CONMUTACIÓN, ENRUTAMIENTO Y TECNOLOGÍAS WAN

DAISSY MARÍA PAYARES BENÍTEZ

MARIANELLA FANDIÑO NIETO

UNIVERSIDAD TECNOLÓGICA DE BOLIVAR

FACULTAD DE INGENIERIA

PROGRAMA DE INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS

2004

CONMUTACIÓN, ENRUTAMIENTO Y TECNOLOGÍAS WAN

DAISSY MARÍA PAYARES BENÍTEZ

MARIANELLA FANDIÑO NIETO

Monografía presentada como requisito para optar el título de Ingenieras de Sistemas

Director

Ing. ISAAC ZÚÑIGA SILGADO

Docente de Tiempo Completo

UNIVERSIDAD TECNOLÓGICA DE BOLIVAR

FACULTAD DE INGENIERIA

PROGRAMA DE INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS

2004

AUTORIZACIÓN

Cartagena de Indias D.T. y C., Mayo de 2004

Nosotras **DAISSY MARÍA PAYARES BENÍTEZ** y **MARIANELLA FANDIÑO NIETO**, identificadas con cédulas de ciudadanía No. **45'540.806** de Cartagena y **45'541.223** de Cartagena, autorizamos a la Universidad Tecnológica de Bolívar para hacer uso de nuestro trabajo de grado y publicarlo en el catálogo online de la Biblioteca.

DAISSY Ma. PAYARES BENÍTEZ
c.c. No. 45'540.806 de Cartagena

MARIANELLA FANDIÑO NIETO
c.c. No. 45'541.223 de Cartagena

Cartagena de Indias, 28 de Mayo 2004.

Señores:
UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR.
Comité de Evaluación de Proyectos.
Escuela de Ingenierías.
Ciudad.

Estimados Señores:

De la manera más cordial, nos permitimos presentar a ustedes para su estudio, consideración y aprobación el trabajo final titulado **"CONMUTACIÓN, ENRUTAMIENTO Y TECNOLOGÍAS WAN"**, presentado para aprobar el Minor en Comunicaciones y Redes.

Esperamos que este proyecto sea de su total agrado.

Cordialmente,

DAISSY Ma. PAYARES BENÍTEZ
c.c. No. 45'540.806 de Cartagena

MARIANELLA FANDIÑO NIETO
c.c. No. 45'541.223 de Cartagena

Cartagena de Indias, Mayo 28 de 2004.

Señores:
UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR.
Comité de Evaluación de Proyectos.
Escuela de Ingenierías.
Ciudad.
Señores:

Estimados Señores:

Con el mayor agrado me dirijo a ustedes para poner a consideración el trabajo final titulado **"CONMUTACIÓN, ENRUTAMIENTO Y TECNOLOGÍAS WAN"**, el cual fue llevado a cabo por los estudiantes **DAISSY MARÍA PAYARES BENÍTEZ** y **MARIANELLA FANDIÑO NIETO**, bajo mi orientación como Asesor.

Agradeciendo su amable atención,

Cordialmente,

ISAAC ZÚÑIGA SILGADO
Ingeniero de Sistemas.

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Cartagena de Indias D.T. y C, Mayo de 2004

...A Dios,

A mis Padres, Zayda y Heriberto,

A mis hermanos, Erika Paola y Airton,

Al resto de mi familia y amigos.

Daissy María

...A mis padres, Nelly y Adolfo,

A mis hermanos, Adriana y Jesús

A mi abuela, Carmen

A mi tía, Carmen Alicia

Marianella

AGRADECIMIENTOS

Nuestros más sinceros agradecimientos a:

A Dios, por mantenernos con salud y vitalidad para llevar a cabo nuestros logros Académicos.

A nuestro Director de monografía, MBA. Isaac Zúñiga Silgado, Ingeniero de Sistemas y Docente de tiempo completo de nuestra Universidad, por su acompañamiento, apoyo y colaboración antes y durante el desarrollo del trabajo de grado.

A nuestros padres, por darnos apoyo, fuerzas y los medios para lograr este gran reto académico.

A nuestros profesores y director de programa de Ingeniería de Sistemas, por su motivación y apoyo durante el desarrollo de nuestra carrera.

TABLA DE CONTENIDO

Pág.

LISTA DE CUADROS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

ATM: Modo de Transferencia Asíncrono, modo de conmutación rápida de paquetes donde se reenvían unidades de datos de longitud fija, o celdas, sin que tengan relación unos con otros en cuanto al tiempo.

Capa de aplicación: En el modelo OSI es la capa7. Esta capa brinda servicios a procesos de aplicación (como por ejemplo, correo electrónico, transferencia de archivos y emulación de terminal) que se encuentran fuera del modelo de referencia OSI. Identifica y establece la disponibilidad de los dispositivos con los que se pretende establecer comunicación (y de los recursos requeridos para conectarse con ellos), sincroniza las aplicaciones cooperantes y establece la concordancia de procedimientos para la recuperación de errores y el control de la integridad de los datos.

Capa de enlace de datos: En el modelo OSI es la capa 2. Proporciona tránsito confiable de datos a través de un enlace físico. Se ocupa del direccionamiento físico, topología de red, disciplina de línea, notificación de errores, entrega ordenada de las tramas y del control de flujo. IEEE dividió esta capa en dos subcapas: la subcapa MAC y la subcapa LLC. A veces se le denomina simplemente capa de enlace.

Capa de presentación: En el modelo OSI es la capa 6. Esta capa asegura que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. También se ocupa de las estructuras de datos que usan los programas y, por lo tanto, negocia la sintaxis de transferencia de datos para la capa de aplicación.

Capa de red: En el modelo OSI es la capa 3. Esta capa proporciona conectividad y selección de rutas entre dos sistemas finales. Es la capa en la que se produce el enrutamiento.

Capa de sesión: En el modelo OSI es la capa 5. Esta capa establece, administra y termina las sesiones entre aplicaciones y administra el intercambio de datos entre las entidades de la capa de presentación.

Capa de transporte: En el modelo OSI es la capa 4. Esta capa es responsable por la comunicación confiable de red entre nodos finales. Proporciona mecanismos para el establecimiento, el mantenimiento y la terminación de circuitos virtuales, la detección y recuperación de fallas de transporte y el control del flujo de información.

Capa Física: En el modelo OSI es la capa 1. La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales.

DCE: Equipo de comunicación de datos.

Distancia administrativa: Se utiliza para seleccionar el protocolo de enrutamiento que se prefiere cuando hay más de un protocolo en uso. El valor más bajo indica mayor preferencia. Por lo general, IGRP tiene una distancia administrativa más baja, será el protocolo preferido de enrutamiento.

DTE: Equipo de terminación de circuito de datos.

FDDI: Interfaz de datos distribuidos por fibra óptica, un estándar de Lan basado en una topología de doble anillo con canales de fibra óptica a 100Mbits/s., pero se trata de una opción costosa.

Frame Relay: Formato estándar para redes de conmutación rápida de paquetes donde los paquete se conmutan en la capa de enlace de datos del modelo OSI. Una trama intercambia un grupo de bits entre dispositivos que funcionan en el nivel de enlace de datos para el control de la información, revisión de errores y datos de usuarios.

Hub: Dispositivo de red multipuerto que permite repetir la señal, actualmente están siendo relevados por switches. Operan en modo Half duplex, es decir solo envían o solo reciben, operando solo en la capa 1 del modelo OSI: Capa Física. Debido a que comparten el ancho de banda se producen colisiones.

IGRP: Protocolo de enrutamiento de gateway interior. Protocolo de enrutamiento por vector distancia dinámico, es un protocolo patentado por Cisco, desarrollado a mediados de la década de los 80's, que utiliza métricas tales como el ancho de banda y el retardo para determinar la mejor ruta obteniendo mejores decisiones en sistema autónomos que incluya redes con rutas alternativas, redes que sean grandes y complejas. Publica tres tipos de rutas: Interior, Sistema y Exterior.

1. **Rutas interiores**: Son rutas entre subredes en la red conectada a una interfaz de router, se debe tener en cuenta que si la red está conectada a un router que no está dividido en subredes, IGRP no publica rutas interiores.
2. **Rutas de sistema**: Son rutas hacia redes ubicadas dentro de un sistema autónomo. El software Cisco IOS deriva rutas de sistema desde interfaces de red conectadas directamente y de información de ruta de sistema suministrada por otros routers que utilizan IGRP o servidores de acceso. Estas rutas no incluyen información de subred.
3. **Rutas exteriores**: Son rutas hacia redes ubicadas fuera del sistema autónomo que se tienen en cuenta al identificar un gateway de último recurso. El software Cisco IOS elige un gateway de último recurso de la lista de estas rutas que suministra IGRP. El software utiliza el gateway (router) de último recurso si no tiene una mejor ruta para el paquete y el destino no es una red conectada. Si el sistema autónomo tiene más de una conexión hacia una red externa, los distintos routers pueden seleccionar distintos routers exteriores como el gateway de último recurso.

LAN: Local Area Network. Red de área local. Red de datos de alta velocidad y bajo nivel de error que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan equipos terminales, periféricos y otros dispositivos en un solo edificio u otra área geográficamente limitada. Los estándares de LAN especifican el cableado y la señalización en la capa física y la capa de enlace de datos del modelo de referencia OSI. Ethernet, FDDI y Token Ring son tecnologías de LAN ampliamente utilizadas.

Latencia: Retraso de propagación es el tiempo que tarda una trama o paquete en ir desde un origen hasta el destino.

Modelo OSI: Modelo de referencia para Interconexión de Sistemas Abiertos. Modelo de arquitectura de red desarrollado por ISO e UIT-T. Está compuesto por siete capas, cada una de las cuales especifica funciones de red individuales, por ejemplo, direccionamiento, control de flujo, control de errores, encapsulamiento y transferencia confiable de mensajes. La capa superior (la capa de aplicación) es la más cercana al usuario; la capa inferior (la capa física) es la más cercana a la tecnología de medios. Las dos capas inferiores se implementan en el hardware y el software, y las cinco capas superiores se implementan sólo en el software. Este modelo se usa a nivel mundial como método para la enseñanza y la comprensión de la funcionalidad de la red.

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

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

Operación libre de fragmentos: Los switches tienen 3 modos de operación:

1. **Método de corte o rápido**: El switch sólo lee la dirección MAC destino del encabezado de la trama y luego envía inmediatamente la trama. Este modo es el más rápido pero también puede enviar fragmentos de colisión menores de 64 bytes (un runt).
2. **Almacenamiento y envío**: Espera hasta recibir la trama completa (hasta 1.518 bytes) antes de enviar la trama. Es el modo de conmutación más lento pero el que produce menos errores.
3. **Libre de fragmentos**: Reduce el retardo ya que toma la decisión de envío luego de recibir los primeros 64 bytes. Esto significa que no se enviará ningún "runt", que es el tipo más común de trama defectuosa de Ethernet, resulta la mejor opción para obtener un equilibrio entre la velocidad y la posibilidad de errores.

Los switches de Cisco se pueden configurar para que operen en modo Almacenamiento y envío, Libre de fragmentos o Conmutación rápida, según el modelo.

Organización: Empresas, Instituciones gubernamentales o no gubernamentales,

POTS: Plain Old Telephone Service, Servicio Telefónico Analógico Convencional. Término empleado en Estados Unidos para referirse al servicio telefónico básico, con teléfonos analógicos, ofrecido por las redes públicas.

PPP: Es un protocolo de red de área amplia (WAN) que proporciona servicios de capa 2: enlace de datos del modelo OSI para las conexiones router a router y host a red a través de circuitos síncronos y asíncronos utilizando una interfaz serial. Los PCs los utilizan habitualmente para conectarse a un proveedor de servicios de Internet (ISP) a través de una línea de acceso telefónico (host a red asíncrono) o como un método de encapsulamiento WAN entre varias LAN (router a router síncrono). Es un protocolo internacional, estandarizado y utilizado ampliamente, desarrollado por la Fuerza de Tareas de Ingeniería de Internet (IETF), se considera parte del conjunto de protocolo TCP/IP y soporta una cantidad de protocolos LAN, como IP e IPX, y diversos métodos de autenticación de seguridad, como PAP y CHAP, utilizado en diversos medios físicos, incluyendo cable de par trenzado, fibra o transmisión satelital. Utiliza una variante del control de enlace de datos de alto nivel (HDLC) para el encapsulamiento de paquetes.

Protocolo: Es el lenguaje o las normas de comunicación entre los dispositivos en una red. Descripción formal de un conjunto de reglas y convenciones que rigen la forma en la que los dispositivos de una red intercambian información. Campo dentro de un datagrama IP que indica el protocolo de capa superior (Capa 4) que envía el datagrama.

Protocolos de enrutamiento: Son los protocolos que utilizan los routers para comunicarse entre sí a fin de intercambiar información de forma dinámica acerca de las redes que pueden alcanzar y de la conveniencia de las rutas disponibles. Generalmente, se conocen como protocolos de enrutamiento dinámico y facilitan el proceso de enrutamiento. No son necesarios en una red pequeña si se utilizan solamente rutas estáticas. Los paquetes de protocolo de enrutamiento ocupan ancho de banda y operan independientemente de los paquetes de datos enrutados que atraviesan la red. No hay ninguna información en un paquete IP que se relacione con el protocolo de enrutamiento que se utiliza. Los routers se envían entre sí periódicamente información acerca de las rutas, este proceso se conoce como actualización de las tablas de enrutamiento, de modo que cuando reciben un paquete de protocolo enrutado (como IP) saben a dónde deben enviarlo. Si comparamos la dirección del protocolo enrutado con la dirección de una carta, se puede comparar el protocolo de enrutamiento con el mensajero que se traslada entre los routers para indicarles cuáles son la rutas que están abiertas y cuáles son las más rápidas. Los protocolos de enrutamiento se pueden clasificar en general según si son interiores o exteriores, y se subdividen por tipo: vector distancia o estado de enlace.

Protocolos enrutados: Son aquellos que se pueden enrutar. La información de direccionamiento de la Capa 3 del modelo OSI: Capa de red, se coloca en el encabezado del paquete de datos, lo cual permite que el paquete atraviese múltiples redes para llegar a su destino. Son conocidos también como protocolos enrutables, lo que significa que se pueden enrutar. Para que un protocolo se pueda enrutar, el método de direccionamiento debe tener por lo menos dos partes; un número de red y un número de host. Es la porción de red la que asocia la dirección que permite que un paquete se enrute desde una red a otra. Todos los dispositivos en una red generalmente ejecutan el mismo protocolo enrutado, que es similar a un lenguaje común, para poder comunicarse. La mayoría de los protocolos LAN son protocolos enrutados.

El protocolo enrutado más común es el Protocolo Internet o IP, que es un estándar internacional. IP a veces se denomina TCP/IP pero TCP en realidad es un protocolo de la capa 4 del modelo OSI: Capa de transporte, y no se involucra directamente con el protocolo IP enrutable que funciona en la Capa

3. Para que un dispositivo (computador, servidor, router, etc.) se pueda comunicar en Internet, debe ejecutar el protocolo IP. Las direcciones IP son de 32 bits y contienen una porción de red y una porción de host que asigna, típicamente, el administrador de la red. Otros protocolos de LAN enrutados son Novell IPX, AppleTalk y Decnet.

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

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

PSTN: Public Switched Telephone Network, Redes Públicas de Telefonía Conmutada. Término general que se refiere a la diversidad de redes y servicios telefónicos existentes a nivel mundial. Es la red telefónica básica empleada en todos los países para establecer las comunicaciones vocales. A veces se denomina servicio telefónico analógico convencional (POTS). Esta red fue diseñada originalmente para el uso de la voz y sistemas análogos. La conmutación consiste en el establecimiento de la conexión previo acuerdo de haber marcado un número que corresponde con la identificación numérica del punto de destino

Puertos seriales síncronos: Transmiten bits uno después del otro en una serie por el alambre o cable de fibra.

Red: Agrupación de computadores, impresoras, routers, switches y otros dispositivos que se pueden comunicar entre sí a través de un medio de transmisión. Instrucción que asigna una dirección basada en la NIC con la cual el router está directamente conectado. Instrucción que especifica cualquier red conectada directamente que se desee incluir.

Relés: Es un sistema mediante el cuál se puede controlar una potencia mucho mayor con un consumo en potencia muy reducido.

RIP: Protocolo de información de enrutamiento. Protocolo de enrutamiento por vector distancia, es el más antiguo y utiliza solamente el número de saltos como métrica para determinar la mejor ruta.

Switch: Dispositivo de red multipuerto que filtra, envía e inunda la red con tramas según la dirección de destino de cada trama, operando principalmente en la capa 2 del modelo OSI: Enlace de datos. Sirviendo de punto de conexión para computadores, hubs, servidores, routers y otros

switches. Opera en modo Full duplex y no tiene que detectar colisiones, lo cual permite crear circuitos virtuales entre los dispositivos conectados en sus puertos. Los switches son similares a los computadores, contienen CPU, RAM y un sistema operativo (IOS, Sistema Operativo Internetworking). Conectándose al puerto de consola del switch se permite ver y realizar cambios en la configuración, switches más modernos poseen un servidor Web (HTTP) incorporado y también se pueden manejar a través de su dirección IP utilizando un PC y una interfaz de navegador como Netscape o Internet Explorer.

WAN: Red de área amplia. Red de comunicación de datos que sirve a usuarios dentro de un área geográfica extensa y a menudo usa dispositivos de transmisión suministrados por proveedores de servicio comunes. Frame Relay, SMDS y X.25 son ejemplos de WAN.

RESUMEN

Esta monografía titulada "CONMUTACIÓN, ENRUTAMIENTO Y TECNOLOGÍAS WAN" es presentado por DAISSY MARÍA PAYARES y MARIANELLA FANDIÑO, enmarcada dentro del área de Comunicaciones y Redes del Programa de Ingeniería de Sistemas, donde se recopilan las prácticas de laboratorio presentada por la Academia Networking CISCO en los semestres Switching Basics and Intermediate Routing y WAN Technologies, además, incluye la fundamentación teórica de los laboratorios.

El desarrollo de esta monografía surge por la necesidad de aportar y mejorar el conocimiento y la documentación de las prácticas de laboratorios, ya que antes no se contaba con una herramienta diferente al material Online de Cisco. En este trabajo, se describen la conmutación, el enrutamiento y las tecnologías WAN. Con respecto a la conmutación veremos la historia, la visión, los tipos, los métodos y ventajas de su implementación. En cuanto a enrutamiento se encuentran los conceptos básicos, las clases, los protocolos de enrutamiento con sus características, ACL estándar y extendida, firewalls y filtrado de paquetes. Y de las tecnologías WAN se incluye una introducción a ellas, los estándares WAN, la capa física y la capa enlace de datos WAN, Frame Relay y RDSI (Red Digital de Servicios Integrados).

Las prácticas de laboratorio se pueden realizar, gracias a la sala de laboratorio de redes con la cuenta la Universidad Tecnológica de Bolívar. Ahora los estudiantes del Minor de Comunicaciones y Redes, cuentan con una nueva herramienta de documentación, donde también encontraran un CD que acompaña esta monografía con todos los apoyos bibliográficos y la documentación que se necesitaron para su realización. En el CD, se encuentra la guía completa de los laboratorios.

INTRODUCCIÓN

La Universidad Tecnológica de Bolívar, a través del Centro de Educación Permanente, junto con la Academia Networking Cisco, mediante el Minor en Comunicaciones y Redes, ofrece a estudiantes y profesionales la posibilidad de desarrollar las prácticas de laboratorios de Conmutación, Enrutamiento y Tecnologías WAN, para que en futuras oportunidades del ámbito laboral las implementen de manera más certera.

La presente monografía expone los laboratorios de los siguientes temas: **CONMUTACIÓN, ENRUTAMIENTO Y TECNOLOGÍAS WAN**. El desarrollo de los siguientes laboratorios contribuye a la compresión y afianzamiento de los conceptos que rodean las infraestructuras de las comunicaciones y redes.

Esperamos que esta monografía contribuya al mejoramiento de los cursos ofrecidos por nuestra Universidad en el área de las redes de la Ingeniería de Sistemas, en especial al Minor en Comunicaciones y Redes en convenio con la Academia Networking CISCO. Además, beneficia en la preparación para la Certificación de CISCO, recordemos este importante reto educacional que pretende certificar como profesional altamente cualificado a sus aspirantes, en principal instancia a los participantes del Minor de Comunicaciones y Redes de la Academia Cisco Networking, buscando así su incorporación en el mercado laboral, gracias a los conocimientos y a la habilidad adquirida

durante el desarrollo de los laboratorios, enriqueciendo de manera satisfactoria la experiencia necesaria para desenvolverse con normalidad en su entorno de trabajo.

Esta monografía contiene en sus primeros cuatro capítulos un aporte conceptual y profundización de los temas: conmutación, enrutamiento y tecnologías WAN. La Universidad Tecnológica de Bolívar cuenta con un dotado Laboratorio de Redes, en el cuarto piso del Campus de Ternera, dotado de diversos implementos, entre los cuales podemos nombrar: switches, routers Cisco y terminales de trabajo, también cuenta con docentes e instructores certificados por la Academia Networking Cisco para el desarrollo de los laboratorios incluidos en esta monografía.

CAPÍTULO I

GENERALIDADES DE LA CONMUTACIÓN, ENRUTAMIENTO Y TECNOLOGÍAS WAN

Actualmente en las organizaciones se vive la época moderna de la comunicación, caracterizada por la rapidez de las transmisiones y el intercambio de grandes volúmenes de información. La relación de las personas con el Internet y el correo electrónico toma fuerza por su mayor uso dentro de las organizaciones, en todas sus dependencias: administrativas, financiera, comercial, académica, etc. Mucha de la información que circula se destaca por ser aplicaciones multimedia y servicios sofisticados de la Web. Por lo anterior, demanda mayor exigencia el diseño o crecimiento de la infraestructura de la red que soporta las comunicaciones en cada organización. Cabe mencionar que uno de los objetivos en la implementación de una red, por ejemplo una red de computadores, es servir de medio de comunicación entre las personas que se encuentran distanciadas. En una organización es común que se permita disponer de este tipo de comunicaciones, puesto que se garantiza la rapidez y hace que la cooperación entre grupos de usuarios que se encuentran alejados, y que anteriormente había sido imposible de establecer, pueda realizarse ahora. En la infraestructura de la red de comunicaciones se requiere tener en cuenta muchos aspectos, de los cuales podemos nombrar: “disponibilidad de ancho de banda suficiente para garantizar la transmisión del tráfico por la red, reducir o eliminar las colisiones frecuentes en el tráfico de datos, disponibilidad total de la red y sus dispositivos, implementar tecnología basada en estándares pensando en la escalabilidad y las

posibilidades de migración"*. Ante estos aspectos y tan fundamentales en la construcción o expansión de una red se busca preparar a más personal interesado como potenciales Ingenieros de Sistemas, con gran atracción hacia el campo de las comunicaciones y redes.

Para aportar más a las comunicaciones y redes debemos resaltar los papeles que representan la conmutación, el enrutamiento y las tecnologías WAN dentro del diseño o expansión de la infraestructura de red. Por estos días, toma importancia la conmutación, que puede filtrar el tráfico de datos de forma más eficiente, reduciendo a cero el número de cargas innecesarias en la red. Esta es la principal característica de los dispositivos de conmutación a diferencia de los repetidores y los enrutadores.

En una perspectiva general en el campo de las comunicaciones y redes, se puede definir la conmutación como el proceso por medio del cual se comunican dos hosts a través de una infraestructura de comunicaciones común para transferir información. Observamos en el cuadro 1 diferentes servicios donde son utilizadas las técnicas de conmutación:

Cuadro 1. Técnicas de conmutación en diferentes servicios*

SERVICIO	CONMUTACIÓN		
	Circuito	Mensajes	Paquetes
Telefónico	X	X	
Telegráfico	X	X	
Datos	X	X	X

* Tomado del material entregado por el Ing. Jaime Rueda en el módulo LAN – MAN- WAN del Minor de Comunicaciones y Redes. 2003

* Los servicios de comunicaciones corporativos.
http://www.monografias.com/trabajos13/corpo/corpo.shtml

Ahora en palabras simples, podemos decir que el enrutamiento es la fase de enviar un paquete basándose en la IP destino. El enrutamiento, dentro de las comunicaciones y redes, se define como el proceso de descubrimiento de una ruta hacia la dirección host destino. Dentro de las grandes redes, el enrutamiento es sumamente complejo, debido a la gran cantidad de destinos intermedios potenciales que debe atravesar un paquete antes de llegar al host destino.

Una ruta es el camino que los datos deben realizar cuando viajan a través de una red desde un host a otro. Una de las capacidades características de la Internet, en comparación con otras arquitecturas de red, es que cada nodo que recibe un paquete determinará de inmediato por su cuenta cuál debe ser el próximo paso en la ruta.

Cuando un paquete de IP es recibido por un nodo de la red, éste decidirá qué hacer con él. Para realizar esta tarea consultará su tabla de enrutamiento. Existe el enrutamiento dinámico y estático. Las clases de enrutamiento pueden ser por vector distancia o por estado de enlace. Dentro de las comunicaciones y redes también existen protocolos de enrutamiento, aunque no se deben confundir con protocolos enrutados.

Las comunicaciones y redes según su alcance o escala se clasifican en LAN (Redes de Área Local), MAN (Redes de Área Metropolitana) y WAN (Redes de Área Extensa o de gran alcance). Las más usadas son las redes LAN, y se busca la expansión de ellas pero cuando ya se llega a un punto donde no es práctico implementar las redes LAN, como resultado de los enlaces de grandes distancia que extienden una LAN son la redes de área extensa, las conocidas WAN. Las redes WAN

se extienden sobre un área geográfica amplia. Algunas de las tecnologías WAN*son Frame Relay (Relevo de Tramas), ATM (Asynchronous Transfer Mode, Modo de Transferencia Asíncrono), ISDN (Integrated Services Digital Network, Red Digital de Servicios Integrados).

Finalmente, se dice que el Internet representa uno de los ejemplos más exitosos de las comunicaciones y redes, que se ha obtenido como beneficio de la inversión sostenida y del compromiso de investigación y desarrollo en infraestructuras informáticas. Muchos gobiernos, empresas industriales, la académica, y en general las organizaciones, han sido socios de la evolución y desarrollo de estas nuevas e interesantes tecnologías del mundo actual.

* BLACK, Ulyess. Tecnologías emergentes para redes de computadores. Segunda Edición. Pearson. 1999. Pág. 15

CAPÍTULO II

CONMUTACIÓN

2.1 Historia

En los años 50 surgió la conmutación electrónica, y en la década siguiente se enfoco al área de las redes, realizando algunos intentos de aplicación. Para la configuración de las redes públicas telefónicas conmutadas su método predominante fue la conmutación, en su forma de conmutación de circuitos. Siendo este un gran paso, gracias a la obtención de conexiones directa a la red. Y perfilándose como la primera de las muchas ventajas que pueda tener la conmutación en la aplicación a las redes de datos.

Durante la primera mitad de la década de los 60, organismos industriales, militares y académicos buscaron el desarrollo de la conmutación de paquetes, siendo el primer estudio atribuido a Rand Corporation en 1964 a petición de la Fuerza Aérea de Estados Unidos. Pero muchos esfuerzos no tuvieron trascendencia, hasta la vinculación de la Agencia de Proyectos de Investigación Avanzada (Estados Unidos), más conocida como ARPA, y del Laboratorio Nacional de Física (Reino Unido). El trabajo de Rand Corporation ayudó a pasar de una red jerárquica a una red distribuida. Desde entonces, Internet se basó en la conmutación de paquetes, como Ethernet en el estándar principal para las LAN.

Actualmente Ethernet cumple con la norma IEEE 802.3. Token Ring, definido en la norma 802.5, es uno de los estándares para redes conmutadas que competía para dominar parte del segmento de las LAN.

Token Ring llegó a ser muy popular pero las empresas que lo optaron luego se miraron a Ethernet. Fueron las redes distribuidas quienes más aportaron a la conmutación. Ethernet por su parte se desarrollo para soportar colisiones de paquetes durante la transmisión, se implementan técnicas como Acceso Múltiple mediante detección de portadoras con Detección de Errores* (En inglés conocida con la sigla CSMA/CD). Significando esto que las transmisiones de datos demoran más en llegar y el funcionamiento de la red no es el mejor. Durante los últimos años han ido tomando fuerza otros tipos de redes conmutadas que se relacionan con las WAN (Redes de Área Extensa) como son: ATM, Frame Relay y FDDI.

Podemos afirmar, que la conmutación a través de la historia ha sido fundamental para la evolución de las futuras redes.

2.2 Visión General

La introducción de la conmutación significa que se puede filtrar el tráfico de datos de forma más eficaz, y permite transmitir de uno a uno o de uno a varios, sin inundar la red con cargas innecesarias. Los hubs y routers se limitan a inyectar volúmenes de datos a través de la red y entre las redes. Para la conmutación, se utiliza el dispositivo que se denomina conmutador o bien conocido como switch. El switch se define como el dispositivo que envía y filtra el tráfico de datos

* Funcionamiento CSMA/CD. http://www.guajara.com/wiki/es/wikipedia/c/cs/csma_cd.html

entre segmentos de una red, generalmente en las LAN (Red de Área Local). Por lo general, estos switch operan en la capa 2: enlace de datos del modelo OSI. Recordemos que el modelo OSI consta de siete capas que proporcionan una descripción esencial de configuración y funcionamiento de las redes. Aunque existen dispositivos conocidos como switch de capa 3 y switch de capa 4, que operan en la capa de red y capa de transporte del modelo OSI, respectivamente.

En los últimos meses se han notado aumentos en las funcionalidades de las redes, se podría hacer referencia al avance en el funcionamiento de los switches para que puedan operar en las capas superiores del modelo OSI. En la capa 4 del modelo OSI: capa de transporte, se pueden implementar switch o conmutadores, logrando:

- Identificar el tráfico de aplicaciones críticas.
- Dar prioridad a este tráfico en una red.
- Identificar el tráfico de Web para responder rápido.
- Maximizar el uso y disponibilidad de los servidores.

Los switches distinguen los diferentes tipos de datos que transitan por la red basándose en la clasificación de prioridades. Son muchos los diseños heredados de routers que están llegando al límite de su valor funcional, siendo los switches de capa 3 y 4 quienes presentan mayor versatilidad, adicionándole a esto, las organizaciones buscan incrementar la presencia de los estos switches de nueva generación y evitar incluir dentro de su presupuesto la implementación de routers, por sus altos costos. Se nota el aumento de la implementación de las redes conmutadas. Para la actual época de las comunicaciones optar por una red conmutada conduce al éxito dentro de la era digital.

NOTA: En el CD que acompaña esta monografía encontrarás mayor información en la carpeta: Otros apoyos → Conmutación

Archivos: Guía de Switching 3COM.pdf

2.3 Conmutación Simétrica y Asimétrica*

La conmutación puede se de carácter Simétrica o Asimétrica. La conmutación simétrica se caracteriza por la asignación de un ancho de banda a cada puerto. Todos los puertos tienen el mismo ancho de banda. Mientras que la conmutación Asimétrica asigna un ancho de banda diferente a cada puerto dependiendo de sus necesidades en cada momento determinado.

2.4 Tipos de conmutación

Remontándonos en la historia de las redes públicas de telefonía conmutada, conocidas por su sigla en inglés PSTN – Public Switched Telephone Network**. Estas hacen referencia a la diversidad de redes y servicios telefónicos existentes a nivel mundial.

NOTA: En el CD que acompaña esta monografía encontrarás mayor información en la carpeta: Otros apoyos → Conmutación

Archivos: La Tecnología de Conmutación.htm

* Cisco – Conmutación LAN. http://www.eduangi.com/documentos/2_CCNA2.pdf.
Material Online de Cisco. Semestre 3 – Capítulo 2. http://cisco.netacad.net

** Tecnología de la Conmutación PSTN. http://portalgsm.com/documentación_extendida/83_0_17_0_C/

2.4.1 Conmutación de circuitos

Esta técnica puede ser espacial o temporal, consiste en el establecimiento de un circuito físico previo al envío de información, permaneciendo abierto durante todo el tiempo que dura la transmisión. Se puede resumir en tres etapas, la primera es la etapa de conexión, la segunda etapa es establecer el circ uito entre la fuente y el destino de transmisión y la tercera etapa de desconexión. Es orientada a la comunicación por voz. Anteriormente, hablamos de la PSTN que es el mejor ejemplo de este tipo de conmutación. También, podemos mencionar la Red de Telefonía Conmutada (RTC) y la Red Digital de Servicios Integrados (RDSI)

Con la conmutación de circuitos en las redes de telecomunicaciones surgió un problema: existían programas que deseaban conectarse y ejecutar acciones de un computador al mismo tiempo, pero esto no era posible o no era óptimo aplicándolo. Adicional a esto, el flujo de la información no es de tipo continuo, es discreto. Citando un ejemplo, se puede decir que una persona puede llegar a escribir hasta 2 caracteres por segundo, y esto para una red de telecomunicaciones es muy lento, considerando que normalmente se transmiten hasta 1,600 caracteres por segundo. Esto comenzó a causar problemas, por lo que pensaron en hacer más eficiente este esquema, así que se pensó en otra tipo de conmutación: conmutación de mensajes.

Cuadro 2. Ventajas y desventajas de la Conmutación de circuitos[*]

Conmutación de Circuitos	
VENTAJAS	DESVENTAJAS
La calidad de la conexión no depende del número de comunicaciones que haya en la red	Uso ineficiente de recursos: se mantienen ocupados durante los silencios
El retardo y su variación son mínimos: buena calidad en la conversación.	Existe la posibilidad de que todos los recursos (líneas) estén ocupados y no se pueda establecer la conexión (probabilidad de bloqueo).

2.4.2 Conmutación de mensajes

Es un método basado en el tratamiento de bloques de información, dotados de una dirección de origen y otra de destino. Cada mensaje es conmutado a un circuito. El mensaje va a llegar al conmutador, y el conmutador va a asignar el mensaje a su computador correspondiente; así podemos tener varios mensajes, pero surge un interrogante ¿Cómo reconoce el conmutador qué mensaje corresponde a cada computador? Recordemos que con un identificador en el encabezado del mensaje[*].

Las consecuencias de este tipo de conmutación es el decremento en el desempeño. El encabezado es información adicional, si este fuese muy gran tamaño con respecto a la información, el servicio va a ser mas lento. Se deberá asegurar un desempeño óptimo para lo cual será necesario que el encabezado sea lo más pequeño posible. Además, llevará más tiempo al conmutador analizar y procesar cada encabezado que se encuentre; por eso los conmutadores de mensajes deben de ser muy buenos. Sin embargo, existe una conmutación mejor que la conmutación de mensajes: conmutación de paquetes.

[*] Fundamentos de Telefonía. http://www.freepgs.com/vgozalbes/documents/manuales/f_telf.pdf
[*] Planificación y evaluación de redes: http://iio.ens.uabc.mx/~jmilanez/escolar/redes/01090000.html

2.4.3 Conmutación de paquetes

Es similar a la conmutación de mensajes, sólo que emplea mensajes más cortos y de longitud fija, llamada paquetes, lo que permite el envío de los mismos sin necesidad de recibir el mensaje completo puesto que previamente se ha fraccionado, por lo que resulta más rápida. Cada uno de estos paquetes contiene información suficiente sobre la dirección, tanto de la fuente como la del destino, así como para el control del mismo en caso de que suceda alguna anomalía en la red. Es orientada a la transmisión de datos. Para citar un actual ejemplo de red que haga uso de este tipo de conmutación: Internet, que hace uso del protocolo IP, aunque también podemos mencionar las redes ATM, X.25 y Frame Relay.

La conmutación de paquetes permite que los datos se transmitan paquete a paquete a través de la infraestructura de la red, de manera que cada paquete puede tomar un camino diferente a través de la red. Como no existe un circuito predefinido, la conmutación de paquetes puede aumentar o disminuir el ancho de banda según el caso, manipulando de esta forma las congestiones de paquetes de forma adecuada. Esta conmutación es capaz de enrutar los paquetes, evitando las líneas caídas o congestionadas, debido a los múltiples caminos en la red.

Según el modo de funcionamiento la conmutación de paquetes puede ser:

- Modo Datagrama: Cada paquete es tratado como una entidad por separado sin previa ruta, cada paquete puede seguir diferentes rutas hacia el destino y la entrega no es garantizada en forma ordenada, es una técnica de mejor esfuerzo, porque el tratamiento del error es responsabilidad del usuario no de la red. No existen circuitos virtuales, ni establecimiento ni liberación de llamadas. Además, es el modo más empleado para la transmisión de datos.

- Modo Circuito Virtual: Se requiere fijar una ruta previa, usan encabezamientos cortos, dado que sólo requiere la identificación del circuito virtual, en vez de la dirección completa del destino (parece un circuito dedicado, aunque es compartido). No ocupan recursos, permite capacidad de transmisión, mientras no se envía información. Tenemos los siguientes tipos de circuitos virtuales: SVC, que los establece y libera el usuario, no el operador y los PVC, que los establece y libera el operador, no el usuario.

Existen servicios de datagramas, en los cuales cada paquete se encamina a través de la red como si fuera una entidad independiente, el camino físico entre los extremos de la conexión puede variar a menudo debido a que los paquetes aprovechan aquellas rutas de menor costo, y evitan las zonas congestionadas.

Algunos protocolos de conmutación de paquetes existentes son*:

X.25.: Protocolo normalizado, revisado y probado, ideal para cargas ligeras de tráfico, aunque no son adecuadas para la mayoría del tráfico entre LAN´s por ser lentas y requerir una gran porción de ancho de banda para el tratamiento de errores.

Frame Relay: Servicio más rápido y eficiente que asume el hecho de que la red este libre de errores, lo que ahorra costosos reconocimientos de errores durante su funcionamiento, como en el caso de X.25.

* Planificación y evaluación de redes:
http://iio.ens.uabc.mx/~jmilanez/escolar/redes/01090000.html.

SMDS: Servicio Conmutado de Datos Multimegabit (Switched Multimegabit Data Service), consiste en un servicio basado en celdas, proporcionado por las compañías regionales de operaciones Bell en algunas zonas escogidas. (RBOC's - Regional Bell Operational Corp.) SMDS utiliza la conmutación ATM y ofrece servicios tales como facturación basada en la utilización y gestión de red.

Conmutación de Celdas: Conocidas como Modo de Transferencia Asíncrona (ATM - Asyncronous Transfer Mode), ofrece servicios de conmutación de paquetes rápidos que pueden transmitir a mega o a gigabits por segundo.

2.4.4 Un pequeño paralelo entre conmutación por circuitos y conmutación por paquetes

Cuadro 3. Paralelo entre conmutación de circuitos y conmutación de paquetes

Cuadro Comparativo		
Características	CONMUTACIÓN DE CIRCUITOS	CONMUTACIÓN DE PAQUETE
Ruta dedicado de "cobre"	Si	No
Ancho de banda disponible	Fijo	Dinámico
Posibilidad de desaprovechar ancho de banda	Si	No

NOTA: En el CD que acompaña esta monografía encontrarás mayor información en la carpeta:

Otros apoyos → Conmutación

Archivos: Comunicación de Datos.pdf

2.5 Métodos de conmutación

Los métodos de conmutación son:

- Almacenamiento y reenvío
- Por método de corte

2.5.1 Almacenamiento y reenvío

Consiste en recibir toda la trama y luego reenviarla. También, es conocido como el método de almacenar y transmitir, porque emplea la técnica de almacenar y transmitir (store-and-forward), el conmutador recibe el paquete completo, la almacena en su memoria interna, y lo examina por entero antes de decidir si ha de ser transmitido o filtrado. El inconveniente teórico es que precisan de una memoria para almacenar los paquetes, así como de procesadores y software más potente para evitar la latencia, lo que supone un coste y complejidad de diseño mayores. Pero, indiscutiblemente, sus prestaciones son mejores al eliminar paquetes erróneos de la red e incluso permitir filtros más sofisticados al poder analizarse el paquete completo. Además el argumento de que una latencia menor es mejor, no es válido si tenemos en cuenta que muchos de los protocolos de transporte modernos, como TCP, NFS e IPX en modo ráfaga, permiten el envío de secuencias de múltiples paquetes consecutivos antes de recibir el reconocimiento de que el primero ha sido recibido adecuadamente; y por lo tanto, no se produce ningún latencia en el envío del siguiente paquete, por no haber llegado la señal de reconocimiento del primero, puesto que el segundo y sucesivos ya han sido remitidos.

2.5.2 Por método de corte

- Conmutación de reenvío rápido: Nivel más bajo de latencia. Se reenvía justo después de leer la dirección de destino

- Conmutación sin fragmentos: Se filtran los fragmentos de colisión. Cualquier fragmento que exceda de 64bytes será recibido sin errores. Este modo de latencia se calcula como FIFO (Cola)

Denominado esta maneta por que Corta y Continúa. Dado que la dirección destino está en la primera parte del paquete, el reenvío del mismo puede iniciarse antes incluso de que el paquete entero haya sido recibido por el conmutador, y en ello se basa el método "cortar-continuar" (cut-through). Es decir, el paquete es examinado, tan pronto como se ha podido "cortar" la parte donde esta la dirección destino, al mismo tiempo que se continúa recibiendo el resto del paquete; en el momento en que se ha podido decidir si ha de ser reenviado o filtrado, se puede iniciar su transmisión, aunque no haya sido recibido en su totalidad. La ventaja de este procedimiento es su baja latencia, pero tiene por contra, el inconveniente de que, al no ser examinado el paquete en su totalidad antes de su reexpedición, se pueden propagar errores existentes en el mismo, e incluso fragmentos de paquetes con colisiones, lo que implicará un "consumo" innecesario del ancho de banda del segmento receptor, y por tanto una reducción en las prestaciones del conmutador. Por otro lado, cuando se transmiten paquetes entre redes de diferentes velocidades, no es posible utilizar este método. Citamos el siguiente ejemplo, al enviar un paquete recibido a 100 Mbps., a una red de 10 Mbps., la red receptora no sería capaz de "recoger" a la suficiente velocidad el paquete y se generaría un error, y viceversa. Hay que resaltar que esta misma situación, sin necesidad de que exista diferencia de velocidades, se produce cuando la red destinataria esta congestionada o colapsada[*].

[*] Tecnología y conmutación de redes: http://www.consulintel.es/Html/Tutoriales/Articulos/tecn_conm.html

2.6 Ventajas de la conmutación

La conmutación permite que muchos usuarios se comuniquen en paralelo a través de los circuitos virtuales del switch. Esto permite maximizar el ancho de banda de la red. Incrementa las prestaciones de la red, proporcionando conexiones de alta velocidad entre diferentes segmentos y nodos de la red, sin límite a pesar del incremento en el número de usuarios. Reduce las colisiones, especialmente al existir la posibilidad de dedicar un segmento a cada nodo de la red. Baja los costos, dado que no se requiere modificar el hardware y cableado de todos los nodos de la red. Mejora en la seguridad de la red, al transferir los paquetes sólo a sus direcciones destino y al poder establecer filtros más específicos. Reduce los tiempos de respuesta de la red, totalmente predecibles, lo que permite incluso aplicaciones multimedia en redes que inicialmente no estaban preparadas para ello.

2.7 Switches Capa 2, Capa 3 y Capa 4

Los switches sólo podían funcionar en la capa 2 del modelo OSI: enlace de datos, mientras que en la capa 3 de este mismo modelo: capa de red se utilizaban routers, pero ahora vemos como los switches pueden trabajar en la capa de red y hasta en la capa de transporte. Todo este proceso es conocido como conmutación multicapas, asociado a las siglas MLS, que pretende:

- Mejorar las arquitecturas de red existentes.
- Mayor facilidad de rápido crecimiento para poder ampliar su capacidad de red.
- Escalabilidad en la cantidad de paquetes transmitidos.
- La conmutación y el enrutamiento de alta velocidad llega a todos lo puertos, y por consiguiente a todos las interfaces y protocolos de red.

La actual evolución de los esquemas de conmutación ha inducido a que las tecnologías de conmutación y enrutamiento se integren en un solo dispositivo, llegando a la posibilidad de incrementar el rendimiento, disminuir la latencia y obtener mayor escalabilidad en el ancho de banda. El dispositivo conocido como switch era asociado solo con la capa 2 del modelo OSI: enlace de datos. Hoy en día, también se asocia a las capas 3 y 4 del modelo OSI: red y transporte, respectivamente[*].

La conmutación con visión multicapa brinda la posibilidad de obtener dispositivos con mejor capacidad de decisión. Lo anterior, coincide con la necesidad de segmentar la LAN, a fin de conseguir el mejoramiento de la disponibilidad del ancho de banda y evitar los problemas de congestión en la red.

NOTA: En el CD que acompaña esta monografía encontrarás mayor información en la carpeta: Otros apoyos.

Archivos: Acerca de switches capa 2, capa 3 y capa 4.htm

Prácticas de laboratorios y taller sobre switches.doc

En resumen…

Una conmutación no requiere conexiones permanentes entre dos puntos fijos. En su lugar, permite a los usuarios establecer conexiones temporales entre múltiples puntos cuya duración corresponde a

[*] ¿Switching VS. Routing? http://neutron.ing.ucv.ve/revista-e/No4/articulo.htm

la de la transmisión de datos. Existen dos tipos de conmutación, que son muy usados. La conmutación de circuitos, utilizada en las llamadas telefónicas; y la conmutación de paquetes, que se adapta mejor a la transmisión de datos. Sin duda, se puede afirmar que el incremento en el uso de switches, cada vez más sofisticados y modulares en todo tipo de redes, e incluso en un futuro no muy lejano, la desaparición total de hubs y routers, tanto locales como remotos, puesto que los conmutadores pueden cumplir perfectamente todas sus funciones.

CAPÍTULO III

ENRUTAMIENTO

3.1 Conceptos básicos de Enrutamiento*

3.1.1 Determinación de la Ruta

La determinación de Ruta se presenta en la Capa de red, la cual se concentra en el objetivo principal del Router, pues este se encarga de escoger la mejor opción entre una gama de rutas disponibles.

La determinación de Ruta se presenta en la Capa de red, la cual se concentra en el objetivo principal del Router, pues este se encarga de escoger la mejor opción entre una gama de rutas disponibles.

En capa 3, se rutean los paquetes de la fuente al destino final a través de Routers intermedios, conociendo de antemano la topología de la subred, evitando asi la congestión y manejando los casos donde la fuente y el destino estén en redes distintas.

3.1.2 Tablas de Ruteo y Métricas

El Router es responsable de crear y mantener tablas de ruteo para cada capa de protocolo de red, estas tablas son creadas ya sea estáticamente o dinámicamente.

* MONTOYA, Alcides. Enrutamiento. http://www.eafit.edu.co/cursos/

De esta manera el Router extrae de la capa de red la dirección destino y realiza una decisión de envío basado sobre el contenido de la especificación del protocolo en la tabla de ruteo.

La inteligencia de un Router permite seleccionar la mejor ruta, basándose sobre diversas métricas, más que por la dirección MAC destino.

Estos factores incluyen:

- Ancho de banda: capacidad de transmisión de datos de un enlace.
- Retardo: cantidad de tiempo requerido para transportar un paquete por cada enlace desde el origen hacia el destino.
- Carga: cantidad de actividad en un recurso de red tal como un Router o un enlace.
- Confiabilidad: generalmente se refiere al índice de error de cada enlace de red.
- Número de saltos: cantidad de Routers que un paquete debe atravesar antes de llegar a su destino.
- Costo: valor arbitrario, generalmente basado en el ancho de banda, el gasto monetario u otras mediciones, asignado por un administrador de red.

La desventaja es que el proceso adicional de procesado de frames por un Router puede incrementar el tiempo de espera o reducir el desempeño del Router cuando se compara con una simple arquitectura de Switch.

3.1.3 Funciones Básicas de los Routers

- Segmentar la red dentro de dominios individuales de broadcast.

- Suministrar un envío inteligente de paquetes.
- Soportar rutas redundantes en la red.
- Aislar el tráfico de la red ayuda a diagnosticar problemas, puesto que cada puerto del Router es una subred separada, el tráfico de los broadcast no pasa a través del Router.
- Proporcionar seguridad a través de sofisticados filtros de paquetes, en ambiente LAN y WAN.
- Permitir diseñar redes jerárquicas, que deleguen autoridad y puedan forzar el manejo local de regiones separadas de redes internas.
- Integrar diferentes tecnologías de enlace de datos, tales como Ethernet, Fast Ethernet, Token Ring, FDDI y ATM.

3.1.4 Rutas Estáticas y Dinámicas*

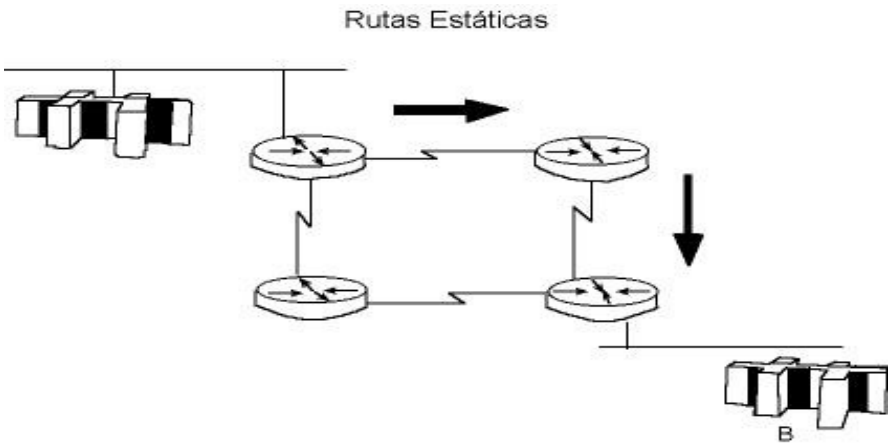
Las rutas estáticas son gestionadas manualmente por el administrador de red, siempre que un cambio se presente en la topología de internetwork.

Tienen las siguientes características:

- Rutas Estáticas
- Permiten la configuración manual de las tablas de enrutamiento.
- Las tablas no podrán ser modificadas en forma dinámica
- Falta de flexibilidad frente a fallas de los enlaces
- No son necesarios las cargas y procesos asociados a un protocolo de descubrimiento de rutas.
- Es fácil establecer barreras de seguridad bajo este modelo.

* Enrutamiento. http://www.wl0.org/~sjmudd/wireless/network-structure/html/x284.html

Figura 1. Rutas estáticas



Las rutas dinámicas se actualizan automáticamente a través de un proceso de enrutamiento cuando se recibe información de la red, estos cambios son informados a los demás Routers como parte del proceso de actualización.

El éxito del enrutamiento dinámico depende de dos funciones básicas del Router:

- El mantenimiento de una tabla de enrutamiento.
- La distribución oportuna del conocimiento, bajo la forma de actualizaciones de enrutamiento, hacia otros Routers.

El enrutamiento dinámico se basa en un protocolo de enrutamiento para compartir el conocimiento entre los Routers. Un protocolo de enrutamiento define el conjunto de reglas utilizadas por un Router cuando se comunica con los Routers vecinos. Por ejemplo, un protocolo de enrutamiento describe:

- Cómo enviar actualizaciones.

- Qué conocimiento contienen esas actualizaciones.
- Cuándo enviar ese conocimiento.
- Cómo ubicar a los destinatarios de las actualizaciones.

El enrutamiento dinámico revela todo acerca de la red, mientras que el enrutamiento estático posee mas flexibilidad en cuanto a seguridad se refiere, ya que cuando se quiera acceder a una red a través de un solo camino, una sola ruta hacia la red puede ser suficiente, evitándose así el gasto que implica el enrutamiento dinámico.

Algunas de las ventajas del enrutamiento estático con respecto al dinámico son:

- El enrutamiento estático posee varias aplicaciones útiles. Mientras que el enrutamiento dinámico tiende a revelar todo lo que se conoce acerca de la internetwork, es posible que por razones de seguridad se desee ocultar parte de una internetwork.
- El enrutamiento estático le permite especificar la información que desea revelar acerca de redes restringidas.
- Una ruta estática puede ser suficiente cuando se puede acceder a una red a través de un solo camino. Este tipo de red se denomina red de conexión única. La configuración del enrutamiento estático para una red de conexión única (stub) evita el gasto que implica el enrutamiento dinámico.

NOTA: En el CD que acompaña esta monografía encontrarás mayor información en la carpeta: Otros apoyos → Enrutamiento

Archivos: enrutamiento-parte1-marzo2004.pdf

3.1.5 Algoritmos de Enrutamiento*

El algoritmo de enrutamiento decide en qué línea de salida se debiera transmitir un paquete que llega. Propiedades deseables:

- Correctitud y sencillez.
- Robustez. Una red puede tener que operar por años y experimentará fallas de software y hardware.
- El algoritmo de enrutamiento no debe requerir que se reinicializa la red después de fallas parciales.
- Estabilidad. Debiera tener un equilibrio.
- Justicia y optimalidad. Están frecuentemente contradictorias. Se necesita una balanza entre la eficiencia global y la justicia al individual. ¿Qué podemos optimizar? El retraso por paquete o la utilización global de la red son posibilidades. Estos también están contradictorios, porque con 100% utilización los retrasos aumentan. Una solución intermedia es minimizar el número de saltos.
- Los algoritmos pueden ser adaptativos o no. Los primeros cambian sus decisiones de enrutamiento para reflejar la topología y el tráfico en la red. Los últimos son estáticos.

El principio de optimalidad. Si el RouterJ está en el camino óptimo desde Router I a Router K, entonces la ruta óptima desde J a K está en la misma ruta. El conjunto de rutas óptimas forma el árbol de hundir (sink tree). El fin de los algoritmos de enrutamiento es descubrir y usar los árboles de hundir de todos los Routers. Un problema es que la topología cambia.

* El nivel de red: Generalidades. http://www.uv.es/~montanan/redes/redes_02.rtf

Camino más corto. Se calculan los caminos más cortos usando alguna métrica. Posibilidades: el número de saltos, la distancia física, el retraso de transmisión por un paquete de prueba, el ancho de banda, el tráfico promedio, el costo de comunicación, etc.

Inundación. Se manda cada paquete que llega sobre todas las otras líneas. Puede generar un número infinito de paquetes, así que se necesita un método para restringir la inundación.

Se puede usar un contador de saltos en cada paquete que se decrementa después de cada salto. Cuando el contador es cero se descarta el paquete.

Se pueden guardar números de secuencia agregados por cada Router a los paquetes. Los Routers mantienen listas de los números de secuencia más altos vistos y descartan los paquetes que son duplicados. En la inundación selectiva se mandan los paquetes solamente sobre las líneas que salen más o menos en la dirección correcta.

3.2 Clases de enrutamientos

3.2.1 Enrutamiento Vector distancia

En esta clase de enrutamiento, cada Router mantiene una tabla o vector que almacena las mejores distancias y rutas conocidas a cada destino, actualizándose con el intercambio de información con los Routers vecinos.

Todo Router almacena en su tabla una entrada para cada uno de los Routers en la subred. Las entradas almacenan la línea preferida de salida, de acuerdo a la métrica utilizada.

Cada Router tiene que medir las distancias a sus vecinos, intercambiando sus tablas T mseg, estas tablas vecinas son utilizadas para que el Router calcule una nueva tabla en base a estas.

Este enrutamiento por vector de distancia sufre el problema que incorpora buenas noticias rápidamente pero malas noticias muy lentamente. Las actualizaciones no validas seguirán andando en círculos hasta que algún proceso detenga el recorrido, este problema se conoce como Conteo al Infinito, produciéndose así que el numero de saltos se incremente cada vez cuando un paquete atraviesa otro Router, recorriendo así la red en un bluque debido a la información incorrecta de las tablas de enrutamiento.

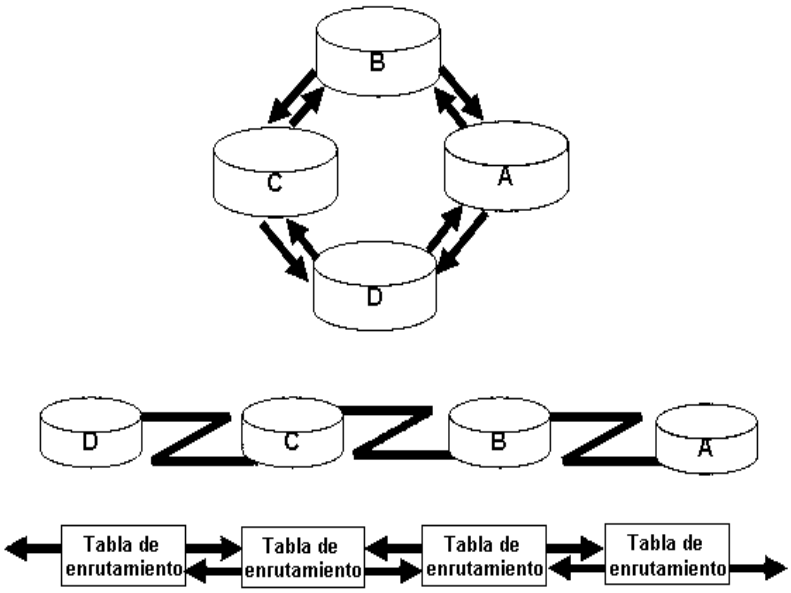
Este problema de conteo al infinito se puede evitar mediante temporizadores de espera que funcionan de la siguiente manera:

- Cuando un Router recibe una actualización por parte de un vecino que indica que una red previamente accesible ahora se encuentra inaccesible, el Router marca la ruta como inaccesible e inicia un temporizador de espera. Si en algún momento, antes de que expire el temporizador de espera, se recibe una actualización por parte del mismo vecino indicando que la red se encuentra nuevamente accesible, el Router marca la red como accesible y elimina el temporizador de espera.
- Si llega una actualización desde un Router vecino distinto con una métrica más conveniente que la originalmente registrada para la red, el Router marca la red como accesible y elimina el temporizador de espera.
- Si en algún momento antes de que expire el temporizador de espera se recibe una actualización de un Router vecino diferente con una métrica inferior, se ignorará la actualización. El ignorar

una actualización con una métrica inferior mientras el temporizador de espera se encuentra activado, permite ganar más tiempo para que el conocimiento de un cambio perjudicial se propague a través de toda la red.

Un ejemplo del vector distancia es el siguiente:

Figura 2. Vector distancia



Se tiene una topología como la que nos indica la Figura 2, donde el Router B recibe información del Router A. El Router B agrega un número de vector-distancia basado en la métrica que se utilice como puede ser el número de saltos, de esta manera aumenta el vector-distancia y luego transfiere esta nueva tabla de enrutamiento a su otro vecino, el Router C. Este mismo proceso paso a paso se produce en todas las direcciones entre los Routers directamente vecinos.

3.2.2 Enrutamiento por estado de enlace

En este cada Router tiene que:

- Descubrir sus vecinos y sus direcciones.
- Medir el retraso o costo a cada vecino.
- Construir un paquete con la información que ha averiguado.
- Mandar este paquete a todo los Routers.
- Calcular la ruta mínima a cada Router.

DESCUBRIR LOS VECINOS. Cuando se bootea un Router, manda paquetes especiales de saludos sobre cada línea punto-a-punto estos constituyen las publicaciones estado de enlace (LSA). Los vecinos contestan con sus direcciones únicas. Si más de dos Routers están conectados por la LAN, se modela la LAN como un nodo artificial.

MEDIR EL COSTO. El Router manda paquetes de eco a lo cual los recipientes tienen que contestar inmediatamente. Se divide el tiempo por el viaje de ida y vuelta para determinar el retraso.

Un punto interesante es si debiera incluir en el retraso la carga de la línea, si incluimos la carga, se usan las líneas menos cargadas, que mejora el rendimiento; pero es posible tener oscilaciones grandes en el uso de las líneas.

CONSTRUIR EL PAQUETE. El paquete consiste en la identidad del emisor, un número de secuencia, la edad, y la lista de vecinos y retrasos. Se pueden construir los paquetes periódicamente o solamente después de eventos especiales.

DISTRIBUIR LOS PAQUETES DE ESTADO DE ENLACE. Esto es la parte más difícil del algoritmo, porque las rutas en los Routers no cambian juntas. La idea fundamental es usar la inundación.

Para restringir la inundación se usan los números de secuencia que se incrementan cada vez se reenvía un paquete.

Los Routers mantienen pares del Router fuente y el número de secuencia que han visto, y descartan los paquetes viejos. Los paquetes nuevos se reenvían sobre todas las líneas salvo la de llegada.

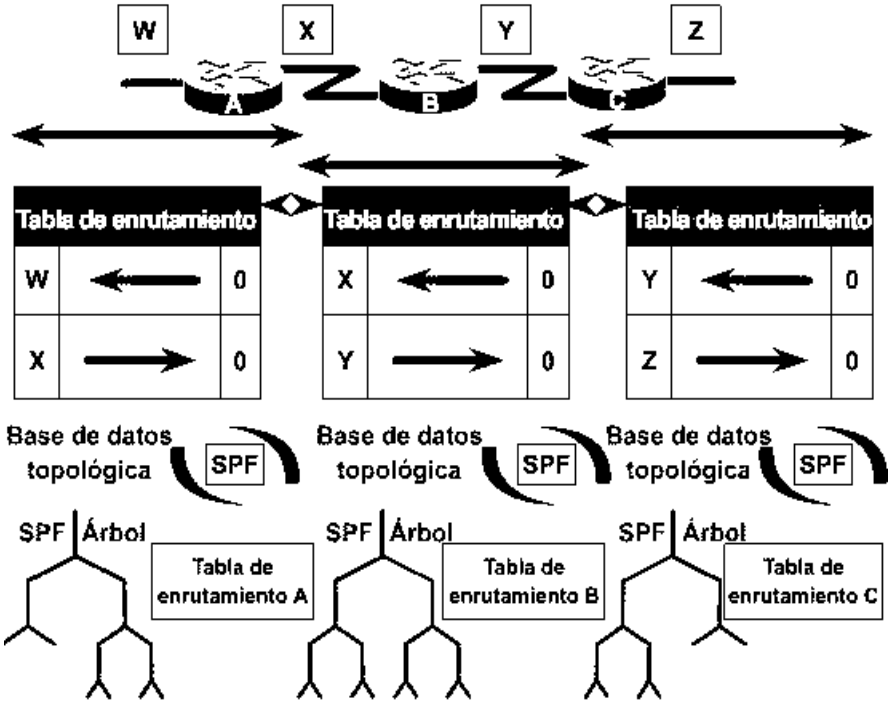
Para evitar que el número de secuencia se desborde, se usan 32 bits.

- Para evitar que los paquetes puedan vivir por siempre, contienen un campo de edad que se decrementa.
- Si un Router cae o un número de secuencia se convierte malo, se perderán paquetes. Por lo tanto se incluye un campo de edad en cada entrada en la lista.
- Se decrementa este campo cada segundo y se descarta la información que tiene una edad de cero.

CALCULAR LAS RUTAS. Se usa el algoritmo de Dijkstra. Un problema es que, debido a errores en los Routers, puede haber problemas en las rutas.

En la Figura 3 se ilustra un ejemplo descriptivo del intercambio de tablas de enrutamiento:

Figura 3. Intercambio de tablas de enrutamiento



Este intercambio requiere del siguiente proceso:

- Los Routers intercambian LSA entre sí. Cada Router empieza con redes directamente conectadas para las cuales posee información directa.
- Cada Router en paralelo con los demás Routers genera una base de datos topológica que contiene todas las LSA de la internetwork.
- El algoritmo SPF calcula la accesibilidad de la red. El Router construye esta topología lógica como un árbol, con él mismo como raíz, y con todas las rutas posibles hacia cada red dentro de la internetwork que usa el protocolo estado-enlace. Entonces clasifica estas rutas, colocando la ruta más corta primero.

- El Router hace una lista de sus mejores rutas y de los puertos que permiten acceder a estas redes destino, dentro de la tabla de enrutamiento.

3.2.3 Comparación del enrutamiento por vector de distancia y de estado de enlace*

Cuadro 4. Comparación del enrutamiento por vector distancia y por estado de enlace

Vector Distancia	Estado-Enlace
Visualiza la topología de red desde el punto de vista del vecino.	Obtiene una visión común de toda la topología de red.
Agrega vectores de distancia de Router a Router.	Calcula la ruta mas corta hacia los otros Routers.
Actualizaciones frecuentes, periódicas: convergencia lenta.	Actualizaciones activadas por eventos: Convergencia más rápida.
Envía copias de las tablas de enrutamiento hacia los Routers vecinos	Envía actualizaciones de enrutamiento de estado de enlace hacia los otros Routers

NOTA: En el CD que acompaña esta monografía encontrarás mayor información en la carpeta: Otros apoyos → Enrutamiento

Archivos: Enrutamiento-parte2-marzo2004.pdf

* Comparación entre los protocolos de enrutamiento por vector-distancia y de estado-enlace. Semestre 2 CCNA, capitulo 11.5.1

3.3 Protocolos enrutados y de enrutamiento

3.3.1 Diferencia protocolo enrutados y de enrutamiento

Existe una marcada diferencia entre protocolo enrutado y protocolo de enrutamiento. Los protocolos enrutados son los que se desplazan a través de una red. Tales como el Protocolo de control de transmisión/Protocolo Internet (TCP/IP) y el Intercambio de paquetes de internetworking (IPX). Los protocolos de enrutamiento enrutan los protocolos enrutados a través de una red, tales como:

- IGRP.
- Primero la ruta libre más corta (OSPF).
- Protocolo de gateway exterior (EGP).
- Protocolo de gateway fronterizo (BGP).
- Enrutamiento OSI.
- Red avanzada de par a par (APPN).
- Sistema intermedio-Sistema intermedio (IS-IS).
- RIP.

Los Routers soportan múltiples protocolos de enrutamiento independientes, tales como IGRP y RIP. Esta capacidad le permite al Router entregar paquetes desde varios protocolos enrutados, como TCP/IP e IPX, a través de los mismos enlaces de datos.

3.3.2 Clases de protocolos de enrutamiento

Los protocolos de enrutamiento se dividen ampliamente en dos clases:

Protocolos de Enrutamiento Interiores: Se utilizan para enrutar información dentro de las redes que están bajo una administración de red común. Todos los protocolos IP interiores se deben especificar con una lista de redes relacionadas antes de que se puedan iniciar las actividades de enrutamiento. Un proceso de enrutamiento escucha las actualizaciones de otros Routers en estas redes y envía un broadcast de su propia información de enrutamiento en esas mismas redes. Dentro de estos tenemos:

- RIP (Routing Informanon Protocol)
- IGRP (Interior Gateway Routing Protocol)
- EIGRP (Enhanced IGRP)
- OSPF (Open Shortest Path First)

Protocolos de Enrutamiento Exteriores: Se utilizan para intercambiar información de enrutamiento entre redes que no comparten una administración común. Los protocolos de enrutamiento exterior requieren antes del enrutamiento una lista de los Routers vecinos con los que intercambiarán información de enrutamiento, así como también una lista de las redes para publicarlas como directamente alcanzables. Dentro de estos tenemos:

- Is-Is
- EGP
- BGP
- IDRP

3.3.3 Características básicas de los diferentes protocolos de enrutamiento

Routing Information Protocol RIP

- Protocolo IGP más utilizado (distribuido gratis).
- Vector distancia clásico.
- Propósito general no sólo para IP.
- Transporte sobre UDP/IP.
- Mensajes de petición de información y mensajes de información.

Open Shortest Path First OSPF

- Protocolo IGP.
- Estado de enlaces.
- Más robusto y complejo (autentificación, enrutamiento en base a TOS, reparto de carga).
- Métrica adimensional.
- Transporte sobre IP.

Exterior Gateway Protocol EGP

- Protocolo EGP (cómo no).
- Mecanismos principales.
- Adquisición de vecinos administrativos.
- Comprobación de continuidad.
- Intercambio de información de alcanzabilidad (lista de redes con distancia).

Border Gateway Protocol BGP

- Protocolo EGP.

- Vector de distancia modificado (no indica métrica, sino camino exacto a seguir).
- Transporte sobre TCP/IP.
- Última revisión en 1994, BGP4.
- trabaja con redes de diferentes sistemas autónomos.
- Muy bueno para interconectar distintos grupos wireless.

IGRP

- Protocolo de gateway interior por vector distancia.
- Combinación de métricas (retardo, ancho de banda, confiabilidad y carga de red).
- Utiliza esperas, split horizons (horizontes divididos) y actualizaciones inversas.
- Hay que crear el proceso de enrutamiento IGRP.

NOTA: En el CD que acompaña esta monografía encontrarás mayor información en la carpeta: Otros apoyos → Enrutamiento

Archivos: Capa 3 Protocolos.pdf

enrutamiento-parte3-marzo2004.pdf

enrutamiento-parte4-rip-marzo2004.pdf

enrutamiento-parte5-ospf-bgp-marzo2004.pdf

enrutamiento-parte6-igrp-marzo2004.pdf

3.4 ACL*

Las ACL son listas de instrucciones que se aplican a una interfaz del Router. Estas listas indican al Router qué tipos de paquetes se deben aceptar y qué tipos de paquetes se deben denegar. La aceptación y rechazo se pueden basar en ciertas especificaciones, como dirección origen, dirección destino y número de puerto. Las ACL le permiten administrar el tráfico y examinar paquetes específicos, aplicando la ACL a una interfaz del Router. Cualquier tráfico que pasa por la interfaz debe cumplir ciertas condiciones que forman parte de la ACL.

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 ACL se pueden configurar en el Router para controlar el acceso a una red o subred. Por ejemplo, en el Distrito Escolar Washington, las ACL se pueden usar para evitar que el tráfico de los estudiantes pueda entrar a la red administrativa.

Las ACL filtran el tráfico de red controlando si los paquetes enrutados se envían o se bloquean en las interfaces del Router. El Router examina cada paquete para determinar si se debe enviar o descartar, según las condiciones especificadas en la ACL. Entre las condiciones de las ACL se pueden incluir la dirección origen o destino del tráfico, el protocolo de capa superior, u otra información.

Las ACL se deben definir por protocolo. En otras palabras, es necesario definir una ACL para cada protocolo habilitado en una interfaz si desea controlar el flujo de tráfico para esa interfaz. (Observe

* ACL. Semestre 3 de CCNA, capitulo 6.1.1, 6.2.2, 6.3 y 6.4

que algunos protocolos se refieren a las ACL como filtros.) Por ejemplo, si su interfaz de Router estuviera configurada para IP, AppleTalk e IPX, sería necesario definir por lo menos tres ACL. Las ACL se pueden utilizar como herramientas para el control de redes, agregando la flexibilidad necesaria para filtrar los paquetes que fluyen hacia adentro y hacia afuera de las interfaces del Router.

Hay muchas razones para crear ACL. Por ejemplo, las ACL se pueden usar para:

- Limitar el tráfico de red y mejorar el rendimiento de la red.
- Brindar control de flujo de tráfico.
- Proporcionar un nivel básico de seguridad para el acceso a la red.

Una ACL es un grupo de sentencias que define cómo los paquetes:

- Entran a las interfaces de entrada
- Se reenvían a través del Router
- Salen de las interfaces de salida del Router

El principio del proceso de comunicaciones es el mismo, ya sea que las ACL se usen o no. Cuando un paquete entra en una interfaz, el Router verifica si un paquete es enrutable o puenteable. Ahora, el Router verifica si la interfaz de entrada tiene una ACL. Si existe, ahora se verifica si el paquete cumple o no las condiciones de la lista. Si el paquete es permitido, entonces se compara con las entradas de la tabla de enrutamiento para determinar la interfaz destino.

Las sentencias de la ACL operan en orden secuencial lógico. Si se cumple una condición, el paquete se permite o deniega, y el resto de las sentencias de la ACL no se verifican. Si las sentencias de la ACL no se verifican, se impone una sentencia implícita de "denegar cualquiera". Esto significa que, aunque la sentencia "denegar cualquiera" no se vea explícitamente en la última línea de una ACL, está allí.

3.4.1 Wildcard

Una máscara wildcard es una cantidad de 32 bits que se divide en cuatro octetos, en la que cada octeto contiene 8 bits. Un bit de máscara wildcard de 0 significa "verificar el valor de bit correspondiente" y un bit 1 de una máscara wildcard significa "no verificar (ignorar) el valor de bit correspondiente".

Una máscara wildcard se compara con una dirección IP. Los números uno y cero se usan para identificar cómo tratar los bits de la dirección IP correspondientes. Las ACL usan máscaras wildcard para identificar una sola o múltiples direcciones para las pruebas de aprobar o rechazar. El término máscara wildcard es la denominación aplicada al proceso de comparación de bits de máscara y proviene de una analogía con el "wildcard" (comodín) que equivale a cualquier otro naipe en un juego de póquer.

Aunque ambas son cantidades de 32 bits, las máscaras wildcard y las máscaras de subred IP operan de manera diferente. Recuerde que los ceros y unos en una máscara de subred determinan las porciones de red, subred y host de la dirección IP correspondientes. Los ceros y unos en un

wildcard, como se ha observado, determinan si los bits correspondientes en la dirección IP se deben verificar o ignorar para los fines de la ACL.

Como hemos visto, los bits de ceros y unos en una máscara wildcard de ACL hacen que la ACL verifique o ignore el bit correspondiente en la dirección IP. Ver Anexo 9 Wildcards.

3.4.2 ACL estándar.

Se deben usar las ACL estándar 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 verifican la dirección origen de los paquetes que se deben enrutar. El resultado permite o deniega el resultado para todo un conjunto de protocolos, según las direcciones de red, subred y host. Por ejemplo, se verifican los paquetes que vienen de E0 para establecer la dirección origen y protocolo. Si se permiten, los paquetes salen a través de S0, que se agrupa en la ACL. Si no se permite, se descarta.

3.4.3 ACL extendidas.

Las ACL extendidas se usan con mayor frecuencia para verificar condiciones porque ofrecen una mayor cantidad de opciones de control que las ACL estándar. Se puede usar una ACL extendida cuando se desea permitir el tráfico de la Web pero denegar el Protocolo de transferencia de archivos (FTP) o telnet desde las redes que no pertenecen a la empresa. Las ACL extendidas verifican las direcciones origen y destino de los paquetes. También pueden verificar protocolos, números de

puerto y otros parámetros específicos. Esto ofrece mayor flexibilidad para describir las verificaciones que debe realizar la ACL. Se pueden permitir o denegar paquetes según su origen o destino.

Para una sola ACL, se pueden definir múltiples sentencias. Cada una de estas sentencias debe hacer referencia al mismo nombre o número identificatorio, para relacionar las sentencias a la misma ACL. Se puede establecer cualquier cantidad de sentencias de condición, con la única limitación de la memoria disponible. Por cierto, cuanta más sentencia se establezcan, mayor será la dificultad para comprender y administrar la ACL. Por lo tanto, la documentación de las ACL evita la confusión.

Las ACL estándar filtran el tráfico según una dirección y máscara origen. Las ACL estándar también pueden permitir o denegar todo el conjunto de protocolos Internet (IP). Puede ser necesario encontrar una forma más precisa de control del tráfico y el acceso.

Para un control más preciso de filtrado de tráfico se usan las ACL extendidas. Las sentencias de las ACL extendidas verifican la dirección origen y destino. Además, al final de la sentencia de la ACL extendida, se obtiene precisión adicional con un campo que especifica el número de puerto de protocolo opcional TCP o del Protocolo de datagrama del usuario (UDP). Estos pueden ser números de puerto conocidos para TCP/IP.

3.5 Firewalls

Un Firewall es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y la WAN. El firewall determina cual de los servicios de red pueden ser

accesados dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo tráfico de información a través de la WAN deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

Los firewalls administran los accesos posibles de la WAN a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se exponen al ataque de otros servidores. Esto significa que la seguridad en la red privada depende de la "Dureza" con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

El firewall permite al administrador de la red definir un "choke point" (envudo), manteniendo al margen los usuarios no-autorizados (tal, como., hackers, crakers, vándalos, y espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Uno de los beneficios clave de un firewall es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran nuestra red privada.

El firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa, este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el transito de los datos. Esto se podrá notar al acceder la organización al Internet, la

pregunta general es "si" pero "cuando" ocurrirá el ataque. Esto es extremadamente importante para que el administrador audite y lleve una bitácora del tráfico significativo a través del firewall. También, si el administrador de la red toma el tiempo para responder una alarma y examina regularmente los registros de base. Esto es innecesario para el firewall, desde que el administrador de red desconoce si ha sido exitosamente atacado.

3.6 Filtrar por paquetes

Este Router toma las decisiones de rehusar/permitir el paso de cada uno de los paquetes que son recibidos. El Router examina cada datagrama para determinar si este corresponde a uno de sus paquetes filtrados y que a su vez haya sido aprobado por sus reglas. Las reglas de filtrado se basan en revisar la información que poseen los paquetes en su encabezado, lo que hace posible su desplazamiento en un proceso de IP. Esta información consiste en la dirección IP fuente, la dirección IP destino, el protocolo de encapsulado (TCP, UDP,ICMP, o IP tunnel), el puerto fuente TCP/UDP, el puerto destino TCP/UDP, el tipo de mensaje ICMP, la interface de entrada del paquete, y la interface de salida del paquete. Si se encuentra la correspondencia y las reglas permiten el paso del paquete, este será desplazado de acuerdo a la información a la tabla de ruteo, si se encuentra la correspondencia y las reglas niegan el paso, el paquete es descartado. Si estos no corresponden a las reglas, un parámetro configurable por incumplimiento determina descartar o desplazar el paquete.

Servicio dependiente del filtrado: Las reglas acerca del filtrado de paquetes a través de un Router para rehusar/permitir el trafico esta basado en un servicio en especifico, desde entonces muchos servicios vierten su información en numerosos puertos TCP/UDP conocidos.

Por ejemplo, un servidor Telnet esta a la espera para conexiones remotas en el puerto 23 TCP y un servidor SMTP espera las conexiones de entrada en el puerto 25 TCP. Para bloquear todas las entradas de conexión Telnet, el Router simplemente descarta todos los paquetes que contengan el valor del puerto destino TCP igual a 23. Para restringir las conexiones Telnet a un limitado numero de servidores internos, el Router podrá rehusar el paso a todos aquellos paquetes que contengan el puerto destino TCP igual a 23 y que no contengan la dirección destino IP de uno de los servidores permitidos.

Algunas características típicas de filtrado que un administrador de redes podría solicitar en un Router filtra-paquetes para perfeccionar su funcionamiento serian:

- Permitir la entrada de sesiones Telnet únicamente a una lista especifica de servidores internos.
- Permitir la entrada de sesiones FTP únicamente a los servidores internos especificados.
- Permitir todas las salidas para sesiones Telnet.
- Permitir todas las salidas para sesiones FTP.
- Rehusar todo el trafico UDP.

La mayoría de sistemas firewall son desplegados usando únicamente Routers filtra-paquetes. Otros que tienen tiempo planean los filtros y configuran el Router, sea este pequeño o no, el costoso para implementar la filtración de paquetes no es cara; desde que los componentes básicos de los Routers

incluyen revisiones estándar de software para dicho efecto. Desde entonces el acceso a Internet es generalmente provisto a través de interfaces WAN, optimando la operación del Router moderando el tráfico y definiendo menos filtros. Finalmente, el Router de filtrado es por lo general transparente a los usuarios finales y a las aplicaciones por lo que no se requiere de entrenamiento especializado o software especifico que tenga que ser instalado en cada uno de los servidores.

CAPÍTULO IV

TECNOLOGÍAS WAN

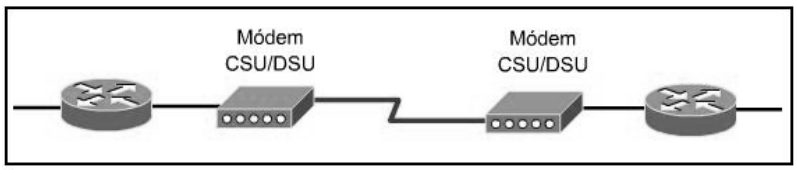
4.1 Introducción a las WAN

4.1.1 Topología de Redes WAN

Cuando se usa una subred punto a punto, una consideración de diseño importante es la topología de interconexión del Router. Las redes WAN típicamente tienen topologías irregulares.

Una posibilidad para una WAN es un sistema de satélite o de radio en tierra. Cada Router tiene una antena por medio de la cual puede enviar y recibir, algunas veces los Routers están conectados a una subred punto a punto de gran tamaño, y únicamente algunos de ellos tienen una antena de satélite. Por su naturaleza las redes de satélite son de difusión y son más útiles cuando la propiedad de difusión es importante.

Figura 4. Ejemplo de una WAN



En la Figura 4 se muestra una WAN típica junto con el equipo requerido para las conexiones. Un Router envía el tráfico desde la red local, a través de la conexión de área extensa, hacia el destino remoto. El Router puede estar conectado tanto a una línea analógica como a una línea digital.

En este tipo de conexión, los Routers se conectan a las líneas analógicas a través de módem o a líneas digitales a través de Unidades de Servicio de Canal/Unidades de Servicio de Datos (CSU/DSUs: Channel Service Unit/Data Service Units). El tipo de servicio de transmisión determina la clase de equipo que el área extensa necesita para su funcionamiento.

4.1.2 Líneas Dedicadas y Líneas Conmutadas

Las redes WAN pueden incluir tanto líneas dedicadas como líneas conmutadas. Una línea dedicada es una conexión permanente entre dos puntos que normalmente se alquila por meses.

Un servicio de línea conmutada no requiere conexiones permanentes entre dos puntos fijos. En su lugar, permite a los usuarios establecer conexiones temporales entre múltiples puntos cuya duración corresponde a la de la transmisión de datos. Existen dos tipos de servicios conmutados:

- Servicios de conmutación de circuitos: en este tipo de conexión se establece un canal dedicado, denominado circuito, entre dos puntos por el tiempo que dura la llamada. El circuito proporciona una cantidad fija de ancho de banda durante la llamada y los usuarios sólo pagan por esa cantidad de ancho de banda el tiempo que dura la llamada.

  Las conexiones de conmutación de circuitos tienen dos serios inconvenientes. El primero es que debido a que el ancho de banda en estas conexiones es fijo, no manejan adecuadamente las avalanchas de tráfico, requiriendo frecuentes retransmisiones. El segundo inconveniente es que estos circuitos virtuales sólo tienen una ruta, sin caminos alternativos definidos.
- Servicios de conmutación de paquetes: en este tipo de conexión se suprime el concepto de circuito virtual fijo. Los datos se transmiten paquete a paquete a través del entramado de la red

o nube, de manera que cada paquete puede tomar un camino diferente a través de la red. Como no existe un circuito virtual predefinido, la conmutación de paquetes puede aumentar o disminuir el ancho de banda según sea necesario, pudiendo manejar adecuadamente las avalanchas de paquetes de forma adecuada. Los servicios de conmutación de paquetes son capaces de enrutar los paquetes, evitando las líneas caídas o congestionadas, debido a los múltiples caminos en la red.

4.1.3 Redes Públicas

Las redes públicas son los recursos de telecomunicación de área extensa pertenecientes a las operadoras y ofrecidos a los usuarios a través de suscripción. Estas operadoras incluyen a:

- Compañías de servicios de comunicación local.
- Compañías de servicios de comunicación a larga distancia. Una compañía de comunicación a larga distancia (IXC: Interexchange carriers) es un operador de telecomunicaciones que suministra servicios de larga distancia como AT&T, MCI y US SPRINT.
- Proveedores de servicios de valor añadido. Los proveedores de servicio de valor añadido (VACs: Value-added carriers, ofrecen con frecuencia, servicios de comunicación de área amplia como complemento a su verdadero negocio.

4.1.4 Redes Privadas

Una red privada es una red de comunicaciones privada construida, mantenida y controlada por la organización a la que sirve. Como mínimo una red privada requiere sus propios equipos de

conmutación y de comunicaciones. Puede también, emplear sus propios servicios de comunicación o alquilar los servicios de una red pública o de otras redes privadas que hayan construido sus propias líneas de comunicaciones.

Aunque una red privada es extremadamente cara, en compañías donde la seguridad es imperante así como también lo es el control sobre el tráfico de datos, las líneas privadas constituyen la única garantía de un alto nivel de servicio. Además, en situaciones donde el tráfico de datos entre dos puntos remotos excede de seis horas al día, emplear una red privada puede ser más rentable que utilizar la red pública.

4.1.5 Líneas Analógicas

Las líneas analógicas son las típicas líneas de voz desarrolladas inicialmente para llevar tráfico de voz. Este tipo de líneas son parte del servicio telefónico tradicional, por lo que se encuentran en cualquier lugar. Aunque el tráfico de datos digitales no es compatible con las señales de portadora analógica, se puede transmitir tráfico digital sobre líneas analógicas utilizando un módem, el cual modula las señales digitales sobre servicios de portadora analógica. La máxima tasa de transferencia de tráfico digital posible sobre líneas analógicas está en 43,000 bps.

4.1.6 Líneas Digitales

Las líneas digitales están diseñadas para transportar tráfico de datos, que es digital por naturaleza. En vez de utilizar un módem para cargar datos sobre una señal portadora digital, utilizará un canal

de servicio digital/unidad de servicio de datos (CSU/DSU), el cual únicamente proporciona una interfaz a la línea digital. Las líneas digitales pueden transmitir tráfico de datos a velocidades de hasta 45 Mbps y están disponibles tanto para servicios dedicados como conmutados.

4.2 Estándares WAN*

Los protocolos de capa física WAN describen cómo proporcionar conexiones eléctricas, mecánicas, operacionales, y funcionales para los servicios de una red de área amplia. Estos servicios se obtienen en la mayoría de los casos de proveedores de servicio WAN.

Los protocolos de enlace de datos WAN describen cómo los marcos se llevan entre los sistemas en un único enlace de datos. Incluyen los protocolos diseñados para operar sobre recursos punto a punto dedicados, recursos multipunto basados en recursos dedicados, y los servicios conmutados multiacceso tales como Frame Relay.

Los estándares WAN son definidos y manejados por un número de autoridades reconocidas incluyendo las siguientes agencias:

- Internacional Telecommunication Union Telecommunication Standardization Sector (ITU-T)
- Intemational Organization for Standardization (ISO).
- Intemet Engineering Task Force (IETF).
- Electronic Industries Association (ETA).

* Estándares WAN. http://www.eduangi.com/documentos/16_CCNA.pdf

Los estándares WAN describen típicamente tanto los requisitos de la capa física como de la capa de enlace de datos.

4.3 Capa Física: WAN

La capa física WAN describe la interfaz entre el equipo terminal de datos (DTE) y el equipo de conexión de los datos (DCE). Típicamente, el DCE es el proveedor de servicio, y el DTE es el dispositivo asociado. En este modelo, los servicios ofrecidos al DTE se hacen disponibles a través de un módem o unidad de servicio del canal/unidad de servicios de datos (CSU/DSU).

Algunos estándares de la capa física que especifican esta interfaz son:

- EIA/TIA-232D: Esta norma fue definida como una interfaz estándar para conectar un DTE a un DCE.
- EIA/TIA-449: Junto a la 422 y 423 forman la norma para transmisión en serie que extienden las distancias y velocidades de transmisión más allá de la norma 232.
- V.35: Según su definición original, serviría para conectar un DTE a un DCE síncrono de banda ancha (analógico) que operara en el intervalo de 48 a 168 kbps.
- X.21: Estándar CCITT para redes de conmutación de circuitos. Conecta un DTE al DCE de una red de datos pública.
- G.703: Recomendaciones del ITU-T, antiguamente CCITT, relativas a los aspectos generales de una interfaz.
- EIA-530: Presenta el mismo conjunto de señales que la EIA-232D.

- High-Speed Serial Interface (HSSI): Estándar de red para las conexiones seriales de alta velocidad (hasta 52 Mbps) sobre conexiones WAN.

4.4 Capa de Enlace de Datos: Protocolos WAN*

Las tramas más comunes en la capa de enlace de datos, asociadas con las líneas seriales sincrónicas se enumeran a continuación:

- Synchronous Data Link Control (SDLC): Es un protocolo orientado a dígitos desarrollado por IBM. SDLC define un ambiente WAN multipunto que permite que varias estaciones se conecten a un recurso dedicado. SDLC define una estación primaria y una o más estaciones secundarias. La comunicación siempre es entre la estación primaria y una de sus estaciones secundarias. Las estaciones secundarias no pueden comunicarse entre sí directamente.
- High-Level Data Link Control (HDLC): Es un estándar ISO. HDLC no pudo ser compatible entre diversos vendedores. HDLC soporta tantas configuraciones punto a punto como multipunto.
- Link Access Procedure Balanced (LAPB): Utilizado sobre todo con X.25, puede también ser utilizado como transporte simple de enlace de datos. LAPB incluye capacidades para la detección de pérdida de secuencia o extravío de marcos así como también para intercambio, retrasmisión, y reconocimiento de marcos.
- Frame Relay: Utiliza los recursos digitales de alta calidad donde sea innecesario verificar los errores LAPB. Al utilizar un marco simplificado sin mecanismos de corrección de errores, Frame Relay puede enviar la información de la capa 2 muy rápidamente, comparado con otros protocolos WAN.

* Protocolos de enrutamiento. http://www.eduangi.com/documentos/16_CCNA.pdf

- Point-to-Point Protocol (PPP): Descrito por el RFC 1661, dos estándares desarrollados por el IETF. El PPP contiene un campo de protocolo para identificar el protocolo de la capa de red.
- X.25: Define la conexión entre una terminal y una red de conmutación de paquetes.
- Integrated Services Digital Network (ISDN): Un conjunto de servicios digitales que transmite voz y datos sobre las líneas de teléfono existentes.

4.5 Frame Relay

Frame Relay es un producto de la Red Digital de Servicios Integrados (ISDN: Integrated Services Digital Networks). Constituye la parte correspondiente de servicio de datos de conmutación de paquetes de ISDN diferenciada y ofrecida como un servicio separado. A pesar de su relativa baja velocidad, la arquitectura mejorada de conmutación de paquetes de frame relay puede interesar al administrador de red que busca incrementar la velocidad de una conexión de datos de área extensa.

Frame Relay, es un producto de conmutación de paquetes que conecta dos redes de área local a través de una red pública de conmutación de paquetes. De una manera simple, una trama procedente de una LAN se encapsula en una trama frame relay, y se transmite por la red frame relay hasta la LAN destino.

Frame relay, divide los datos del usuario en paquetes que son transmitidos sobre la red y ensamblados en el destino. Los datos se dividen en tramas de longitud variable que contienen las direcciones de destino, luego son remitidas a la red frame relay para su transferencia. Aunque su modo de trabajo es casi idéntico al de conmutación de paquetes, la diferencia se centra en el nivel

en que trabajan, para ser más claros: la conmutación de paquetes opera en el nivel 3 del modelo de referencia OSI, mientras que frame relay opera en el nivel 2. Esto significa que frame relay es un protocolo más simple que X.25 y otros protocolos de conmutación de paquetes, realizando menos comprobación y corrección de errores, pero ofreciendo mayor velocidad.

El paquete frame relay esta conformado por los siguientes campos:

- Delimitador de comienzo de trama.
- Campo de nivel de enlace (cabecera frame relay).
- Identificador de conexión de enlace de datos.
- Apropiada para descartar.
- Campo de datos de usuario.
- Secuencia de verificación de trama.

Soporta distintos tipos de conexiones que cooperan conjuntamente para formar el entramado de la red frame relay:

- Puertos de conexión. Un puerto de conexión es un punto físico de acceso a la red frame relay que define la máxima cantidad de datos que puede ser enviada a la red en cualquier momento a través de todos los PVCs. El puerto de conexión es la interfaz a la red frame relay pública o privada, y va desde 56 Kbps hasta 1,536 Kbps. El puerto de conexión asigna los datos dinámicamente entre los circuitos virtuales permanentes.
- Circuitos virtuales permanentes. Un circuito virtual permanente (PVC: Permanent Virtual Circuit) es un camino a través de la red frame relay que conecta dos puntos. Un PVC constituye un ancho de banda dedicado que garantiza un nivel de servicio, denominado velocidad de

información comprometida (CIR: Commited Information Rate), a una estación determinada. El administrador de red solicita los PVCs al suministrador del servicio frame relay, el cual los configura de acuerdo a las especificaciones del administrador de red. Los circuitos virtuales permanentes están activos y disponibles para la red suscriptora en todo momento.

- Circuitos virtuales conmutados. Los circuitos virtuales conmutados (SVC: Switched Virtual Circuits) son circuitos establecidos ad hoc según la necesidad de la estación emisora, incrementando la flexibilidad del ancho de banda del circuito. Aunque forma parte del estándar, no todos los proveedores lo ofrecen.

Como se ha mencionado, la naturaleza de gran parte del tráfico en las redes frame relay es en ráfagas, lo que significa que la mayoría del tiempo los dispositivos transmiten pocos datos o ningún dato. Por esto, frame relay facilita a los administradores de red la posibilidad de conectar varias conexiones de este tipo al mismo segmento.

El rendimiento que ofrece frame relay es muy bueno, ya que generalmente se encuentra disponible a velocidades entre 56 Kbps hasta 1.544 Mbps. Admite además, ráfagas de transmisión de hasta 45 Mbps, y tiene una baja latencia (alrededor de 20 mts). Lo mejor de frame relay es su escalabilidad, presenta una gran facilidad para añadir más ancho de banda mediante la velocidad de información comprometida (CIR: Committed Information Rate) conjuntamente con la posibilidad de enviar picos de tráfico superiores al CIR.

4.6 RDSI: Red Digital de Servicios Integrados (ISDN)

ISDN es considerado en la actualidad, como una forma rentable de proporcionar:

- Acceso remoto para usuarios que se conectan a las LANs de sus compañías.
- Un enlace apropiado para ciertas conexiones entre LAN.
- Tráfico de fax entre oficinas con gran ancho de banda.
- Acceso a Internet a alta velocidad.
- Las líneas ISDN se componen de varios tipos de canales:
- Canal B: Transporta la voz o los datos generados por el terminal del usuario (a una velocidad de 64 Kbps).
- Canal D: Transporta la señalización de llamada (a una velocidad de 16 ó 64 Kbps) y también puede utilizarse para transmitir datos por conmutación de paquetes.
- Canal H: Es un canal que permite la transferencia de información de usuario a velocidades superiores a 64 Kbps. No transportan información de señalización para control de llamadas ISDN. Existen cuatro tipos: Estos canales se pueden agrupar, desde el punto de vista de instalación del cliente, bien en la modalidad más sencilla o Acceso Básico (dos canales B y un canal D) o en forma de Acceso Primario (30 canales B y un canal D, en este caso de 64 Kbps).

Existen dos estándares de ofertas de servicios, denominados accesos:

- Acceso Básico (BRI). Proporciona 2 canales B de 64 Kbps y un canal D de 16 Kbps para señalización de los canales B. Con los equipos apropiados se pueden unir los dos canales B juntos para conseguir un ancho de banda máximo de 128 Kbps. El BRI es apropiado para ser utilizado en oficinas pequeñas, redes LAN pequeñas o de tamaño medio, o para teletrabajadores que deseen conectarse a la LAN de su compañía.
- Acceso Primario (PRI). Proporciona 30 canales B de 64 Kbps y un canal D de 64 Kbps para señalización. Los canales B pueden ser fundidos en una de las configuraciones denominadas,

servicios H, descritas anteriormente. Esas líneas pueden utilizarse como troncales de alta velocidad para transferencia de archivos de gran tamaño y de otros flujos continuos de datos o se pueden dividir con un multiplexor para proporcionar canales para múltiples dispositivos.

Además de los ya mencionados, existen otra serie de ventajas, aplicaciones, como son:

1. Ventajas

- Excepcional rapidez en los tiempos de establecimiento y de liberación de la llamada, inferiores a 0,5 segundos.
- Gran fiabilidad y alta calidad de voz al ser todo el camino digital.
- Alta velocidad de transmisión y baja tasa de errores.
- Flexibilidad en el uso de las líneas ISDN, que no está limitado por la naturaleza de la información ni por la fuente generadora.
- Simplicidad y seguridad al tener un acceso único.

CAPÍTULO V

LABORATORIOS*

5.1 LABORATORIO No. 1

REPASO DE LA CONFIGURACIÓN DE LABORATORIO DEL ROUTER

Objetivos:

- Analizar las diferentes conexiones físicas de una configuración de red existente.
- Diferenciar los tipos de cableado para las diversas conexiones en la configuración de determinada topología de red.

Información Básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio pretende examinar y documentar las conexiones físicas entre Routers y otros dispositivos de laboratorio, tales como, Hubs, Switches y computadores.

Metodología:

Desarrollar esta practica en conjunto con la siguiente, ya que esta le proporcionara un esquema de direccionamiento IP.

* CNNA. Material Online. http://cisco.netacad.net.
AMATO, Vito, Cisco Systems, Inc. ACADEMIA DE NETWORKING DE CISCO SYSTEMS: GUÍA DEL PRIMER AÑO. Segunda edición. Pearson. 1024 páginas

Conformar grupos de trabajo de 3 a 5 personas, un grupo realizará la configuración física del router y otro grupo diseñará el esquema de direccionamiento Clase B.

Recursos:

- 5 Computadores (mínimo), con Sistema Operativo Windows e HyperTerminal Instalados.
- 5 Routers Cisco (modelo de la serie 2600 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 el computador con el puerto de consola (con convertidores de RJ-45 a DB9).
- 3 conjuntos de cables seriales de WAN V.35 (DTE macho/ DCE hembra) para conectarse de router a router.
- Cables Ethernet CAT5 o CAT6 de conexión directa para conectar los Routers y computadores a los Hubs y Switches.

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.2 LABORATORIO No. 2

REPASO DE LAS SUBREDES DEL ROUTER

Objetivos:

- Desarrollar un esquema de direccionamiento Clase B con subredes.
- Manejar con exactitud los comandos del IOS para la configuración de los Routers.
- Manejar las utilidades como el Winipcfg.exe, para tener información mas detallada de los parámetros de la red como dirección IP, mascara de subred y Gateway.
- Utilizar el comando ping para verificar la correcta configuración de la red tanto LAN como WAN.

Información básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio para desarrollar un esquema de direccionamiento teniendo en cuenta una dirección de red de clase B, la cual se va a dividir posteriormente en subredes. Para esto usted debe ser capaz de configurar los Routers y los computadores, utilizando el material de ayuda proporcionado por el IOS. En la práctica anterior se realizaron las diferentes conexiones físicas ahora usted debe ser capaz de direccionarla de acuerdo a la topología de red utilizada en esta.

Metodología:

Conformar grupos de trabajo de 3 a 5 personas, un grupo realizará la configuración física del router y otro grupo diseñará el esquema de direccionamiento Clase B y asignara la dirección IP a los diferentes dispositivos.

Recursos:

- 5 Computadores (mínimo), con Sistema Operativo Windows e HyperTerminal Instalados.
- 5 Routers Cisco (modelo de la serie 2600 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 el computador con el puerto de consola (con convertidores de RJ-45 a DB9).
- 3 conjuntos de cables seriales de WAN V.35 (DTE macho/ DCE hembra) para conectarse de router a router.
- Cables Ethernet CAT5 o CAT6 de conexión directa para conectar los Routers y computadores a los Hubs y Switches.

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.3 LABORATORIO No. 3

ACTUALIZACIÓN DEL IOS/TFTP

Objetivos:

- Conocer el software Cisco IOS y la memoria del Router.

- Recuperar la Flash de una imagen IOS mediante un servidor TFTP, a través de la imagen existente en un Router.
- Actualizar el IOS de un Router a través de un servidor TFTP.

Información Básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio para determinar cuales son los requisitos para actualizar la versión del IOS de determinado Router, así como también determinar la cantidad de memoria flash que tiene disponible y cuanto espacio de esta ocupa el IOS. Es importante realizar una copia de la imagen del IOS actual, antes de renovarla.

Metodología:

Usted tiene la opción de trabajar en forma individual o en equipo.

Recursos:

- Un computador, con Sistema Operativo Windows e HyperTerminal Instalados.
- Un Router Cisco modelo de la serie 2600.
- Cable Roll over, conectado al puerto de consola del Router y al computador.
- Cable Cross over, conectado al Router y al computador; o en su defecto un Hub conectado al computador y al Router.
- Un servidor TFTP instalado en el computador

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.4 LABORATORIO No. 4

ACTUALIZACIÓN DE LA MEMORIA DEL ROUTER, ACTUALIZACIÓN DEL SIMM DE DRAM Y ACTUALIZACIÓN DE LA SIMM DE LA FLASH DE CÓDIGO DE SISTEMA

Objetivos:

- Tener un conocimiento básico sobre la actualización de la memoria DRAM y Flash del Router.

Información Básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio que será útil para determinar la versión y el IOS del Router, y así conocer los requisitos necesarios para su actualización, para esto necesitamos verificar cuanta memoria Flash hay disponible y cuanta utiliza el IOS, como también verificar la cantidad de DRAM.

Metodología:

Usted tiene la opción de trabajar en forma individual o en equipo.

Recursos:

- Un computador, con Sistema Operativo Windows e Hyper Terminal Instalados.
- Un Router Cisco modelo de la serie 2600.
- Cable rollover, conectado al puerto de consola del Router y al computador.
- Cable crossover, conectado al Router y al computador; o en su defecto un Hub conectado al computador y al Router.
- Un servidor TFTP instalado en el computador.
- Destornillador de hoja plana de tamaño mediano (1/4 de pulgada).
- Correa para muñeca para evitar ESD (descargas electrostáticas).
- El SIMM de DRAM requerido para la actualización planificada.
- Los SIMM de código de sistema.

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.5 LABORATORIO No. 5

CARACTERÍSTICAS, CONSOLA DE ADMINISTRACIÓN Y OPCIONES DE PUERTO DEL SWITCH

Objetivos:

- Analizar e identificar en un modelo de switch Ethernet sus interfaces físicas, los cables, conexiones y dispositivos que se pueden conectar a este switch logrando la descripción de su funcionamiento dentro de una red.
- Realizar la conexión del switch a través de su puerto de consola con un computador que tenga instalado HyperTerminal para la exploración y configuración de la consola de administración y revisión de firmware.
- Configurar y verificar los valores de red de los computadores para comprobar la compatibilidad con los valores de los switches y routers.
- Utilizar el menú de configuración del sistema para la configuración de la operación libre de fragmentos
- Habilitar la operación Full Duplex y Puerto rápido utilizando el menú de configuración de puerto.

Información Básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio para examinar y configurar un switch Ethernet: Características físicas y funciones de los switches en una red. Practicaremos varias configuraciones del switch Ethernet y menús de Interfaz del usuario a través de la consola de administración. También, podremos establecer la dirección IP del switch. También, veremos la configuración de un switch que opere en el modo de conmutación libre de fragmentos, habilitaremos un puerto para permitir una operación Full Duplex y Puerto rápido.

Metodología:

Afianzamiento de los conceptos del capítulo 2 del semestre 3 de la Academia Cisco Networking.

Visibilidad del switch por todos sus lados para inspeccionar las conexiones físicas.

Conformar 2 grupos de trabajo para realizar este laboratorio.

Disponibilidad de un computador con HyperTerminal para realizar la conexión al puerto de consola del switch y una conexión Ethernet para hacer Telnet al switch.

Recursos:

- 1 Computador, con Sistema operativo Windows e HyperTerminal debidamente instalado.
- 1 Switch Cisco (modelo 19xx o 28xx) con manuales.
- Cable de consola (Roll over).
- Cable Ethernet CAT5 o CAT6 del computador a un puerto Ethernet de switch.

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.6 LABORATORIO No. 6

NAVEGADOR DE CONFIGURACIÓN DEL SWITCH

Objetivos:

- Configurar la dirección IP del switch utilizando el menú de la Consola de administración.

- Identificar los valores de red de los computadores verificando la compatibilidad con valores de los switches y routers.
- Examinar el cableado y la conectividad IP desde el computador al switch utilizando los comandos Ping y Telnet.
- Utilizar un computador que tenga instalando algún software navegador para conectarse con el switch y verificar el estado del puerto.

Información básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio para acceder al switch a través del navegador del computador (Netscape o Internet Explorer) y realizar las verificaciones de la configuración del switch y las estadísticas de puerto. Actualmente, existen switches con software de servidor Web HTTP incorporado para soportar la administración de switch basada en navegador.
Con la tecnología de agrupación de switches de Cisco, puede manejar hasta 16 switches con una sola dirección IP. Es muy importante asignar una contraseña al switch si va a asignar una dirección IP.

Metodología:

Afianzamiento de los conceptos del capítulo 2 del semestre 3 de la Academia Cisco Networking.
Visibilidad del switch por todos sus lados para inspeccionar las conexiones físicas.
Conformar 2 grupos de trabajo para realizar este laboratorio.

Disponibilidad de un computador con HyperTerminal para realizar la conexión al puerto de consola del switch y una conexión Ethernet para hacer Telnet al switch.

Recursos:

- 1 Computador, con Sistema operativo Windows e HyperTerminal debidamente instalado.
- 1 Switch Cisco (modelo 19xx o 28xx) con manuales.
- Cable de consola (Roll over).
- Cable Ethernet CAT5 o CAT6 del computador a un puerto Ethernet de switch.

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.7 LABORATORIO No. 7

CREACIÓN DE VLAN

Objetivos:

- Conocer las diferentes opciones del Switch relacionadas con las VLAN.
- Crear VLAN, nombrarlas y configurar cada uno de sus puertos.
- Probar la funcionalidad de las VLAN intercambiando los diferentes Computadores.

Información Básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio donde se va a trabajar con redes de área local virtuales (VLAN), las cuales agrupan a los usuarios bajo cierto perfil, para realizarlo basta con asignarle determinados puertos de un switch a un grupo determinado, disminuyendo el broadcast.

Metodología:

Conformar grupos de trabajo de 3 a 5 personas, un grupo realizará la configuración del switch y otro grupo realizara una investigación sobre switches en el sitio Web de Cisco.

Recursos:

- Dos computadores con sistema operativo Windows e HyperTerminal.
- Switch Cisco.
- Cable de consola (roll-over) y adaptador DB-9/RJ45 o cable de módem nulo DB-9.
- Cable Ethernet CAT 6 desde cada computador a un puerto Ethernet del switch.

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.8 LABORATORIO No. 8

VLAN DE ADMINISTRACIÓN DE SWITCH

Objetivos:

- Administrar, verificar y cambiar la configuración de una red VLAN para el switch.
- Trabajar con el dominio de administración del switch.

Información Básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio se trabajará con las redes de área local virtuales (VLAN), visualizando las diferentes opciones de administración conectado desde el puerto de consola del switch.

Metodología:

Conformar grupos de trabajo de 3 a 5 personas, un grupo realizará la configuración del switch y otro grupo realizara una investigación sobre switches en el sitio Web de Cisco.

Recursos:

- Dos computadores con sistema operativo Windows e HyperTerminal.
- Switch Cisco.
- Cable de consola (Roll over) y adaptador DB-9/RJ45 o cable de módem nulo DB-9.
- Cable Ethernet CAT 6 desde cada computador a un puerto Ethernet del switch.

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.9 LABORATORIO No. 9

ACTUALIZACIÓN DEL FIRMWARE DEL SWITCH / TFTP

Objetivos:

- Mostrar información acerca del firmware actual del switch.
- Examinar las opciones de memoria y actualización del switch.
- Utilizar un servidor TFTP para actualizar un switch a una nueva versión del software firmwareObjetivo 1

Información Básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio se determinará cuál es la versión del firmware que el switch ejecuta en la actualidad y se familiarizará con los requisitos necesarios para realizar la actualización a una versión más reciente. En esta práctica de laboratorio se describe el método del servidor TFTP para actualizar el firmware.

Metodología:

Se deben conformar grupos de 3 o 5 personas, un equipo trabajara con el switch y el otro investigara sobre switches.

Recursos:

- Computador con sistema operativo Windows e HyperTerminal.
- Switch Cisco.
- Cable de consola (roll-over) y adaptador DB-9/RJ45 o cable de módem nulo DB-9.
- Cable Ethernet CAT 6 desde cada computador a un puerto Ethernet del switch.
- Servidor TFTP instalado en un computador.

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.10 LABORATORIO No. 10

VLAN MULTISWITCH

Objetivos:

- Usar la consola de administración para verificar las opciones del menú relacionadas con las VLAN.
- Crear una nueva VLAN, nombrarla y desplazar puertos miembro a ella.

- Probar la funcionalidad de las VLAN desplazando una estación de trabajo de una VLAN a otra.
- Habilitar el enlace troncal ISL (enlace interswitch) en puertos troncales para los dos switches.

Información Básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio trabajando con redes de área local virtuales de Ethernet (VLAN). Las VLAN se pueden usar para separar grupos de usuarios según la función en lugar de la ubicación física. Un administrador de red puede crear VLAN adicionales y trasladar algunos puertos a esas VLAN. Esto crea dominios de broadcast más pequeños que ayudan a reducir y localizar el tráfico de red. Las VLAN también se pueden crear usando puertos desde múltiples switches que se unen en un enlace troncal en un backbone. Para que dos VLAN se comuniquen deben estar conectadas a un Router.

Metodología:

Se deben conformar grupos de 3 o 5 personas, un equipo trabajara con el switch y el otro investigara sobre switches.

Recursos:

- Dos computadores con sistema operativo Windows e HyperTerminal.
- 2 Switch Cisco.
- Cable de consola (Roll over) y adaptador DB-9/RJ45 o cable de

módem nulo DB-9.

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.11 LABORATORIO No. 11

DISEÑO DE LAN CONMUTADA

Objetivos:

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

Información básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio para diseñar una pequeña red donde nos centraremos en la Topología física y en los componentes de la capa de 2 del modelo OSI: Enlace de datos. Debemos tener en cuenta las consideraciones necesarias para elección de los routers, switches, tipos de cables, entre otros elementos.

Metodología:

Afianzamiento de los conceptos del capítulo 4 del semestre 3 de la Academia Cisco Networking.

Conformar varios grupos de trabajo para realizar este laboratorio.

Recursos:

- Computadores con acceso a Internet para la investigación de productos Cisco y otras marcas donde se incluyan los Catálogos de distribuidores de equipos de comunicaciones de datos.
- 1900 / 2820 series Ethernet switches
- 2900 series Fast Ethernet switches
- 3500 series Gigabit Ethernet switches

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.12 LABORATORIO No. 12

PROTOCOLOS ENRUTADOS Y DE ENRUTAMIENTO

Objetivos:

- Comparar las características de los protocolos enrutados y de enrutamiento a través de ejemplos de cada uno de ellos explorando en la configuración de un router aquellos que se encuentren activos.
- Expresar la relación entre: enrutado y protocolos de enrutamiento dinámicos y protocolos estáticos, protocolos interiores y exteriores, vector distancia, estado de enlace y protocolos de enrutamiento híbridos.

Información básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio para una mejor compresión de los protocolos enrutados y de enrutamiento, los cuales son responsables del funcionamiento de un router. Exploraremos el IOS del router los protocolos enrutados y de enrutamiento observando cuales se encuentran activos o en ejecución, nos apoyaremos en la función del router.

Metodología:

Es fundamental comprender la diferencia entre protocolos enrutados y de enrutamiento para dominar los conceptos de internetworking, es básico repasar el Capítulo 5 del semestre 3 de la Academia Cisco Networking.

Disponibilidad de un computador con HyperTerminal para realizar la conexión al puerto de consola del router.

Recursos:

- 5 routers de Cisco, con hubs y switches debidamente configurados.
- Computadores para conectarse a los routers.
- Cable de consola (Roll over).
- Cable Ethernet CAT5 o CAT6 desde el computador al hub o switch

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.13 LABORATORIO No. 13

MIGRACIÓN DE RIP A IGRP

Objetivos:

- Verificar el buen funcionamiento de los protocolos de enrutamiento y la tabla de enrutamiento interpretando las entradas de red.
- Evaluar la configuración de las rutas estáticas.
- Comparar RIP con IGRP basándose en la distancia administrativa.
- Convertir una red de router basada en RIP en IGRP

Información básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio para implementar dos protocolos de enrutamiento interior dinámicos: Protocolo de información de enrutamiento (RIP) y Protocolo de enrutamiento de gateway interior (IGRP).

Metodología:

Nos conectaremos al router a través del puerto de consola para verificar el estado de la tabla de enrutamiento IP, así como también las redes que pueden ser alcanzadas por cada router. La habilidad para aplicar e interpretar los protocolos de enrutamiento es esencial para el mantenimiento de las internetworks.

Es fundamental manejar los conceptos de internetworking del Capítulo 5 del semestre 3 de la Academia Cisco Networking.

Disponibilidad de un computador con HyperTerminal para realizar la conexión al puerto de consola del router.

Recursos:

- 5 routers de Cisco, con hubs y switches debidamente configurados.
- Computadores para conectarse a los routers.
- Cable de consola (Roll over).
- Cable Ethernet CAT5 o CAT6 desde el computador al hub o switch

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.14 LABORATORIO No. 14

CONFIGURACIÓN DE IGRP

Objetivos:

- Configurar IGRP como el protocolo de enrutamiento de la red realizando los ajustes en las métricas configurables.

Información básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio para realizar las configuraciones en el protocolo de enrutamiento interior dinámico: Protocolo de enrutamiento de gateway interior (IGRP). Los routers pueden ejecutar múltiples protocolos de enrutamiento y enrutados, por lo visto en el laboratorio anterior a este.

Metodología:

Nos conectaremos al router a través del puerto de consola para eliminar de éste todos los protocolos dinámicos y las rutas estáticas, consulte en el anterior laboratorio como eliminar las rutas.

Conformar grupos de trabajos por cada router disponible en el laboratorio.

Es fundamental manejar los conceptos de internetworking del Capítulo 5 del semestre 3 de la Academia Cisco Networking.

Disponibilidad de un computador con HyperTerminal para realizar la conexión al puerto de consola con el router.

Recursos:

- 5 routers de Cisco debidamente configurados, o la cantidad disponibles en el laboratorio.
- 5 Computadores para conectarse a los routers.
- 5 Cables de consola (Roll over).

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.15 LABORATORIO No. 15

IGRP DE MÚLTIPLES RUTAS

Objetivos:

- Implementar las métricas de IGRP utilizadas en la selección de rutas para comprender la ruta que se selecciona para enrutar datos a un computador en particular.

Información Básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio para configurar los routers que utilizaran IGRP y observaran cómo IGRP utiliza las métricas para seleccionar la mejor ruta.

Metodología:

Se recomienda trabajar en grupos de 3 o más personas. Antes de empezar esta práctica de laboratorio, es fundamental manejar los conceptos de internetworking del Capítulo 5 del semestre 3 de la Academia Cisco Networking.

Disponibilidad de un computador con HyperTerminal para realizar la conexión al puerto de consola con el router.

Recursos:

- 5 routers de Cisco debidamente configurados, o la cantidad disponibles en el laboratorio.
- 5 Computadores para conectarse a los routers.

- 5 Cables de consola (Roll over).
- 4 Hubs Ethernet
- 1 Switch Ethernet
- 5 Cables de consola serial con convertidores de RJ-45 a DB9.
- 4 Conjuntos de cables seriales (DTE macho / DCE hembra)
- Cables Ethernet CAT5 o CAT6 de conexión directa.
- Transceivers AUI (DB15) a Ethernet RJ-45 para convertir las interfaces del router AUI a 10BASE-T RJ-45.

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.16 LABORATORIO No. 16

ACL ESTÁNDAR

Objetivos:

- Repasar las características y capacidades de las Listas de control de acceso IP estándar (ACL).
- Desarrollar una ACL estándar para permitir o denegar tráfico específico.
- Aplicar una ACL IP estándar a una interfaz de Router.
- Eliminar una ACL de una interfaz de Router y de un Router.

Información Básica:

Ver ANEXO 1.

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

Metodología:

Se puede trabajar individualmente o en equipos.

Recursos:

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

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.17 LABORATORIO No. 17

ACL EXTENDIDAS Y ACL EXTENDIDAS DE INTERNET

Objetivos:

- Repasar las características y capacidades de las listas de control de acceso IP extendidas (ACL).
- Desarrollar una ACL IP extendida para permitir o denegar tráfico específico.
- Aplicar una ACL IP extendida a una interfaz de Router.

Información Básica:

Ver ANEXO 1.

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

En esta práctica de laboratorio se trabaja con las ACL extendidas para regular el tráfico que se permite que pase a través del Router, según el origen y el tipo de tráfico. Las ACL son una

herramienta importante para controlar qué paquetes, y qué tipo de paquetes pueden pasar a través de un Router desde una red a otra.

Metodología:

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

Recursos:

- Configuración de laboratorio estándar de 5 Routers de Cisco, con hubs y switches.
- Estación de trabajo conectada al puerto de consola del Router mediante un cable rollover.
- Diseñar y planificar una ACL, según requisitos de seguridad específicos.
- Trabajar con las capacidades más avanzadas de las listas de control de acceso IP extendidas (ACL).
- Desarrollar una ACL extendida con múltiples sentencias.
- Desarrollar una ACL extendida para controlar el tráfico de Internet utilizando uno o más Routers.
- Desarrollar una ACL IP extendida para permitir o denegar otro tráfico específico del protocolo IP.

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.18 LABORATORIO No. 18

ENRUTAMIENTO IPX

Objetivos:

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

Información Básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio trabajará con el protocolo enrutado de Intercambio de paquetes de internetworking (IPX) de Novell. Los protocolos de capa 3 del modelo OSI, como IP e IPX, contienen información en sus paquetes que indica la red de proveniencia del paquete y a qué red se enviará. Los protocolos enrutables (como IP e IPX) son aquellos que pueden permitir que los paquetes se enruten entre redes y que les permiten que se dirijan desde una ubicación hacia otra. Los routers pueden ejecutar múltiples protocolos de enrutamiento (por ej., RIP e IGRP) y enrutados (IP e IPX). Para poder enrutar tanto IP como IPX, el Router debe mantener múltiples tablas de enrutamiento, una para cada tipo de protocolo enrutado que se reconoce.

Metodología:

Se puede trabajar individualmente o en equipos.

Recursos:

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

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.19 LABORATORIO No. 19

COMANDOS WAN

Objetivos:

- Explorar las capacidades WAN del router de acuerdo a la terminología usada en el semestre 4 sobre las WAN.
- Experimentar con algunos de los comandos del IOS relacionados con las WAN.

Información Básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio para introducirnos a las redes de área extensa o de gran alcance y el papel que desempeñan los router en ella.

Leer el Anexo 3.

Metodología:

Es fundamental manejar los conceptos de WAN del semestre 4 de la Academia Cisco Networking. También, se puede respaldar los conceptos con la guía del segundo año de la Academia Cisco Networking.

Recursos:

- Routers de Cisco, con hubs y switches.
- Terminales conectadas al puerto de consola de los routers disponibles.
- Manuales del router y acceso al sitio Web de Cisco

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.20 LABORATORIO No. 20

CONFIGURACIÓN DE PPP

Objetivos:

- Comprender en las conexiones seriales síncronas los diferentes tipos de encapsulamiento WAN.
- Convertir de encapsulamiento HDLC a PPP en una conexión WAN.

Información Básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio para centrarnos en el protocolo PPP (Protocolo punto a punto). Convirtiendo los enlaces WAN entre los routers de laboratorio de HDLC a PPP. Se debe establecer el encapsulamiento PPP en ambos extremos de la conexión WAN.

Metodología:

Es fundamental manejar los conceptos de PPP del semestre 4 de la Academia Cisco Networking. También, se puede respaldar los conceptos con la guía del segundo año de la Academia Cisco Networking, en el capítulo que trata sobre el protocolo PPP.

Se puede desarrollar a manera individual o grupal.

Recursos:

- Routers de Cisco.
- Hubs.

- Switches.
- 2 de esos routers disponibles para los enlace WAN con encapsulamiento HDLC, por defecto.
- Terminales conectadas al puerto de consola de cada router.

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

5.21 LABORATORIO No. 21

CONFIGURACIÓN DE FRAME RELAY

Objetivos:

- Afianzar los requisitos y opciones para las comunicaciones de Frame Relay simulando la configuración de un switch y de enlaces Frame Relay entre dos routers.

Información Básica:

Ver ANEXO 1.

De acuerdo a la anterior topología de red desarrollaremos este laboratorio se centra en el Protocolo de Conmutación de Paquete Frame Relay para realizar la conexión de dispositivos en una Red de Área Amplia (WAN).

Metodología:

Es fundamental manejar los conceptos de Frame Relay del semestre 4 de la Academia Cisco Networking. También, se puede respaldar los conceptos con la guía del segundo año de la Academia Cisco Networking, en el capítulo que trata sobre el protocolo Frame Relay.

Se puede desarrollar a manera individual o grupal.

Debemos tener en cuenta que esta práctica de laboratorio es simulada, porque es muy poco probable que se pueda disponer de un circuito real con una nube Frame Relay disponible para conectar y probar los cambios de configuración realizados a los routers.

Recursos:

- 3 Routers de Cisco con la versión de IOS 11.2 o posterior.
- Puertos seriales del router central conectados a cables seriales DCE.
- Hubs
- Switch conectado a los routers finales.
- Terminales conectadas a cada puerto de consola del router

Descripción:

NOTA: En el CD que acompaña esta monografía encontrarás la descripción del laboratorio en la carpeta: Capitulo V → Laboratorios

Archivos: Guía de Laboratorios.doc

CONCLUSIONES Y RECOMENDACIONES

Al llegar a este punto de la monografía se logra la satisfacción de cumplir con el objetivo trazado, dejando al programa de Ingeniería de Sistemas la fundamentación y documentación de la conmutación, del enrutamiento y de las tecnologías WAN que soportan el buen desarrollo de las prácticas de laboratorios de los semestre 3 y 4 de la Academia Networking Cisco, también en el CD que acompaña esta monografía se encuentra el material bibliográfico que nos sirvió de respaldo en la fundamentación y conceptualización.

La Universidad Tecnológica de Bolívar puede brindar a los próximos integrantes de futuros Minor en Comunicaciones y Redes, la posibilidad de que ellos también desarrollen las diferentes prácticas de laboratorios contempladas en los semestres Switching Basics and Intermediate Routing y WAN Technologies de la Academia Networking Cisco. El estudiante cuenta con esta documentación que les facilita su implementación en el Laboratorio de redes de la Universidad, porque contiene la práctica de cada laboratorio que se encuentra en la Guía de Laboratorio y la teoría de los temas que se manejan para cada laboratorio.

Se refuerza la comprensión de las siete capas del modelo OSI y su relación con el modelo TCP/IP, mediante la configuración de Switches y Routers durante el desarrollo de varias prácticas. Esto permite al estudiante del Minor, y en general del área de las Comunicaciones y Redes, encontrar un mejor afianzamiento de los conceptos de las capas del Modelo OSI, las cuales son base para la compresión de la infraestructura de una red.

La exploración de los switches Ethernet en el laboratorio de redes permite reunir mejor información sobre los conceptos de conmutación LAN y de VLAN. El estudio de las características y funcionamiento en la red de los switches, llevan al estudiante a comprender la evolución e implementación de estos dispositivos en las capas de red y transporte del Modelo OSI, y en un futuro, no muy lejano, en las siguientes capas.

Durante el desarrollo del laboratorio: Diseño de LAN conmutada, se comprenden las principales características de una red y la implementación de una metodología básica para el diseño de una LAN. Esto permite el fortalecimiento práctico de los conceptos de las capas del modelo OSI. Además, la investigación sobre los diferentes dispositivos que se utilizan durante este laboratorio lleva a explorar un tema nuevo: cableado estructurado.

La implementación de las prácticas con los protocolos de enrutamiento y enrutados soportados por los dispositivos de internetworking disponibles en el laboratorio de Redes de la Universidad Tecnológica de Bolívar, ayudó a la profundización sobre el tramado de cada uno y a conocer cuáles son sus características más relevantes, permitiéndonos así efectuar una comparación entre cada uno de ellos.

Se implementó en el laboratorio la práctica de Listas de Control de Acceso (ACL) estándar y extendida, utilizando los diferentes comandos del IOS de Cisco permitió que se analizará la forma de filtrar paquetes en la administración del tráfico y lograr examinar cada paquete que entra o sale de la LAN.

Se realizó una práctica completa con el protocolo enrutado de Intercambio de paquetes de Internetworking (IPX) de Novell, donde se configuró cada Router que estaba siendo utilizado para que enrutará los paquetes mediante este, con el fin de dar soporte a los clientes y servidores NetWare que implementan este tipo de protocolo.

El estudio del Protocolo de Conmutación de Paquete Frame Relay para la realización de conexiones entre los dispositivos en una Red de Área Amplia (WAN). Permite concluir, que Frame Relay es un servicio conmutado multiacceso, el cual incrementa la velocidad de una conexión de datos de área extensa, y obteniendo algunas diferencia con los demás protocolos que trabajan con conmutación de paquete. Frame Relay opera en la capa 2: enlace de datos del Modelo OSI, lo cual significa que es mucho más simple realizando menos comprobación y corrección de errores e incrementando la velocidad.

Los fundamentos de diseño WAN y el papel de los routers en ellas, se implementaron en las prácticas de los protocolos PPP, RDSI, IPX y Frame Relay. En la práctica PPP, se permitió obtener una mayor compresión del papel que desempeñan las conexiones seriales síncronas en los diferentes tipos de encapsulamiento WAN, se realizaron conversiones de encapsulamiento de HDLC a PPP en una WAN. En RDSI, se investigó acerca de este protocolo permitiendo su exploración conceptual. Adicional a esto, se encontraron varias páginas Web acerca de RDSI en Colombia que están incluidas en el CD.

NOTA: En el CD que acompaña esta monografía encontrarás mayor información en la carpeta: Otros apoyos → RDSI en Colombia → EPM.

Archivo: MICROEMPRESAS TELEFONIA LOCAL - ETB S_A_ ESP.htm

En las redes LAN se tuvo en cuenta la topología y los componentes de las tres primeras capas del Modelo OSI: física, de enlace de datos y de Red, para evaluar los requerimientos básicos de diseño para la implementación de una LAN. Son estas tres primeras capas del Modelo OSI, las que permiten diseñar una buena interconexión física de redes, explorando e implementando en los laboratorios los switches y routers se logró comprender el funcionamiento de ellos dentro de las redes permitiendo configurar los diferentes protocolos que se manejan.

Con la fundamentación de las tecnologías WAN contenida en esta monografía, se desarrollan con mayor seguridad los laboratorios del Semestre 4: WAN Technologies. Implementando protocolos como PPP Y Frame Relay. También, se logró documentar acerca de las Listas de Control de Acceso (ACL), por medio de un ejemplo práctico, se encuentra de anexo en esta monografía.

El Protocolo de Conmutación de Paquete Frame Relay permite la conexión de dispositivos en una Red de Área Amplia (WAN). La interconexión de LAN permite llegar a las WAN, por eso es necesario conocer los diseños que se implementan en las LAN.

Se recomienda para el aprovechamiento de esta monografía que después de leerla se consulte el material de apoyo que se encuentra en el CD. También, se debe consultar la Guía del Primer y Segundo año de la Academia de Networking Cisco para ampliar los conocimientos que se involucran durante el desarrollo de las diferentes prácticas de laboratorios.

Para quienes deseen seguir aportando conocimientos al área de las comunicaciones y redes se les recomienda profundizar en la fundamentación de los diferentes protocolos que se implementan en los diferentes laboratorios.

Además del material aquí documentado, también se debe navegar en el material en línea que brinda la Academia Networking Cisco en su página, http://cisco.netacad.net y en la Ciscopedia (en el CD se incluye el archivo de instalación), para una mejor compresión de las estructuras de los laboratorios.

En lo posible utilizar la topología de red recomendada. Sin embargo, no cerramos las posibilidades a la implementación de los laboratorios con otras topologías de red que no se aparezcan descritas en esta monografía.

Identificar antes de cada laboratorio los diferentes recursos que se usan para llevar a cabo el buen desarrollo de la práctica, esto con el fin de evitar daños entre los diversos dispositivos que se implementan.

Consultar a un instructor de la Academia Cisco si no se tiene claro el objetivo de la práctica de laboratorio, o en caso de confusiones entre las funciones de los dispositivos. También, se cuenta con la ayuda de los profesores del Minor.

Revisar los recursos antes de realizar la práctica, como son cables con los respectivos conectores, etc., de acuerdo a los requerimientos y características básicas de la topología del laboratorio.

BIBLIOGRAFÍA

Libros:

- BLACK, Ulyess .Tecnologías emergentes para redes de computadores. Segunda Edición. Pearson. 1999
- PANCUCCI, Dom. Soluciones de Conmutación. Guía de Switching 3COM. Primera Edición. © 3Com Europe Ltd. 2001. España.
- AMATO, Vito, ACADEMIA DE NETWORKING DE CISCO SYSTEMS: GUÍA DEL PRIMER AÑO. Cisco Systems, Inc. Segunda edición. Pearson Educación. 1024 páginas. 2000

Trabajo de Investigación:

- ORTIZ ISLAS, Antonio; GALLEGOS GALLEGOS, Patricia; Diseño de Redes IP. México, 2002, 40 h. Trabajo de Investigación. Departamento de Ingeniería Electrónica - Área de Comunicaciones. Centro de Investigación en Computación - IPN.
- RUEDA RIVERA, Jaime Antonio. Redes LAN – MAN – WAN. Cartagena. 2003. Minor de Comunicaciones y Redes. Universidad Tecnológica de Bolívar.

Páginas Web:

- CISCO NETWORKING ACADEMY: Material Online CCNA. Semestres Switching Basics and Intermediate Routing y WAN Technologies.

  http://cisco.netacad.net

- CISCO:

  http://www.cisco.com

- Modulo LAN – MAN – WAN

  http://www.monografias.com/trabajos13/corpo/corpo.shtml

- CSMA/CD

  http://www.guajara.com/wiki/es/wikipedia/c/cs/csma_cd.html

- Cisco - Conmutación LAN:

  http://www.eduangi.com/documentos/2_CCNA2.pdf.

- Tecnologías de conmutación PSTN:

  http://portalgsm.com/documentacion_extendida/83_0_17_0_C/

- Fundamentos de Telefonía:

  http://www.freepgs.com/vgozalbes/documents/manuales/f_tel.pdf

- Planificación y evaluación de redes:

  http://iio.ens.uabc.mx/~jmilanez/escolar/redes/01090000.html

- Tecnología y conmutación de redes:

  http://www.consulintel.es/Html/Tutoriales/Articulos/tecn_conm.html

- ¿Switching vs. Routing?

  http://neutron.ing.ucv.ve/revista-e/No4/articulo.htm

- Enrutamiento y Protocolos de enrutamiento:

  http://www.eafit.edu.co/cursos/

  http://www.gfc.edu.co/estudiantes/anuario/2001/sistemas/halime/enruter.html#SEC1

  http://www.eduangi.com/documentos/16_CCNA.pdf

- Estructuras de redes:

  http://www.wl0.org/~sjmudd/wireless/network-structure/html/x284.html

- El nivel de red: Generalidades

  http://www.uv.es/˜montanan/redes/redes_02.rtf

- Estándares WAN:

  http://www.eduangi.com/documentos/16_CCNA.pdf

Bibliografía recomendada para Consulta

Libros

- STALLINGS, William. Comunicaciones y redes de computadores. Sexta Edición. Prentice – Hall. 200
- Ciscopedia v1.0. Copyright Cisco Systems, Inc. 2001, 2002. World Wide Education

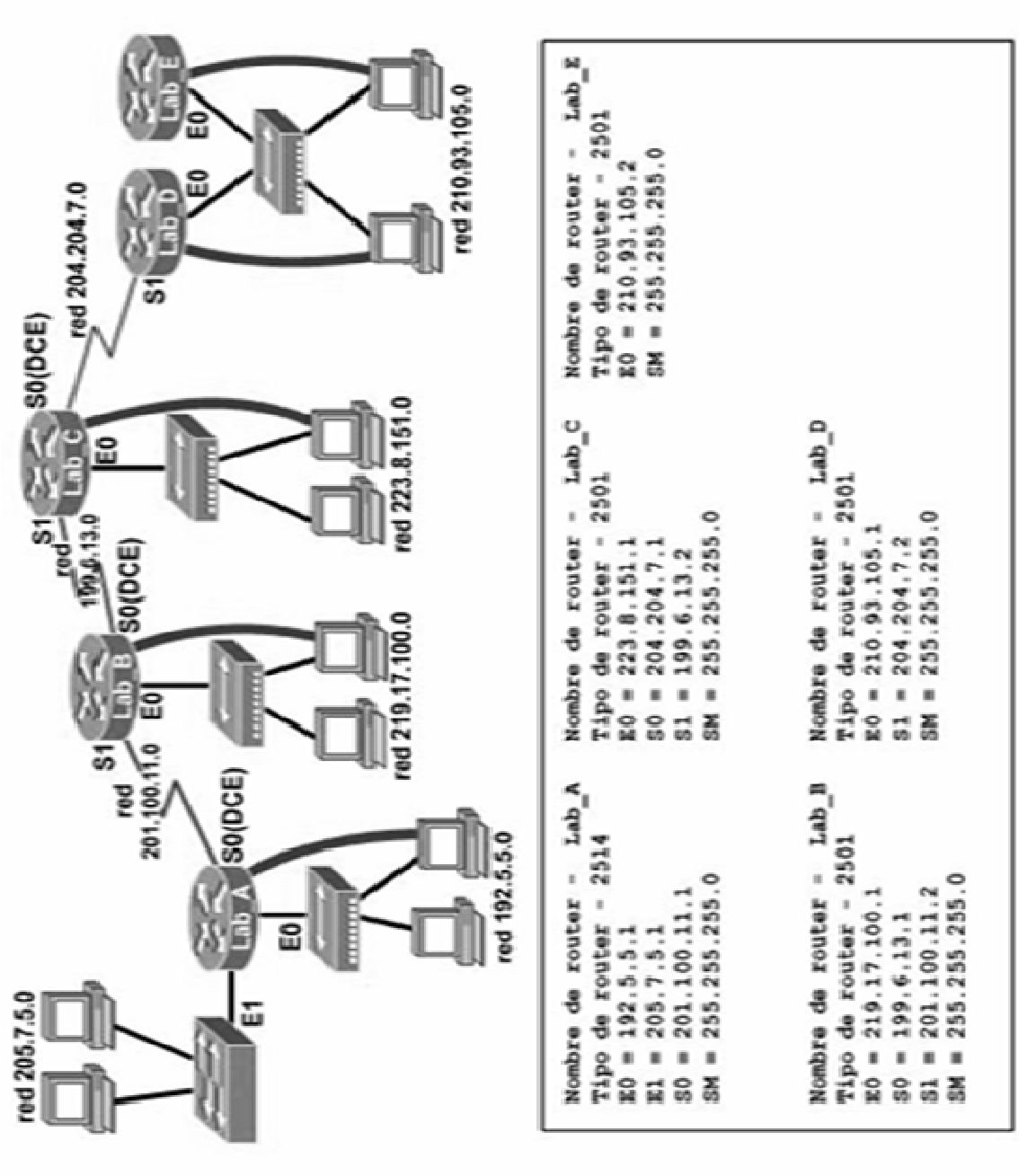
Páginas Web:

- CISCO: http://www.cisco.com
- IBM: http://www.ibm.com
- 3COM: http://www.3com.com

- Manuales:http://es.tldp.org/Manuales-LuCAS/AA_Linux_colegio- 1.1/AA_Linux_colegio-1.1-html/x12688.htm
- Routers: http://lfuente.8m.com/Routers.htm
- Tecnologías de comunicaciones: Una mirada el estado del arte. http://www.disol.com.co/Documentos/tech2.pdf

ANEXO 1

TOPOLOGÍA DE RED RECOMENDADA PARA LOS LABORATORIOS[*]



[*] Academia Cisco Online: http://cisco.netacad.net

ANEXO 2

Laboratorio No. 11

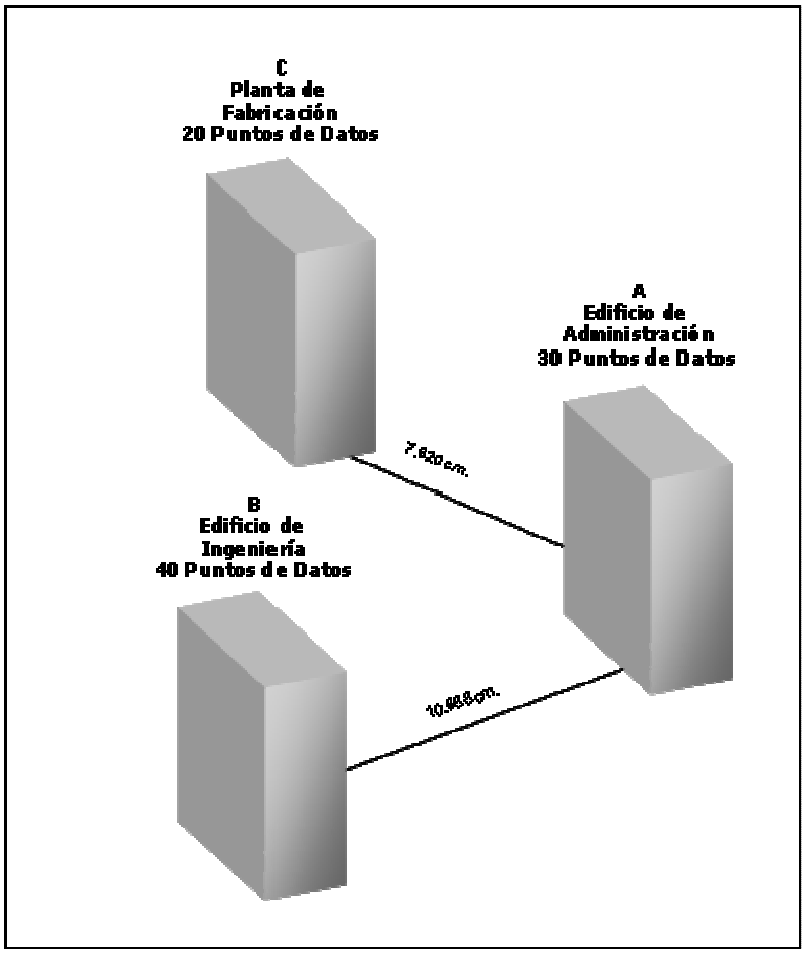


Figura 1: Empresa

ANEXO 3

LAN vs. WAN

Las redes de área local, LAN, normalmente se componen de un grupo de computadores interconectados mediante hubs o switches utilizando cable físico (cable de cobre de par trenzado y fibra multimodo). Las WAN se componen de dos o más LAN ubicadas en sitios geográficamente separados. Normalmente usan servicios suministrados por una portadora de larga distancia con transmisión a través de fibra o microondas para conectar los sitios. Una organización puede ser propietaria del equipo que interconecta sus sitios WAN pero con mayor frecuencia arrienda enlaces WAN a un proveedor de servicios.

Routers y WAN

Aunque se pueden utilizar routers para subdividir las LAN de campus para limitar el tamaño de los dominios de broadcast y ayudar a mantener la seguridad, en general se usan con mayor frecuencia para interconectar las LAN formando WAN. El router es la interfaz o gateway desde la LAN a la WAN. En las WAN de la mayoría de las organizaciones, cada ubicación tiene por lo menos un router con una interfaz o enlace a una o más ubicaciones en la WAN. Esto se logra normalmente a través de una CSU/DSU (Unidad de Servicio de Canal / Unidad de Servicio de Datos). Hoy en día, inclusive las organizaciones pequeñas con una sola ubicación necesitan un router para conectarse a la WAN más grande del mundo, Internet.

Las WAN y el modelo OSI

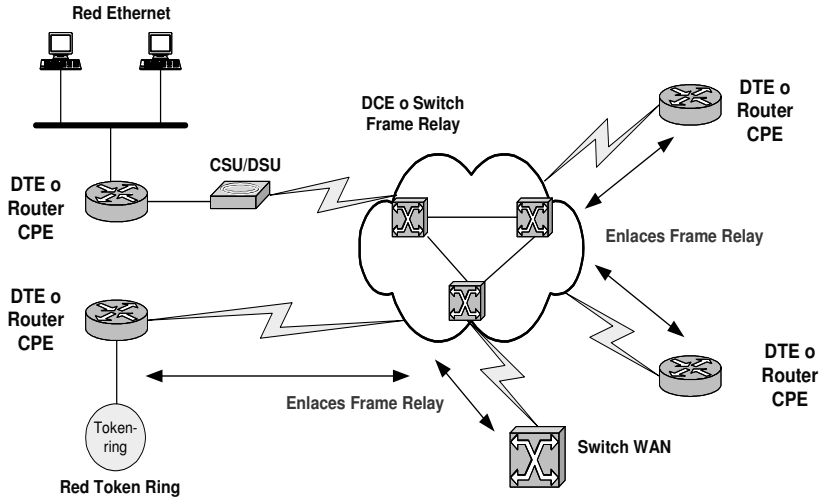
Los enlaces WAN normalmente operan a nivel de Capa 2 del modelo OSI: enlace de datos y convierten el encapsulamiento de trama LAN como Ethernet o Token Ring en encapsulamiento de trama de Capa 2 de área amplia como HDLC, PPP o Frame Relay. Por ejemplo, supongamos que hay dos LAN Ethernet interconectadas mediante un enlace WAN (como T1) y una Terminal en la LAN A necesita conectarse a un servidor en la LAN B. La Terminal envía un paquete a la interfaz Ethernet (por ej., E0) del router en la LAN A. Este router elimina el encabezado de trama LAN Ethernet, lo reemplaza por un encabezado de trama WAN como Frame Relay o PPP y lo envía desde una de sus interfaces seriales (por ej., S0). Cuando el router en LAN B recibe el paquete en su interfaz serial, elimina el encabezado de trama WAN y lo reemplaza por el encabezado de trama LAN Ethernet. El paquete se entrega al servidor local en la LAN B a través de la interfaz Ethernet del router.

ANEXO 4

FRAME RELAY*

Frame Relay es una tecnología de conmutación rápida de tramas que corre sobre enlaces confiables a velocidades hasta de 2.048 Mbps., y no hace verificación de errores en los datos, esta característica permite que transporte datos más rápidamente que tecnologías de conmutación de paquetes como X.25.

La red Frame Relay consiste de switches suministrados por el proveedor de los enlaces en la que los ruteadores del cliente se conectan como equipos terminales de datos (DTE). A cada cliente se le asigna un circuito virtual para que pueda hacer uso de la red. Por ejemplo:



* ORTIZ ISLAS, Antonio; GALLEGOS GALLEGOS, Patricia; Diseño de Redes IP. México, 2002, 40 h. Trabajo de Investigación. Departamento de Ingeniería Electrónica - Área de Comunicaciones. Centro de Investigación en Computación - IPN.

ANEXO 5

RDSI

RED DIGITAL DE SERVICIOS INTEGRADOS

La Red Digital de Servicios Integrados ofrecida por las compañías telefónicas, utiliza tecnología digital para transportar información de diversos tipos tales como datos, voz y video. Existen dos tipos de interfaces en esta tecnología la interfase básica (BRI) y la interfase primaria (PRI). La interfaz BRI suministra dos enlaces de datos de 64 kbps (llamados canales B) y un enlace de 16 kbps, para operaciones de control del enlace (llamado canal D). La interfaz primaria (PRI) soporta enlaces E1 (2.048 Mbps), y suministra 30 enlaces de 64 kbps para datos y 1 canal de 64 kbps para el control de la transmisión*.

Actualmente pese a que la RDSI todavía esta a medio construir, los ingenieros ya están pensando en su sucesora: la RDSI de banda ancha. Esta nueva red será, fundamentalmente, idéntica a la RDSI actual con la diferencia de que la velocidad mínima de los canales será de 2 Mbps., pudiendo llegar a los 100. Los investigadores ya están desarrollando toda una nueva gama de aplicaciones para esta nueva tecnología, que podrá sentar las bases de toda una nueva gama de servicios basados en la televisión de alta definición.

* ORTIZ ISLAS, Antonio; GALLEGOS GALLEGOS, Patricia; Diseño de Redes IP. México, 2002, 40 h. Trabajo de Investigación. Departamento de Ingeniería Electrónica - Área de Comunicaciones. Centro de Investigación en Computación - IPN.

NOTA: En el CD que acompaña esta monografía encontrarás información sobre algunas estadísticas, proveedores y funcionamiento RDSI, en la carpeta: Otros apoyos → RDSI en Colombia.

Referencia Bibliografía:

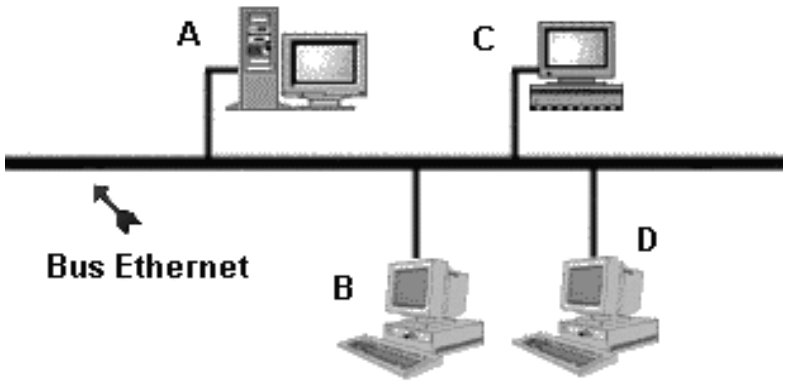
- Documento sobre Telefonía Local – Año 2001: http://www.dnp.gov.co/ArchivosWeb/Direccion_Infraestructura_Energia/Telecomunicaciones/Telefonia_Local/Documento_Telefonia_Local_2001.pdf
- El sector de las comunicaciones en la década de los 90's – Análisis Estadístico "Operadores de telefonía local y/o extendida en operación" Pág. 20 – SS: http://www.crt.gov.co/documentos/infeconomica/publi_sector/AnexoEstadistico.pdf
- Proveedor ETB - RDSI BÁSICO http://www.etb.com.co/empresas/microem/tproducto.asp?prod=64&cat=&rol=B
- Proveedor TELEARMENIA TELECOM – Servicio RDSI http://www.telearmenia.net.co/59.htm

ANEXO 6

ETHERNET*

En estos momentos, las redes Ethernet son el tipo más popular de red en el mundo. Esta tecnología es fácil de implementar y el costo por puerto es el mas bajo comparativamente a otras tecnologías. Estas redes son fáciles de administrar y los equipos necesarios para implementar este tipo de redes, se encuentran ampliamente disponibles en el mercado.

Las redes Ethernet, emplean el protocolo CSMA/CD (carrier sense multiple access with collision detection, Acceso Múltiple mediante detección de portadoras con Detección de Errores). En estas redes todos los miembros de la LAN transmiten datos de manera aleatoria y cuando ocurre alguna colisión en la red las estaciones dejan de transmitir. Las redes Ethernet, son un ejemplo típico de las redes de broadcast.



* ORTIZ ISLAS, Antonio; GALLEGOS GALLEGOS, Patricia; Diseño de Redes IP. México, 2002, 40 h. Trabajo de Investigación. Departamento de Ingeniería Electrónica - Área de Comunicaciones. Centro de Investigación en Computación - IPN.

En la figura anterior, cuando la estación de trabajo A desea transmitir datos a la red, primero debe escuchar el bus y determinar si alguien esta ocupando el canal. Si la red esta ocupada, espera a que se libere el canal antes de intentar enviar datos. Dependiendo del tamaño del bus y del número de estaciones en la red LAN, es posible que se presente alguna colisión en la red. Cuando las estaciones de trabajo detectan una colisión en la red esperan un tiempo aleatorio para intentar ocupar el canal.

La posibilidad de que se presente una colisión depende de los siguientes parámetros:

- El numero de estaciones en la red - Mientras mas estaciones existan en la red LAN, mayor es la probabilidad de que se presenten colisiones.
- La longitud de la red - En redes extensas es mayor la posibilidad de que se presenten colisiones.
- La longitud del paquete de datos - Las tramas de datos grandes toman mas tiempo para transmitirse, esto incrementa la posibilidad de una colisión. El tamaño de una trama en una red Ethernet varia entre 64 y 1516 bytes.

La tecnología Ethernet ha evolucionado desde 10 Mbps (10BaseT) hasta 100 Mbps (100BaseT) o FastEthernet, en cableado de par trenzado y actualmente se alcanzan velocidades de 1 Gbps (Gigabit Ethernet).

La tecnología FastEthernet es diez veces más rápida que Ethernet, esta tecnología opera sobre enlaces de fibra óptica o cableado de par trenzado. La tecnología Gigabit Ethernet ó IEEE 802.3z es

diez veces mas rápida que FastEthernet y reduce la distancia de la red de forma significativa comparada con Ethernet.

Con la introducción de switches que proveen una conexión dedicada a 10 ó 100 Mbps a cada usuario, la velocidad de transferencia de datos se ha incrementado y es posible manejar diversas aplicaciones de manera simultánea. A continuación se presenta una tabla que muestra la relación entre las aplicaciones y el ancho de banda.

Aplicaciones	Ancho de banda ocupado (Mbps)
Aplicaciones de red (correo electrónico, salvar archivos)	2
Voz	0.064
Videos MPEG-1	0.6
Videoconferencia	0.384
Ancho de banda total	< 4

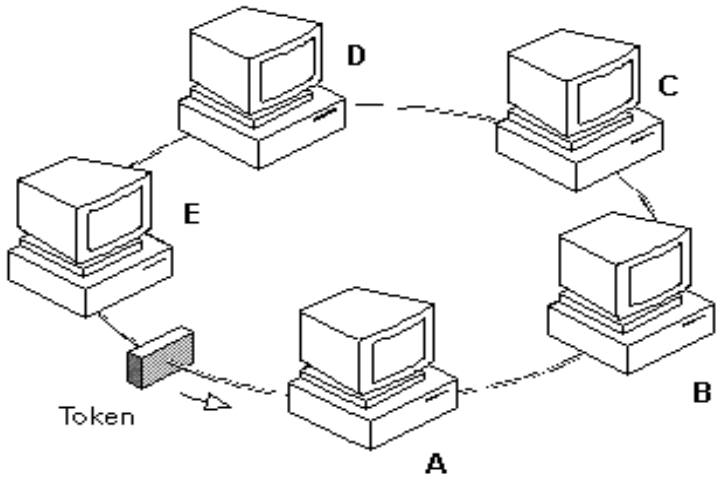
La tecnología Ethernet se comporta bien en aplicaciones que no demandan una gran cantidad de ancho de banda. Debido a su naturaleza indeterminística en la entrega de datos, los tiempos de respuesta de una red Ethernet no pueden ser valorados.

ANEXO 7

TOKEN RING*

Token Ring llegó a ser muy popular pero las empresas que lo optaron luego se miraron a Ethernet. Fueron las redes distribuidas quienes más aportaron a la conmutación.

La tecnología Token Ring se desarrollo en la década de los 70's y ocupa el segundo lugar en importancia detrás de Ethernet y soporta velocidades de 4, 16 ó 100 Mbps. Esta tecnología es un ejemplo de una red de paso de testigo en la que los miembros de la red transmiten datos solo cuando capturan el Token, en las redes Token Ring no se presenta el fenómeno de colisiones característico de las redes Ethernet.



* ORTIZ ISLAS, Antonio; GALLEGOS GALLEGOS, Patricia; Diseño de Redes IP. México, 2002, 40 h. Trabajo de Investigación. Departamento de Ingeniería Electrónica - Área de Comunicaciones. Centro de Investigación en Computación - IPN.

Como se muestra en la figura, todas las estaciones están conectadas en forma de anillo, el acceso al anillo esta controlado por el token que circula a través del anillo. Cuando la estación A desea transmitir datos a la estación D, captura el token y cambia el contenido de la trama, ya que agrega datos al token y retransmite la trama. Cuando la trama alcanza a la estación B, esta estación, verifica si transporta datos para ella, ya que los datos se dirigen a la estación D, entonces B retransmite la trama y esta acción se repite hasta que la trama llega a la estación D. La estación D guarda una copia de la información y retransmite la trama al anillo. Posteriormente, la trama de información circula alrededor del anillo hasta que llega a la estación emisora A y entonces la trama se elimina. La estación emisora puede verificar si la trama se recibió y se copió en el destino.

La técnica de paso de testigo permite que los retardos puedan determinarse. Otra característica de las redes Token Ring, es que ofrecen diagnósticos de red y métodos de auto recuperación del enlace tales como:

- Diagnostico de enlaces
- Detección de pérdida de señal.
- Funciones de monitoreo activo del anillo.
- Detección de errores de transmisión y reportes.
- Aislado de componentes en falla para una recuperación automática del anillo.

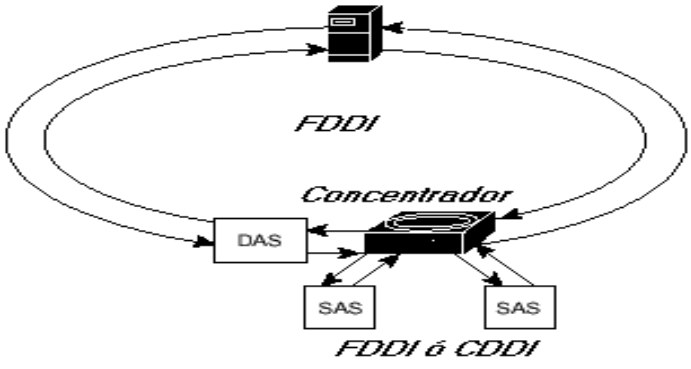
ANEXO 8

FDDI*

FIBER DISTRIBUTED DATA INTERFACE

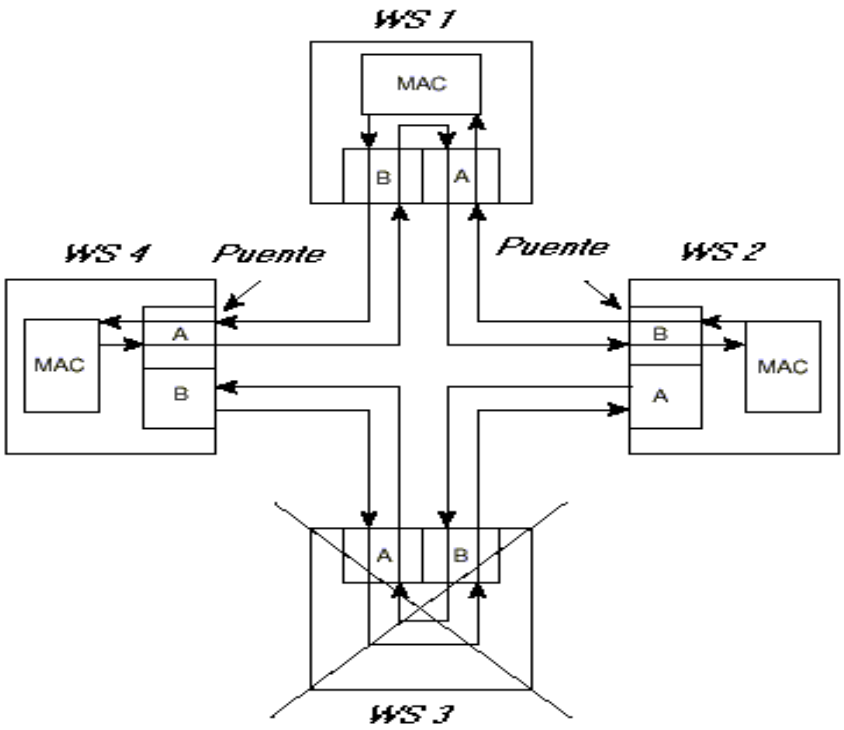
La tecnología FDDI fue desarrollada a principios de la década de los 80, para conexiones de host a alta velocidad, posteriormente los administradores de red la utilizaron para establecer enlaces troncales o de backbone. Al igual que Token Ring, FDDI emplea el método de paso de testigo para operar y se diferencia de Token Ring en cuanto a que utiliza dos anillos en lugar de uno, un anillo primario y un anillo secundario. El anillo principal es el que se usa normalmente, dejando al anillo secundario en modo de espera. FDDI ofrece flexibilidad y redundancia y puede conectar estaciones en forma dual (DAS – Dual Attachment Station) o única (SAS- Single Attachment Station).

En modo DAS las estaciones conectan a la red los puertos A y B disponibles como se muestra en el diagrama.



* ORTIZ ISLAS, Antonio; GALLEGOS GALLEGOS, Patricia; Diseño de Redes IP. México, 2002, 40 h. Trabajo de Investigación. Departamento de Ingeniería Electrónica - Área de Comunicaciones. Centro de Investigación en Computación - IPN.

En la configuración mostrada anteriormente, la red consiste de un anillo primario y un anillo secundario. Bajo condiciones normales, los datos viajan por el anillo primario y el anillo secundario funciona como respaldo del enlace. Cuando se presenta una falla en la red, las estaciones conectadas directamente a la estación en falla puentean sus enlaces primarios con el anillo de respaldo y nuevamente la red entra en operación. De este modo, la red recupera el anillo primario como se muestra en la siguiente figura.



ANEXO 9

ACL

LISTA DE CONTROL DE ACCESO*

NOTA: En el CD que acompaña esta monografía encontrarás mayor información en la carpeta: Otros apoyos → Enrutamiento → ACL

Archivos: Fundamentación y Práctica de ACL.pdf

EJEMPLO DE WILDCARD

Tenemos determinada identificación de red 192.5.34.0 con su respectiva 0.0.0.255 máscara wildcard.

0.0.0.255 escrito en notación decimal equivaldría a 00000000.00000000.00000000.11111111 escrito en sistema binario. Se comparan octeto a octeto cada uno de bits de la dirección de subred 192.5.34.0 con los de la máscara wildcard. Visto de esta manera, se correspondería cada bit superior con el inferior.

11000000.00000101.00100010.00000000

00000000.00000000.00000000.11111111

* UNIDAD DOCENTE DE REDES. Práctica No. 4 – Configuración de Routers: Listas de Control de Acceso. Área de arquitectura y tecnologías de computadores. Departamento de Informática. Universidad de Castilla – La Mancha. España http://www.info-ab.uclm.es

Los bits de wildcard “0” indican que se verifican los bits de la dirección IP contra la cual se contrastan. Los bits de wildcard “1” indican que se ignoran los bits contra los cuales se comparan. Como los bits “1” sólo afectan a la porción de host de esa dirección de red, esto se interpreta que podrán pasar por determinada interfaz del Router aquellos hosts cuya dirección IP comience con 192.5.34.xxx o sea serán desde 192.5.34.1 hasta 192.5.34.254. La dirección 192.5.34.0 no se destina al uso como host sino que queda asignada como identificación de red.

GUÍA DEL CD

MONOGRAFÍA: **CONMUTACIÓN, ENRUTAMIENTO Y TECNOLOGÍAS WAN**

CARPETA	**ARCHIVOS**
PROPUESTA DE LA MONOGRAFÍA	Propuesta Conmutación, Enrutamiento y Tecnologías WAN
ÍNDICES – GLOSARIO	Tabla de Contenido Lista de cuadros Lista de figuras Lista de anexos Glosario Apoyo - Glosario general Guía del CD
CAPÍTULO I	Capítulo I Generalidades de la conmutación, del enrutamiento y de las tecnologías WAN
CAPÍTULO II	Capítulo II Conmutación
CAPÍTULO III	Capítulo III Enrutamiento.doc
CAPÍTULO IV	Capítulo IV Tecnologías WAN
CAPÍTULO V	Capítulo V Laboratorios – Presentados
CONCLUSIONES Y RECOMENDACIONES –	Conclusiones y recomendaciones

BIBLIOGRAFÍA	Bibliografía
ANEXOS	Todos los Anexos
SUSTENTACIÓN	Sustentación Conmutación, Enrutamiento y Tecnologías WAN
PRÁCTICAS DE LABORATORIOS	21 Laboratorios uno en cada archivo
OTROS APOYOS	Conmutación Enrutamiento Tecnologías WAN Historia de las comunicaciones Modelo OSI Artículos de Interés general Temario de la teoría de redes
Monografía Completa	