router(config-if)#**

- Verificar el funcionamiento de la ACL con el comando **show running-config.**

## 1.5 ANÁLISIS DE RESULTADOS

## 1.6 RECOMENDACIONES

## 1.7 CONCLUSIONES

## BIBLIOGRAFÍA

Curriculum CCNA (Cisco certified network associate curriculum) Semester 3 [online]. Cisco System, Inc. Cisco Networking Academy Program, 2000. Versión 2.1.2 en español. Disponible en Internet: http://curriculum.netacad.net/servlet/org.cli.delivery.rendering.servlet.CCServlet/SessionID=1054916637179372,LMSID=CNAMS,Theme=cnamstheme,Style=ccna,Language=es,Version=1,RootID=knet-btccna3v2121001l,Engine=static/toc.html

## ANEXO W. GLOSARIO

**Buffer:** Separador

**Comando:** Sentencia con la cual se puede ejecutar una orden o función en un dispositivo en el cuál se puede programar o configuración, por ejemplo, un router.

**Confiabilidad:** Indica la actual tasa de error. Es una fracción de los paquetes que llegan al destino sin error. Se mide.

**Datagrama:** Paquete de capa 3 (capa de red), en el cual se encapsulan los datos para luego pasar a la capa 2 (capa de enlace de datos).

**Dirección de broadcast:** Es una dirección compuesta exclusivamente por números unos en el campo de host. Cuando se envía un paquete de broadcast en una red, todos los dispositivos de la red lo captan.

**Hardware:** Es conjunto formado por todos los elementos físicos de un sistema informático, como CPUs, terminales, cableado, medios de almacenamiento secundario (cintas, CD-ROMs, diskettes...) o tarjetas de red.

**Host:** Estación de trabajo

**Hub:** Dispositivo que concentran conexiones LAN y permiten el uso de medios de cobre de par trenzado.

***Maximun Transfer Unit*** **(MTU):** La MTU es el máximo tamaño de paquete que puede ser enviado a lo largo de todo el trayecto sin fragmentación.

**Ocupación de la línea:** Indica cuánto de este ancho de banda está actualmente en uso. Éste es medido y cambiará con la carga.

**Protocolo:** Conjunto de reglas que hacen que la comunicación en una red sea más eficiente y que determinan el formato y la transmisión de datos.

**Retardo de la topología:** Es la cantidad de tiempo que pasa hasta llegar al destino a través de la ruta, asumiendo una red no cargada. Desde luego hay un retardo adicional cuando la red está cargada. De todos modos, la carga se mide por la ocupación del canal, no intentando medir el retraso actual.

**Router:** Dispositivo que opera en la capa 3 del modelo OSI (capa de red). Interconectan segmentos de red o redes enteras y hacen pasar paquetes de datos entre redes tomando como base la información de capa3.

**Sistema Autónomo:** esta compuesto por routers, administrados por uno o más operadores, que presentan una visión coherente del enrutamiento ante el mundo exterior.

**Software:** Es el conjunto de programas lógicos que hacen funcional al hardware, tanto sistemas operativos como aplicaciones.

**Subred:** Partes más pequeñas en las cuales se subdividen las redes. Proporcionan flexibilidad al direccionamiento.

**Switch Ethernet:** Dispositivo que brinda ancho de banda dedicado full-dúplex a tráfico proveniente de estaciones de trabajo o segmentos.