UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

REDES VIRTUALES (VLANs), SU TECNOLOGÍA Y SUS APLICACIONES

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN
P R E S E N T A N:

Damián Lorenzo León
Juan Camargo Méndez
Tania Lizbeth Carlos Fortanel

DIRECTOR DE TESIS: M.I. Jorge Valeriano Assem

CD. UNIVERSITARIA MÉXICO DF ABRIL 2004

AGRADECIMIENTOS

A la Universidad Nacional Autónoma de México, por ser nuestra Alma Mater.

Al M.I. Jorge Valeriano Assem, por habernos orientado en la realización de este trabajo.

A los profesores: Ing. Laura Sandoval Montaño, M.C. María Jaquelina López Barrientos, Ing. Norma Elva Chávez Rodríguez e Ing María del Rosario Barragán Paz; gracias por sus observaciones y consejos.

Cuando la meta soñada se ha cumplido, es importante detener el paso y dar gracias a aquellos que han hecho posible. Por tal motivo, no puedo dejar de dar gracias a Dios por hacer posible este momento.

A mis padres Carmen y Luis por todo su apoyo que me han dado en todo momento, por darme la oportunidad de recibir una educación, por haberme guiado por un camino que me ha dado satisfacciones y por todo su amor.

A mis hermanas Teresa y Cecilia, por su motivación que me han dado, para terminar mi carrera; gracias y les deseo lo mejor de la vida.

A mis amigos, que de alguna forma me han motivado y apoyado para llegar hasta aquí; ya que los recordare siempre.

Juan Camargo Méndez

“El corazón del hombre traza su rumbo, pero sus pasos los dirige el Señor”
Proverbios 16.9

A mis padres

Este trabajo es para ustedes, va acompañado de mis mas sincero agradecimiento por ser el gran ejemplo que me ha inspirado a salir adelante. Su gran amor, confianza, paciencia y dedicación hacia mi ha sido el motivo que me ha llevado a hasta este lugar. Los amo muchísimo.

A mi hermano Víctor

Con un profundo cariño, lo mejor que me pudo pasar en la escuela es haberte tenido cerca, gracias por siempre cuidarme y preocuparte por mi, este trabajo también es tuyo.

A Iliana y Minerva

Por todos los bellos momentos que se han quedado grabados en mi mente, su compañía dentro y fuera de la Facultad lleno de fortaleza mi vida al compartir con ustedes risas, lagrimas, tiempos buenos y también tiempos difíciles.

A Vero, Citlali, Jesús, Lina, Abigail, Israel, Carlos, Sergio, Mario

Porque su amistad siempre me ha llenado de alegría y con quien he compartido muchas experiencias.

A mis abuelos, tíos, primos y sobrinos

Quienes han estado cerca de mi, me han depositado su confianza y me han impulsado a seguir adelante.

A mis profesores

Que con sus enseñanzas me han enseñado a buscar el camino de la superación.

Al M. I. Jorge Valeriano Assem

Quien nos brindo su tiempo y su paciencia para la elaboración de éste trabajo.

Finalmente agradezco a la **Facultad de Ingeniería** por la preparación formativa y profesional que me brindo durante mi estancia en ella.

Tania Lizbeth Carlos Fortanel

A mi esposa **Elsa**, por su apoyo incondicional y
permanente, por alentarme a seguir adelante
en todo momento, por su paciencia
y gran cariño.

A mis padres **Maurilio y Maximina**, por su apoyo
y el haberme brindado la oportunidad
de superarme en la vida.

A mis hermanos por su cariño y apoyo.

A Dios, por darme las fuerzas necesarias
para seguir adelante y alcanzar uno de mis objetivos.

Gracias

Damián Lorenzo León

INDICE

INTRODUCCIÓN

En general una red es un conjunto de computadoras que se utilizan para compartir recursos y el objetivo es hacer que todos los programas, el equipo y especialmente los datos estén disponibles para cualquiera en la red

Los grupos de trabajo en una red, hasta ahora, han sido creados por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo switch ó hub.

Como consecuencia directa, estos grupos de trabajo comparten el ancho de banda disponible y los dominios de broadcast, y con la dificultad de gestión cuando se producen cambios en los miembros del grupo. Más aún, la limitación geográfica que supone que los miembros de un determinado grupo deben de estar situados adyacentemente, por su conexión al mismo concentrador o segmento de la red.

Los esquemas VLAN (Red Virtual de Área Local), nos proporcionan los medios adecuados para solucionar esta problemática, por medio de la agrupación realizada de una forma lógica en lugar de física.

Sin embargo, las redes virtuales siguen compartiendo las características de los grupos de trabajo físicos, en el sentido de que todos los usuarios tienen conectividad entre ellos y comparten sus dominios de broadcast.

La principal diferencia con la agrupación física es que los usuarios de las redes virtuales pueden ser distribuidos a través de una red LAN, incluso situándose en diferentes concentradores de la misma, manteniendo su pertenencia al grupo de trabajo lógico.

Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, logramos, como consecuencia directa, el incremento del ancho de banda en dicho grupo de usuarios.

Además, al poder distribuir a los usuarios en diferentes segmentos de la red, podemos situar puentes y routers entre ellos, separando segmentos con diferentes topologías y protocolos. Así por ejemplo, podemos mantener diferentes usuarios del mismo grupo, unos con FDDI y otros con Ethernet, en función tanto de las instalaciones existentes como del ancho de banda que cada uno precise, por su función específica dentro del grupo.

Todo ello, por supuesto, manteniendo la seguridad deseada en cada configuración por el administrador de la red: Se puede permitir o no que el tráfico de una VLAN entre y salga desde hacia otras redes.

Pero aún se puede llegar más lejos. Las redes virtuales nos permiten que la difusión geográfica no se limite a diferentes concentradores o plantas de un mismo edificio, sino a diferentes oficinas intercomunicadas mediante redes WAN o MAN, a lo largo de países y continentes, sin limitación ninguna más que la impuesta por el administrador de dichas redes.

El objetivo de realizar esta tesis no es solo para cubrir el requisito de titulación, sino también, proporcionar al lector los conocimientos básicos acerca de las VLAN, los

beneficios de su implementación, los inconvenientes de su uso, y finalmente, donde se están aplicando actualmente.

En el primer capitulo se proporciona información general sobre las topologías y protocolos para redes LAN más utilizados, el modelo de referencia OSI.

En el segundo capitulo se habla de los elementos de interconexión de red, así como de los medios de trasmisión que difunden por toda la red física los datos, la interfaz de red que permite a las computadoras conectarse a la red, los sistemas operativos que administran toda la red y los dispositivos como hubs, switches y el routers entre otros, que difunden la información por la red.
El capitulo tres es la base de esta tesis, aquí se engloba toda la información sobre los conceptos relacionados con las redes virtuales de área local (VLANs), también se tratan la segmentación como medida para disminuir la cantidad de colisiones en la red y la conmutación que es un tema muy importante para la construcción de VLANs. Se habla de los diferentes tipos de VLANs, sus ventajas y desventajas, así como de los beneficios que proporcionan a las redes LAN tradicionales.

En el capitulo cuatro se proporcionan las bases para llevar a cabo la implementación de una VLAN, así como algunos ejemplos de cómo es que problemas complejos de redes de diferente índole se resuelven al aplicar redes virtuales.

En el quinto y ultimo capitulo se propone el temario para la asignatura optativa de Redes Virtuales de Área Local con algunas practicas de laboratorio que tienen como objetivo reforzar los conocimientos adquiridos sobre VLANs.

Fundamentos de redes

Capítulo

1

1.1 DEFINICIÓN DE RED.

Una red local es un sistema de comunicaciones de datos que permite a un número de dispositivos independientes comunicarse entre sí.

Las redes en general, consisten en compartir recursos físicos y lógicos; uno de sus objetivos es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario, facilitando la comunicación y el trabajo en grupo. En otras palabras, el hecho de que un usuario se encuentre distanciado de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente. La información que pueden intercambiar las computadoras de una red puede ser de lo más variada: correos electrónicos, vídeos, imágenes etc.

1.1.1 Clasificación de redes.

Podemos clasificar las redes en las dimensiones de la tecnología de transmisión y por su alcance geográfico.

Por su Tecnología de Transmisión:

- **Broadcast:** Las redes de difusión (broadcast) tienen un solo canal de comunicación, por lo que todas las máquinas de la red lo comparten. Si una máquina envía un mensaje corto – en ciertos contextos conocido como paquete -, todas las demás lo reciben, un campo de dirección dentro del paquete especifica el destinatario. Cuando una máquina recibe un paquete verifica el campo de dirección. Si el paquete va destinado a esa máquina, ésta lo procesa; si va destinado a alguna otra lo ignora.

  Por lo general, los sistemas de difusión también permiten el direccionamiento de un paquete a todos los destinos utilizando un código especial en el campo de dirección. Cuando se transmite un paquete con este código, todas las máquinas de la red lo reciben y procesan. Este modo de operación se conoce como difusión (broadcast). Algunos sistemas de difusión también soportan la transmisión a un subconjunto de máquinas, algo conocido como multidifusión (multicast). Un esquema posible es la reserva de un bit para indicar la multidifusión los bits de dirección n-1 restantes pueden contener un número de grupo. Cada máquina puede suscribirse a alguno o a todos los grupos. Cuando se envía un paquete a cierto grupo, se distribuye a todas las máquinas que se suscriben a ese grupo.

- **Point to point (punto a punto):** Constan de muchas conexiones entre pares individuales de máquinas. Para ir del origen al destino, un paquete en este tipo de red podría tener que visitar primero una o más máquinas intermedias. A menudo es posible que haya varias rutas o longitudes diferentes, de manera que encontrar las correctas es importante en redes punto a punto. Por regla general (aunque hay muchas excepciones), las redes más pequeñas localizadas en una misma área geográfica tienden a utilizar la difusión, mientras que las más grandes suelen ser de punto a punto. La transmisión de punto a punto con un emisor y un receptor se conoce como unidifusión (unicast).

Por su alcance geográfico:

- **LAN** (Local Area Network): Una red de área local es un sistema de comunicaciones constituido por un conjunto de hardware (cableado, dispositivos, PC's, servidores, etc.) y software que se distribuyen por una extensión limitada (planta, edificio, grupo de edificios) en el que existen una serie de recursos compatibles (discos, impresoras, bases de datos, etc.), a los que pueden tener acceso los usuarios para compartir información de trabajo.

  Según el comité IEEE 802 una LAN se distingue de otros tipos de redes de datos en que las comunicaciones se restringen a un área geográfica limitada (Figura 1.1), y que pueden depender de un canal físico de comunicaciones con una velocidad binaria alta y que presenta una reducida tasa de errores.

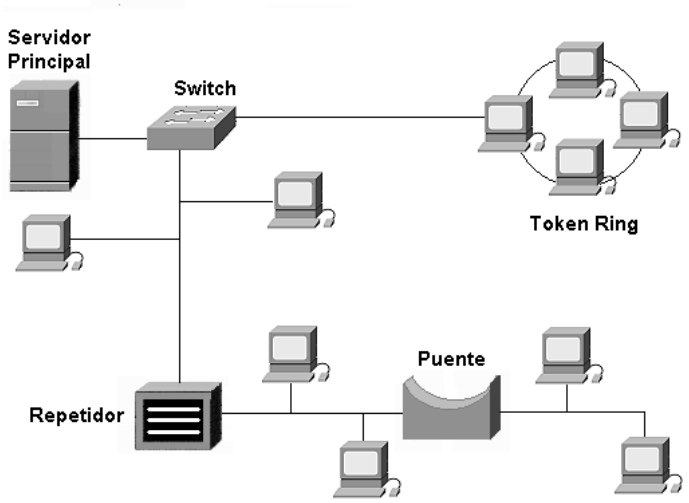


Figura 1.1 Red de área local (LAN)

- **Redes Ethernet.**

  Ethernet, al que también se conoce como IEEE 802.3, es actualmente el estándar más popular para redes LAN. El estándar 802.3 emplea una topología de estrella o de bus. Ethernet permite transmitir datos a través de la red a una velocidad de 10 Mbps, usa un método de transmisión de datos conocido como Acceso Múltiple con Detección de Portadora y Detección de Colisiones (CSMA/CD). Antes de que un nodo envíe algún dato a través de una red Ethernet, primero escucha y se da cuenta si algún otro nodo está transmitiendo información. De no ser así, el nodo transmitirá la información a través de la red. Todos los otros nodos escucharán y el nodo seleccionado recibirá la información. En caso de que dos nodos traten de enviar datos por la red al mismo tiempo, cada nodo se dará cuenta de la colisión y esperará una cantidad de tiempo aleatoria antes de volver a hacer el envío. Aunque CSMA/CD es una forma rápida y eficiente para transmitir datos, una red muy cargada podría llegar al punto de saturación. Sin embargo, con una red diseñada adecuadamente, la saturación rara vez

es preocupante. Existen varios estándares de Ethernet, 10BASE5 (cable coaxial grueso), 10BASE2 (cable coaxial delgado), 10BASE-T (cable UTP) y 10BASEF (fibra óptica) entre otros, que definen las especificaciones de longitud y la topología que debe utilizarse para conectar nodos en la red.

- **Redes Token Ring.**

  Token Ring, también llamado IEEE 802.5, fue ideado por IBM y algunos otros fabricantes. Con operación a una velocidad de 4 Mbps o 16 Mbps, Token Ring emplea una topología física en estrella. La NIC de cada computadora se conecta a un cable que, a su vez, se conecta a un hub central llamado unidad de acceso a multiestaciones (MAU). Token Ring se basa en un esquema de paso de señales (token passing), es decir que pasa un token (o señal) a todas las computadoras de la red. La computadora que esté en posesión del token tiene autorización para transmitir su información a otra computadora de la red. Cuando termina, el token pasa a la siguiente computadora del anillo lógico. Si la siguiente computadora tiene que enviar información, acepta el token y procede a enviarla. En caso contrario, el token pasa a la siguiente computadora del anillo y el proceso continúa. La MAU se salta automáticamente un nodo de red que no esté encendido. Sin embargo, dado que cada nodo de una red Token Ring examina y luego retransmite cada token (señal), un nodo con mal funcionamiento puede hacer que deje de trabajar toda la red. Token Ring tiende a ser menos eficiente que CSMA/CD (de Ethernet) en redes con poca actividad, pues requiere una sobrecarga adicional. Sin embargo, conforme aumenta la actividad de la red, Token Ring llega a ser más eficiente que CSMA/CD.

- **Nuevas tecnologías.**

  Existen varias tecnologías nuevas que satisfacen las necesidades de las redes actuales, incluyendo a Fast Ethernet, FDDI, Frame Relay y ATM.

  Fast Ethernet, llamado también 100BASEX, es una extensión del estándar Ethernet que opera a velocidades de 100 Mbps, un incremento 10 veces mayor que el Ethernet estándar de 10 Mbps.

  La interfaz de distribución de datos por fibra óptica (FDDI) es un estándar para la transferencia de datos por cable de fibra óptica. El estándar ANSI X3T9.5 para FDDI especifica una velocidad de 100 Mbps. Dado que el cable de fibra óptica no es susceptible a la interferencia eléctrica o tan susceptible a la degradación de la señal de red como sucede con los cables de cobre, FDDI permite el empleo de cables mucho más largos que otros estándares de red.

  El Frame Relay (retransmisión de tramas) es un servicio para mover datos de un nodo a otro a una velocidad razonable y bajo costo. El Frame Relay puede verse como una línea virtual rentada. El usuario renta un circuito virtual permanente entre dos puntos y entonces puede enviar tramas o

frames (es decir, paquetes) de hasta 1600 bytes entre ellos. Además de competir con las líneas rentadas, el Frame Relay compite con los circuitos virtuales permanentes de X.25.

ATM, que significa modo de transferencia asíncrona, es un conjunto de estándares internacionales para la transferencia de datos, voz y video por medio de una red a muy altas velocidades. Puesto que opera a velocidades que van desde 1.5 Mbps hasta 1.5 Gbps, ATM incorpora parte de los estándares Ethernet, Token Ring y FDDI para la transferencia de datos.

- **MAN** (Metropolitan Area Network): Las redes de área metropolitana cubren extensiones mayores como pueden ser ciudades (Figura 1.2).

  Mediante la interconexión de las redes LAN, se distribuye la información a diferentes puntos. Bibliotecas, universidades u organismos oficiales suelen interconectarse mediante este tipo de redes.

  Teóricamente, una MAN es de mayor velocidad que una LAN, pero ha habido una división o clasificación: privadas que son implementadas en Áreas tipo campus debido a la facilidad de instalación de Fibra Óptica y públicas de baja velocidad (< 2Mbps).

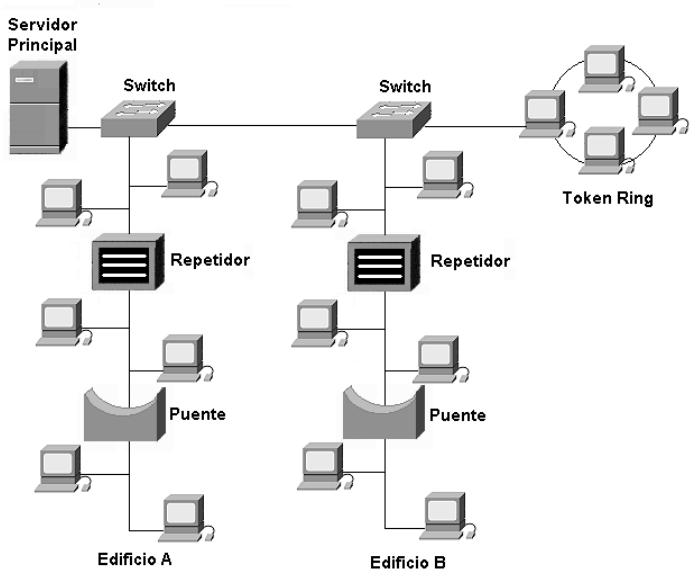


Figura 1.2 Red de área metropolitana

- **WAN** (Wide Area Network): Redes de Cobertura Amplia (WAN) son redes que cubren una amplia región geográfica, a menudo un país o un continente (Figura 1.3). Este tipo de redes contiene máquinas que ejecutan programas de usuario llamadas hosts o sistemas finales (end system). Los sistemas finales están conectados a una subred de comunicaciones. La función de la subred es transportar los mensajes de un host a otro. En este caso los aspectos de la comunicación pura (la subred) están separados de los aspectos de la aplicación (los host), lo cual simplifica el diseño.

En la mayoría de las redes de amplia cobertura se pueden distinguir dos componentes: las líneas de transmisión y los elementos de intercambio de paquetes (conmutadores). Las líneas de transmisión se conocen como circuitos, canales o troncales. Los elementos de intercambio son computadoras especializadas utilizadas para conectar dos o más líneas de transmisión. Las redes de área local están diseñadas de tal forma que tienen topologías simétricas, mientras que las redes de amplia cobertura tienen topología irregular. Otra forma de lograr una red de amplia cobertura es a través de satélites o sistemas de radio.

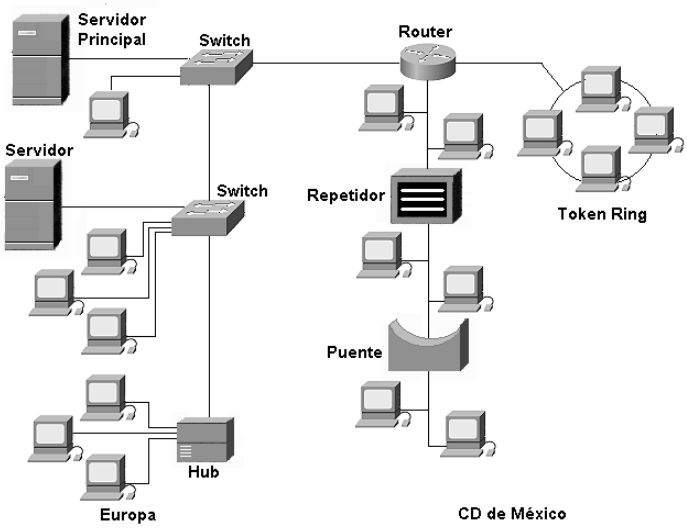


Figura 1.3 Red de área extensa (WAN)

- **INTERNET**: No es del todo una red, sino un inmenso conjunto de redes diferentes que tienen protocolos y servicios comunes (Figura 1.4). Es un sistema poco común por que nadie lo planeó y nadie lo controla.

  La Internet es el nombre de un grupo de recursos de información mundial, éstos, son tan amplios que están más allá de lo que podamos imaginar. Seria un error considerar la Internet sólo como una red o grupo de redes de computadoras conectadas unas con otras. Desde nuestro punto de vista, estas redes, son simplemente el medio que transporta la información. Lo maravilloso y útil de la Internet tiene que ver con la información misma.

- **INTRANET:** La diferencia principal entre los términos "Internet" e "Intranet" es que Internet se emplea para una conexión hacia el exterior de la empresa, mientras que Intranet hace referencia a una conexión dentro de la empresa.

  Una Intranet corporativa no se limita a las conexiones situadas en un lugar específico, sino que puede incluir todas las sucursales de una multinacional, incluso, puede tener una conexión a Internet, permitiendo que algunos o todos los usuarios naveguen a través de un firewall (cortafuegos de seguridad), utilizando un servidor "proxy". También se puede permitir a usuarios externos el acceso a una parte o a toda la Intranet.

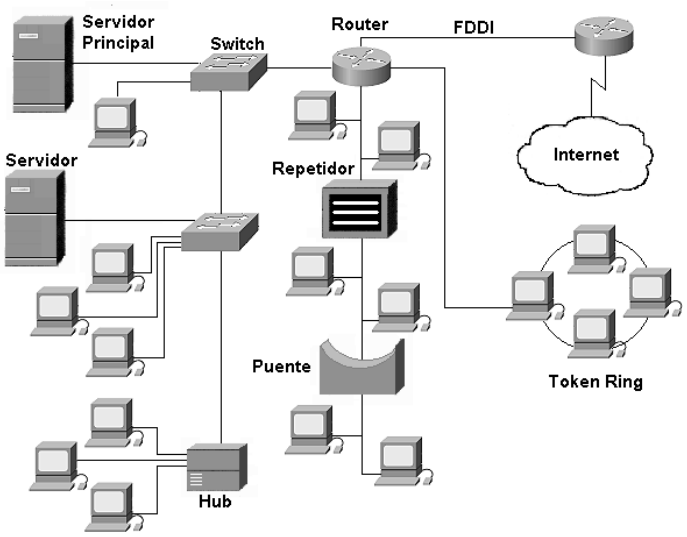


Figura 1.4 Internet

Las intranets utilizan la misma tecnología que Internet para ayudar a todos los miembros de una compañía a comunicarse entre ellos de forma rápida y eficaz. En su forma más simple, una intranet es sólo la red ya existente de una compañía a la cual se añade un software que permite tratar documentos HTML.

Con el mismo software gráfico desarrollado para crear Internet, una intranet proporciona fácil acceso a todo tipo de información localizada en cualquier ordenador conectado a esa red.
Una computadora central, servidor de red de la compañía, maneja todo el tráfico de datos asociado con la transmisión y recepción de archivos. Estos archivos pueden estar en código HTML para ser visualizados mediante el navegador, o ser archivos de datos utilizados por otro programa o bien una combinación de ambos.

Un programa llamado servidor web dice a la computadora central cómo manejar las solicitudes y las transmisiones de forma que cualquier computadora pueda comunicarse en una intranet independientemente del sistema operativo o del tipo de ordenador que sea.

Al empezar a utilizar un navegador, éste manda una solicitud al servidor web. Esta solicitud le pide al servidor que mande de vuelta un archivo al navegador, el cual a su vez se lo muestra al usuario.

Generalmente la primera página mostrada suele ser la página de presentación con información básica de un departamento o de la compañía y está vinculada a otras páginas de la intranet.

1.2 ELEMENTOS DE UNA RED.

Las redes de computadoras se montan con una serie de componentes de uso común y que en mayor o menor medida siempre aparecerán en cualquier instalación. Dichos

componentes se describen a continuación.

- **Protocolo:** Es un conjunto de reglas que definen cómo interactúan las entidades de comunicación, su fin, es proporcionar un servicio. Por ejemplo, HTTP posibilita la descarga de páginas Web. Otros ejemplos son: el protocolo de transferencia de archivos FTP (File Transfer Protocol); El protocolo sencillo para la transferencia de correo SMTP (Simple Mail Transfer Protocol), para el servicio de e-mail; el protocolo de Internet IP (Internet Protocol), para la transferencia de paquetes; el sistemas de nombres de dominio DNS (Domain Name System).

- **Medios de transmisión:** Por medio de transmisión se entiende el soporte físico utilizado para el envío de datos por la red. Son la espina dorsal de la red, por ellos se transmite la información entre los distintos nodos. La mayor parte de las redes existentes en la actualidad utilizan como medio de transmisión cable coaxial, cable par trenzado y fibra óptica. También se utilizan medios inalámbricos como ondas de radio, microondas o infrarrojos, estos son más lentos que los cables o la fibra óptica. Para efectuar la transmisión de la información se utilizan varias técnicas, pero las más comunes son: la banda base y la banda ancha.

  - **Ancho de Banda:** Es la cantidad de información, normalmente expresada en bits por segundo, que puede transmitirse en una conexión durante la unidad de tiempo elegida. También es el rango de frecuencias asignadas a un canal de transmisión, el ancho de banda es una propiedad física del medio y por lo general depende de la construcción , grosor y longitud de este.

    El ancho de banda se calcula restando la frecuencia mas baja de la señal de la frecuencia más alta que aparezca en la misma, por ejemplo, si tenemos un canal telefónico que ocupa una banda que va desde 300 hasta 3300 Hz. Al restar la frecuencia inferior de la superior, obtenemos un ancho de banda de 3000 Hz, o 3 Khz.

  - **Banda Base.**

    Técnica de Banda Base. La banda base es el tipo de transmisión más común dentro de las redes locales. Transmite las señales sin modular y está especialmente indicada para distancias cortas. El canal que trabaja en banda base utiliza todo el ancho de banda, por lo cual solo se puede transmitir una señal simultáneamente. Los medios de transmisión que se pueden utilizar son: cable de par trenzado y cable coaxial de banda base.

    Transmisión de banda base. En este tipo de transmisión se utilizan señales digitales sin necesidad de MODEM. Los usuarios pueden compartir el cable mediante técnicas de multiplexado de tiempo; un usuario utiliza toda la banda pasante del cable durante su tiempo de utilización. Un mismo cable no permite la transmisión de datos , voz y video al mismo tiempo.
  - **Banda Ancha.**

    Técnica de Banda Ancha. Consiste en modular la señal sobre ondas portadoras que pueden compartir el ancho de banda del medio de transmisión

mediante multiplexación por división de frecuencia. Es imprescindible la utilización de un MODEM para modular y demodular la información. Se logran distancias considerables, permitiendo usar, además, los elementos de conexión de la red para transmitir otras señales distintas a las de la propia red, como pueden ser señales de televisión o señales de voz. Los medios de transmisión que se pueden utilizar son: el cable coaxial de banda ancha y el cable de fibra óptica.

Transmisión de banda ancha. En este tipo de transmisión se utilizan módems de radiofrecuencia para generar las señales analógicas de varias frecuencias que son las que recorren la red.

La banda pasante del cable se divide en una serie de rangos de frecuencias o canales y de esta forma se pueden emitir simultáneamente varias señales en el mismo cable y en sentidos diferentes. Además los usuarios pueden compartir un mismo canal basándose en intervalos de tiempo determinados. Un mismo cable permite la transmisión simultanea de datos voz y video.

- **Interfaces de red:** La tarjeta de red (Network Interfase Card) es la que conecta físicamente la computadora a la red. Son tarjetas que se colocan dentro de la computadora. Puesto que todos los accesos a red se realizan a través de ellas se deben utilizar tarjetas rápidas si queremos comunicaciones fluidas.

- **Sistemas operativos de red:** Una colección de computadoras unidas por un medio de comunicación por sí sola no constituye un fin último, por lo tanto resulta necesario que esas computadoras y ese medio estén gobernados por un sistema operativo, el objetivo de dicho sistema operativo es ofrecer al menos los mismos servicios que nos ofrecen los sistemas operativos centralizados, los cuales operan en una sola computadora. Una red de computadoras puede tener dos clases de sistemas operativos:

  - Sistemas Operativos de Red
  - Sistemas Operativos Distribuidos

  En un sistema operativo de red los usuarios están conscientes de la existencia de múltiples computadoras y pueden ingresar en máquinas remotas y copiar archivos de una máquina a otra. Cada máquina ejecuta su propio sistema operativo local y tiene su propio usuario o usuarios locales.

  Los sistemas operativos de red no son fundamentalmente distintos de aquellos para un solo procesador. Obviamente, estos sistemas necesitan un controlador de la interfaz con la red y software de bajo nivel para operarlo, así como programas para realizar inicios de sesión remotos y acceso a archivos remotos, pero estas adiciones no alteran la estructura esencial del sistema operativo.

  Un sistema operativo distribuido, en cambio, presenta el mismo aspecto a los usuarios que un sistema tradicional de un solo procesador, aunque en realidad se compone de múltiples procesadores. Los usuarios no deben enterarse de dónde

se están ejecutando sus programas o almacenando sus archivos; de todo eso debe encargase el sistema operativo automática y eficientemente.

Los verdaderos sistemas operativos distribuidos requieren más que la adición de un poco más de código a un sistema operativo uniprocesador, por que los sistemas distribuidos y centralizados difieren en aspectos cruciales. Los sistemas distribuidos, por ejemplo, a menudo permiten a las aplicaciones ejecutarse en varios procesadores al mismo tiempo, por lo que requieren algoritmos de planificación de procesador más complejos.

- **Servidor de red:** Son computadoras de gran capacidad que permiten a cada una de las computadoras conectadas a la red el acceso a sus recursos. Estos servidores pueden ser de varios tipos:

  - Un servidor de archivos mantiene los archivos en subdirectorios privados y compartidos para los usuarios de red.
  - Un servidor de impresión tiene conectadas una o más impresoras que comparte con los demás usuarios.
  - Un servidor de comunicaciones permite enlazar diferentes redes.

- **Concentrador o Hub:** Es un elemento que provee una conexión central para todos los cables de la red. Los hubs son dispositivos con un número determinado de conectores, habitualmente RJ45 más otro conector adicional de tipo diferente para enlazar con otro tipo de red. Los hay de tipo inteligente que envían la información sólo a quien ha de llegar, mientras que, los normales envían la información a todos los puntos de la red siendo las estaciones de trabajo las que decidirán si se quedan o no con esa información. Están provistos de salidas especiales para conectar otro hub a uno de los puertos permitiendo así ampliaciones de la red.

- **Switch:** Es un dispositivo de propósito específico diseñado para resolver problemas de rendimiento en la red debido a anchos de banda pequeños y embotellamientos.

  Los switches toman decisiones basándose en las direcciones MAC por lo que puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto (Figura 1.5).

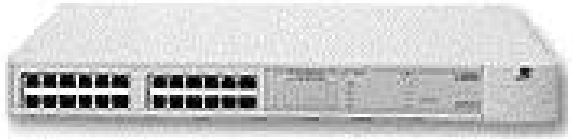


Figura 1.5 Switch

- **Ruteador:** Un ruteador es un dispositivo de propósito general diseñado para segmentar la red, con la idea de limitar tráfico de broadcast y proporcionar seguridad, control y redundancia entre dominios individuales de broadcast, también pueden dar servicio de firewall y un acceso económico a una WAN (Figura 1.6).

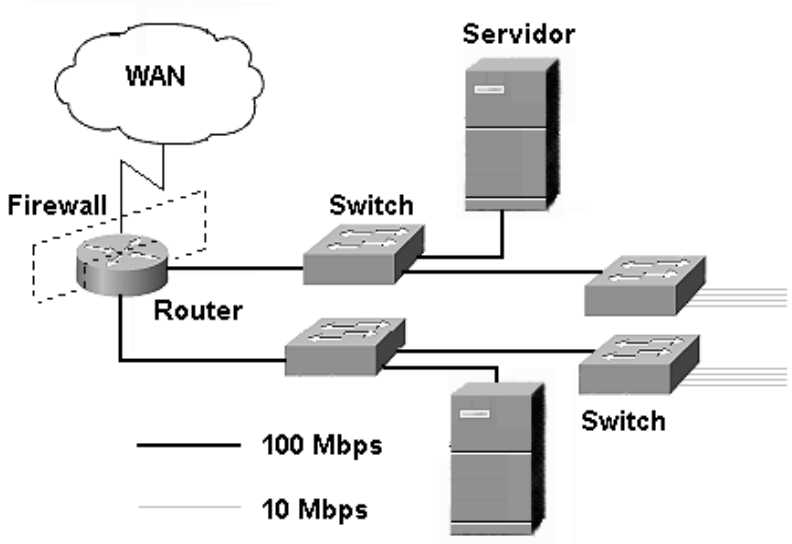


Figura 1.6 Ruteador utilizado como Firewall

1.3 TOPOLOGIAS DE RED.

Las estaciones de trabajo de una red se comunican entre sí mediante una conexión física, y el objeto de estas topologías es buscar la forma más económica y eficaz de conectarlas para, al mismo tiempo, facilitar la fiabilidad del sistema, evitar los tiempos de espera en la transmisión de los datos, conseguir un mejor control de la red y permitir de forma eficiente el aumento de las estaciones de trabajo.

1.3.1 Topología Física de bus.

Una topología de bus usa un cable largo llamado backbone, cables cortos llamados drop conectados al backbone usando conectores tipo T (Figura 1.7). El término de bus es usado en electrónica, tiene que ver con el transporte (bussing) de señales desde un punto a otro. El cable backbone necesita en los extremos elementos que le indiquen el inicio y el fin de la red, y que eviten que la señal siga buscando más dispositivo, estos elementos se llaman terminadores y se conectan a un punto de tierra. En la topología bus se permite que la señal viaje en diferentes direcciones.

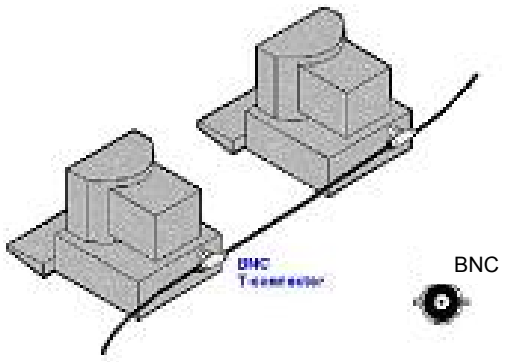


Figura 1.7 Topología de Bus

1.3.2 Topología Física de estrella.

La topología de estrella usa un concentrador central con cables extendiéndose en todas direcciones (Figura 1.8). Cada computadora es conectada a este concentrador a través de una conexión punto a punto. En la topología estrella, las señales viajan desde la computadora conectada por cable hasta el concentrador. Desde ahí la señal es enviada a los demás elementos de la red.

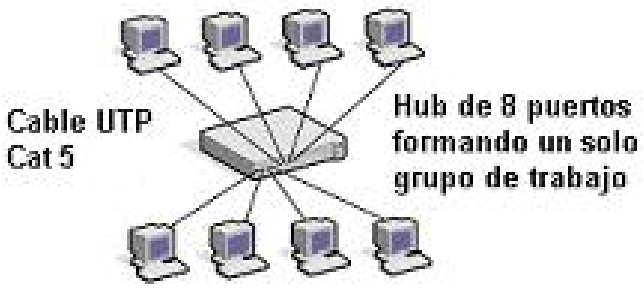


Figura 1.8 Topología de estrella.

1.3.3 Topología Física de anillo.

Una topología anillo es igual a un círculo (un enlace cerrado entre puntos). Cada elemento de la red se conecta al anillo a través de un dispositivo similar a un concentrador (Figura 1.9). Como existe un solo canal, si este falla, sucede lo mismo con toda la red, por lo que es casi imposible aislar la fallas.

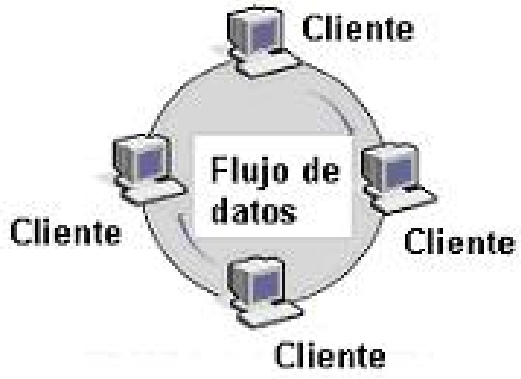


Figura 1.9 Topología de anillo

1.3.4 Topologías Lógicas.

Todas las topologías mencionadas anteriormente son llamadas también topologías físicas porque describen como está instalado el cableado; pero también cada red designa una topología lógica que describe la red desde la perspectiva de las señales que viajan a través de ella.

Un diseño de red puede tener distinta topología física y lógica (es decir, la forma en que esté cableada una red no tiene porque reflejar necesariamente la forma en que viajan las

señales a través de ella).

En la Figura 1.10 se muestra una disposición física de una configuración en estrella. Cada estación envía y recibe señales por el mismo cable. En el concentrador (hub) se mezclan las señales de todas las estaciones y son transmitidas a todas ellas (es decir, actúa igual que si estuviera en una configuración en bus). Por lo tanto, es una topología física de estrella que funciona como una topología lógica de bus.

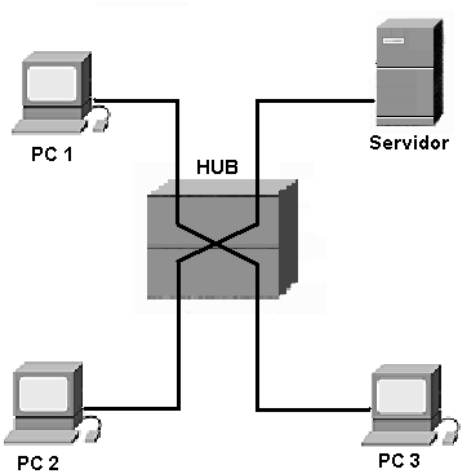


Figura 1.10 Topología lógica de bus y física de estrella

Muchas redes utilizan este modelo ya que es fácil de modificar la situación de cada estación (sólo hay que desconectar un cable) sin perjuicio para la red entera y además, incrementa las posibilidades de detección de problemas en la red.

1.4 MODELOS DE REFERENCIA.

Aunque los protocolos asociados con el modelo OSI ya casi no se usan, el modelo en sí es muy general y aun es válido, y las características tratadas en cada capa son muy importantes. El modelo TCP/IP tiene las propiedades opuestas, es decir, el modelo en si no se utiliza mucho pero los protocolos si; por estas razones analizaremos ambos modelos.

1.4.1 Modelo OSI (Open System Interconnection).

El modelo de Interconexión de Sistemas Abiertos (cuyas siglas en ingles son: OSI) es un estándar basado en siete capas (Figura 1.11). Cada una de ellas con una funcionalidad específica, para permitir la interconexión e interoperatividad de sistemas heterogéneos.
Los objetivos del modelo OSI son:

- Definir un conjunto de recomendaciones que permiten cooperar a sistemas abiertos
- Eliminar los impedimentos técnicos para la comunicación entre sistemas.
- Eliminar la necesidad de describir las operaciones internas de los sistemas.

- Definir los puntos de interconexión para el intercambio de información entre sistemas.
- Aumentar la capacidad de comunicación sin necesidad de hacer caras conversiones y transformaciones entre productos.
- Proporcionar un punto de partida razonable en el caso de que los estándares no cubran todas las necesidades.
- No implica ninguna implantación de tecnología en particular.

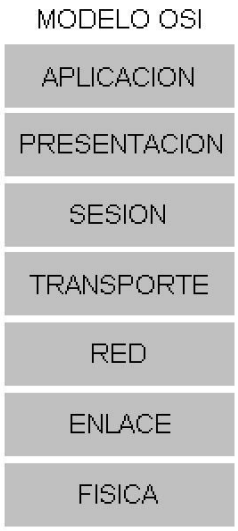


Figura 1.11 Capas del modelo OSI

1.4.1.1 Capa física.

Proporciona los medios mecánicos, eléctricos, funcionales y de procedimiento para activar, mantener y desactivar las conexiones físicas para la transmisión de bits entre entidades de enlace de datos (es decir entre el ETD y el ETCD, Equipo Terminal de Datos y Equipo Terminal de Circuito de datos).

Los medios mecánicos definen el tipo de conector, sus dimensiones físicas, la distribución de pines, etc. Los eléctricos, establecen las características eléctricas, tales como voltaje, impedancia, etc. Los medios funcionales, definen el significado de los niveles de tensión en cada pin del conector. Y los de procedimiento definen las reglas aplicables a ciertas funciones y las secuencias en que estas deben de ocurrir.

Su misión básica consiste en transmitir bits por un canal de comunicación, de manera tal que cuanto envíe el transmisor llegue sin alteración al receptor. Por ejemplo, algunas de las normas dentro de esta capa son RS-232 y V.24.

1.4.1.2 Capa de enlace de datos.

Tiene como objetivo facilitar los medios funcionales y de procedimiento para establecer, mantener y liberar conexiones de enlace de datos entre entidades de red y para transferir unidades de datos del servicio de enlace de datos.

Sus funciones básicas están orientadas a resolver los problemas planteados por falta de fiabilidad de los circuitos de datos, siendo estas funciones: la sincronización y entramado, conexión y desconexión del enlace, control de flujo así como detección y recuperación de errores.

Dentro de este nivel se encuadra el protocolo HDLC (3309), el procedimiento LAP B (7776) y las normas IEEE 802.2-7 para LAN.

1.4.1.3 Capa de red.

Proporciona los medios para establecer, mantener y liberar la conexión a través de una red donde existe una malla compuesta de enlaces y nodos, entre sistemas abiertos que contienen entidades de aplicación en comunicación, así como los medios funcionales y de procedimiento para el intercambio de unidades de datos del servicio de red entre entidades de transporte por conexiones de red.

Es la capa responsable de las funciones de conmutación y encaminamiento de la información; proporciona los procedimientos precisos y necesarios para el intercambio de datos entre el origen y el destino, por lo que es necesario que conozca la topología de la red, con el objeto de determinar la ruta más adecuada. Cuando los extremos están en rutas distintas, la capa de red deberá resolver las diferencias entre las redes, a fin de prestar su servicio a la capa de transporte.

El diseño de esta capa debe considerar a los servicios independientes de la tecnología empleada, que la capa de transporte debe ser indiferente al número, tipo y topología de las redes utilizadas, así como la numeración de la red debe ser uniforme a través de LAN's y WAN's. La especificación X.25 se incluye en este nivel.

1.4.1.4 Capa de transporte.

Efectúa la transferencia de datos entre entidades de sesión y las libera de toda otra función relativa a conseguir una transferencia de datos segura y económica.

Su misión básica es la de optimizar los servicios de la capa de red y corregir las posibles deficiencias en la calidad del servicio, con el auxilio de mecanismos de recuperación para condiciones anormales en las capas inferiores. Proporciona los procedimientos de transporte precisos, con independencia de la red o soporte físico empleado.

Está muy relacionado con la calidad del servicio ofrecido por la red, ya que si no es suficiente, es esta capa la que se encarga de establecer el puente entre las carencias de la red y las necesidades del usuario. Las recomendaciones X.214 y X.224 se encuentran en esta capa.

1.4.1.5 Capa de sesión.

Tiene por objeto proporcionar el medio necesario para que las entidades de presentación en cooperación organicen y sincronicen su diálogo y procedan al intercambio de datos. Para ello, esta capa proporciona los servicios precisos para establecer una conexión de

sesión entre dos entidades de presentación y facilitar interacciones ordenadas de intercambio de datos; estos servicios son:

- Establecimiento de la conexión a petición del usuario
- Liberación de la conexión cuando la transferencia de datos termina
- Intercambio de datos en ambos sentidos
- Sincronización
- Mantenimiento de la sesión para proporcionar un intercambio ordenado de datos entre las entidades de presentación.

Su función básica consiste en realizar el encuadrado de la dirección de sesión hacia el usuario con las direcciones de transporte orientadas a la red y gestionar y sincronizar los datos intercambiados entre los usuarios de una sesión, así como informar sobre incidencias. En la capa de sesión se encuentran las recomendaciones X.215 y X.225.

1.4.1.6 Capa de presentación.

Permite la representación de la información que las entidades de aplicación comunican o mencionan en su comunicación. Es la responsable de que la información se entregue al proceso de aplicación de manera que pueda ser entendida y utilizada. La función de esta capa es proporcionar los procedimientos precisos, incluyendo aspectos de conversión, cifrado y compresión de datos, para representar la información de acuerdo a los dispositivos de presentación del usuario (pantallas, impresoras, etc.) y posibilitar un transporte seguro, fiable y económico entre dos puntos de la red, una vez que las capas anteriores han resuelto el problema de la transmisión de datos y el establecimiento de la sesión de trabajo.
A través de esta capa, los procesos de aplicación adquieren independencia de la representación de los datos, incluyendo en su entorno las posibles transformaciones de códigos y la selección de sintaxis. En este nivel se encuentran normas para videotex, teletex, y telefax y las X.225

1.4.1.7 Capa de aplicación.

La función de esta capa es proporcionar los procedimientos precisos que permitan a los usuarios ejecutar los comandos relativos a sus propias aplicaciones. Los procesos de las aplicaciones se comunican entre sí por medio de las entidades de aplicación asociadas, controladas por protocolos de aplicación y utilizando los servicios de la capa de presentación. La transferencia de archivos y el acceso remoto a archivos son, probablemente, las aplicaciones más comunes de este nivel. Dos normas de esta capa son la X.400 (correo electrónico) y X.500 (directorio).

1.4.2 Modelo TCP/IP (Transport Control Protocol / Internet Protocol).

Aunque poca gente sabe lo que es TCP/IP todos lo emplean indirectamente y lo confunden con un solo protocolo cuando en realidad son varios, de entre los cuales destaca y es el mas importante el protocolo IP.

En 1973, la DARPA (Agencia de Proyectos de Investigaciones Avanzadas para la Defensa de los EU, por sus siglas en inglés) inició un programa de investigación de

tecnologías de comunicación entre redes de diferentes características. El proyecto se basaba en la transmisión de paquetes de información, y tenia por objetivo la interconexión de redes. De este proyecto surgieron dos redes: Una de investigación, ARPANET, y una de uso exclusivamente militar, MILNET.

Para comunicar las redes, se desarrollaron varios protocolos: El protocolo de Internet y los protocolos de control de transmisión. Posteriormente estos protocolos se englobaron en el conjunto de protocolos TCP/IP.

En 1980, se incluyo en el UNIX 4.2 de BERKELEY, y fue el protocolo militar estándar en 1983. Con el nacimiento en 1983 de INTERNET, este protocolo se popularizó bastante, y su destino se unió al de Internet. ARPANET dejo de funcionar oficialmente en 1990.

Algunos de los motivos de su popularidad son:

- Independencia del fabricante
- Soporta múltiples tecnologías
- Puede funcionar en máquinas de cualquier tamaño
- Estándar de EEUU desde 1983

El modelo básico en Internet es el modelo Cliente / servidor. El Cliente es un programa que solicita a otro un servicio. El Servidor es el programa que proporciona este servicio.

La arquitectura de Internet esta basada en capas. Esto hace más fácil implementar nuevos protocolos. El conjunto de protocolos TCP/IP, al estar integrado plenamente en Internet, también dispone de este tipo de arquitectura. El modelo de capas de TCP/IP es algo diferente al propuesto por ISO (International Standard Organization) para la interconexión de sistemas abiertos (OSI) (Figura 1.12) .

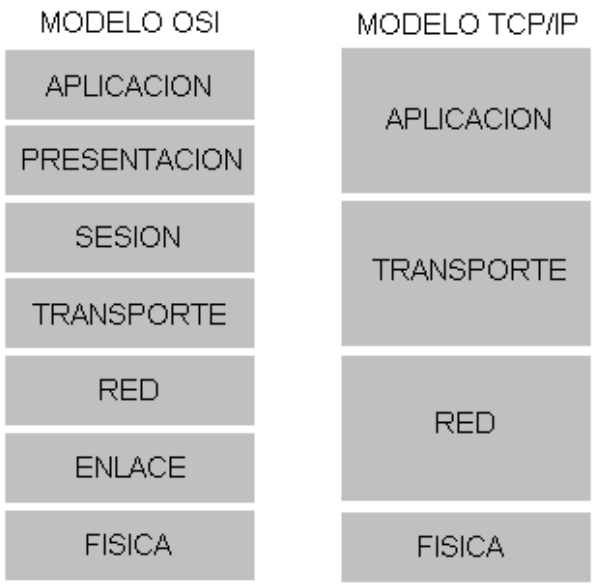


Figura 1.12 Relación de TCP/IP con el modelo OSI

La arquitectura de un sistema en TCP/IP tiene una serie de metas:

- La independencia de la tecnología usada en la conexión a bajo nivel y la arquitectura de la computadora.
- Conectividad universal a través de la red.
- Protocolos estandarizados.

1.4.2.1 Capa de aplicación.

Esta capa corresponde a las aplicaciones que están disponibles para los usuarios, como TELNET, FTP, SNMP. A continuación se mencionan algunos protocolos importantes de esta capa:

- **DNS (Domain Name Server).**

  La mayoría de la gente prefiere utilizar un nombre que sea más fácil de recordar que una dirección numérica. Para hacer esto, un servidor debe transformar el nombre en la dirección correcta. Esto se hacía originalmente en Internet mediante una tabla única situada en un servidor central, donde estaban contenidos todos los nombres de host. Esto era posible debido a que solo existían unos cientos de servidores, pero debido a un gran aumento del número de servidores, fue necesario descentralizar el servidor de nombres y dividirlo en múltiples DNS. Esto redujo el tiempo de respuesta del servidor, y disminuyó el tráfico en la red.

  La estructura del sistema de dominios es similar a la estructura de directorios del DOS o del UNIX. Es decir, es una estructura en forma de árbol, y los archivos están identificados con una ruta de acceso. La diferencia es que en el DNS la ruta empieza con el nombre del nodo en vez del directorio raíz. Además, las rutas en un servidor DNS se escriben en sentido inverso a las del DOS.

  Desde el punto de vista de un programa el funcionamiento de este servicio en muy simple. El programa proporciona un nombre de dominio, y el DNS le devuelve su dirección IP.

  El programa de usuario proporciona el nombre de dominio como una secuencia de palabras. Las palabras están listadas de izquierda a derecha, y la que representa la zona más cercana al usuario es la primera.

  Los programas DNS manipulan el nombre del dominio proporcionado por el usuario de manera que sea fácilmente interpretado por otros programas.

  DNS es un protocolo de la capa de aplicación y esta clasificado como una utilidad por convenio entre los usuarios y el administrador del sistema, en vez de una parte integrada en los servicios de usuario.

  Siguiendo el modelo Cliente / servidor, DNS consiste en un usuario, un cliente, un servidor de nombres local y un servidor de nombres remoto. En términos de las especificaciones, DNS consiste en un programa de usuario, un cliente, un servidor de nombres, y un servidor de nombres remoto. Cada host debe implementar un

mecanismo utilizando el cliente DNS para convertir nombres de host en direcciones IP.

Un nodo DNS se representa por una etiqueta en el interior del nombre de dominio, y todos los nodos tienen unos archivos de recursos (resource records *(RRs)*) que contienen información que habilita el programa DNS para encontrar el nombre de dominio solicitado.

- **SNMP (Simple Network Management Protocol).**

  El protocolo SNMP se utiliza para administrar múltiples redes físicas de diferentes fabricantes, es decir Internet, donde no existe un protocolo común en la capa de Enlace. La estructura de este protocolo se basa en utilizar la capa de aplicación para evitar el contacto con la capa de enlace

1.4.2.2 Capa de transporte.

Provee comunicación extremo a extremo desde un programa de aplicación a otro. Puede proveer un transporte confiable asegurándose de que los datos lleguen sin errores y en la secuencia correcta. Coordina a múltiples aplicaciones que se encuentren interactuando con la red simultáneamente de tal manera que los datos que envíe una aplicación sean recibidos correctamente por la aplicación remota. En esta capa se encuentran los protocolos UDP y TCP.

- **UDP (User Datagram Protocol).**

  El protocolo UDP proporciona aplicaciones con un tipo de servicio de paquetes orientado a transacciones. El UDP es simple, eficiente e ideal para aplicaciones como el TFTP y el DNS. Una dirección IP sirve para dirigir el paquete hacia una maquina en particular, y el numero de puerto de destino en la cabecera UDP se utiliza para dirigir el paquete UDP a un proceso especifico localizado en la cabecera IP.

  La cabecera UDP también contiene un numero de puerto origen que permite al proceso recibido conocer como responder al paquete de datos.

- **TCP (Transport Control Protocol).**

  El protocolo TCP proporciona un servicio de comunicación que forma un circuito, es decir, que el flujo de datos entre el origen y el destino parece que sea continuo. TCP proporciona un circuito virtual el cual es llamado conexión.

  Al contrario que los programas que utilizan UDP, los que utilizan el TCP tienen un servicio de conexión entre los programas llamados y los que llaman, chequeo de errores, control de flujo y capacidad de interrupción.

  Existen dos tipos de interfaces entre la conexión TCP y los otros programas. El primero es utilizar la pila de los programas de la capa de red. Como en esta capa solo esta el protocolo IP, la interfase la determina este protocolo. El segundo tipo

es la interfaz del programa de usuario. Esta interfaz puede variar según el sistema operativo, pero en general tiene las siguientes características.

La interfaz envuelve el programa de usuario llamando a una rutina que introduce entradas en una estructura de datos llamada bloque de control de transmisión (TCB). Las entradas se realizan inicialmente en la pila de hardware y transferidas al TCB por medio de una rutina de sistema. Estas entradas permiten al TCP asociar un usuario con una conexión particular, de modo que pueda aceptar comandos de un usuario y mandarlos a otro usuario en la otra parte de la conexión.

TCP utiliza identificadores únicos para cada parte de la conexión. Esto se utiliza para recordar la asociación entre dos usuarios. Al usuario se le asigna un nombre de conexión para utilizarlo en futuras entradas del TCB. Los identificadores para cada extremo de la conexión se llaman sockets. El socket local se construye concatenando la dirección IP de origen y el número de puerto de origen. El socket remoto se obtiene concatenando la dirección IP de destino y el número de puerto de destino.

El par de sockets de una conexión forman un único numero en Internet. El UDP tiene los mismos sockets, pero no los recuerda. A continuación se explican los comandos más usuales:

- ***Open*:** Inicia una conexión o comienza a escuchar un socket. El usuario tiene un nombre de conexión local que actúa como un puntero dentro del TCB.
- ***Send*:** El comando Send manda datos del buffer especificado.
- ***Receive*:** El comando Receive es un mensaje de error si el nombre local proporcionado no es utilizado antes con el comando Open.
- ***Close*:** El comando Close hace que se cierre una conexión. Se produce un error si la conexión especificada no ha sido abierta, o si no se tiene autorización para cerrar la conexión.
- ***Status*:** El comando Status solo tiene una variable asociada, que es el nombre de la conexión.
- ***Abort*:** El comando Abort hace que todos los comandos Send y Receive asociados al nombre de la conexión local se interrumpan. La entrada del usuario del TCB se elimina y se envía un mensaje especial de reinicio a la entidad del otro lado de la conexión.

El TCP recuerda el estado de cada conexión por medio del TCB. Cuando se abre una conexión, se efectúa una entrada única en el TCB. Un nombre de conexión se le asigna al usuario para activar los comandos de la conexión. Cuando se cierra una conexión se elimina su entrada del TCB.

1.4.2.3 Capa de red.

Controla la comunicación entre un equipo y otro. Conforma los paquetes IP que serán enviados por la capa inferior. Desencapsula los paquetes recibidos pasando a la capa superior la información dirigida a una aplicación.

- **IP(Internet Protocol)**

  El protocolo IP especifica que la unidad básica de transferencia de datos en el TCP/IP es el paquete. Los paquetes pueden ser retrasados, perdidos, duplicados, enviados en una secuencia incorrecta o fragmentados intencionalmente para permitir que un nodo con un buffer limitado pueda coger todo el paquete. Es la responsabilidad del protocolo IP reensamblar los fragmentos del paquete en el orden correcto. En algunas situaciones de error los paquetes son descartados sin mostrar ningún mensaje mientras que en otras situaciones los mensajes de error son recibidos por la maquina origen (esto lo hace el protocolo ICMP).

  El protocolo IP también define cual será la ruta inicial por la que serán mandados los datos. Cuando los paquetes viajan de unos equipos a otros, es posible que atraviesen diferentes tipos de redes. El tamaño máximo de estos paquetes de datos puede variar de una red a otra, dependiendo del medio físico que se emplee para su transmisión. A este tamaño máximo se le denomina MTU (Maximum Transmission Unit), y ninguna red puede transmitir un paquete de tamaño mayor a esta MTU.

  Las direcciones IP hacen que el envío de datos entre computadoras se haga de forma eficaz, de un modo similar al que utilizan los números de teléfono. Es un identificador único que diferencia una computadora de otra en la red y ayuda a localizar donde se encuentra. Una dirección IP es requerida para cada computadora y componente en la red.

  Las direcciones IP tienen 32 bits, formados por cuatro campos de 8 bits separados por puntos. Cada campo puede tener un valor comprendido entre 0 y 255. Una dirección tiene dos partes, el Host ID y Network ID.

  La primera parte de la dirección IP es el Network ID, el cual identifica el segmento de la red en la cual la computadora esta localizada, todas las computadoras en el segmento tienen el mismo Network ID.

  La segunda parte de la dirección IP es el Host ID, el cual identifica una computadora u otro dispositivo en el segmento, el Host ID para cada Host debe ser único en un Network ID.

  Existen varias clases de direcciones IP, y son usadas para asignar Networks ID. A una organización se le asigna un rango de direcciones IP, el cual es referido por las direcciones de Network ID y esta basado en el tamaño de la organización, por ejemplo, una organización con 200 Host se le asigna un Network ID de clase C mientras que a una organización con 20,000 Host se le asigna un Network ID de clase B.

  - La clase A contiene 7 bits para direcciones de red, con lo que permite tener hasta 128 redes, con 16,777,216 computadoras cada una. Las direcciones estarán comprendidas entre 0.0.0.0. y 127.255.255.255., y la mascara de subred será 255.0.0.0.

- La clase B contiene 14 bits para direcciones de red y 16 bits para direcciones de Hosts. El numero máximo de redes es 16,536 redes, con 65,536 computadoras por red. Las direcciones estarán comprendidas entre 128.0.0.0 y 191.255.255.255, y la mascara de subred será 255.255.0.0.

- La Universidad Nacional Autónoma de México se encuentra en esta clase, ya que cuenta con más de 38,000 computadoras, 350 servidores Internet, 100 redes internas LAN, 100 redes externas WAN; 1,950 kilómetros de fibra óptica, dentro de los diversos campus universitarios con direcciones IP como la siguiente: 132.248.10.1 ó servidor.unam.mx.[1]

  donde :

  - 132 mx dominio mundial México
  - 248 UNAM dominio nacional UNAM
  - 10 dominio regional Dirección General de Servicios de Cómputo Académico
  - 1 servidor nombre propio de la computadora.

- La clase C contiene 21 bits para direcciones de red y 8 para hosts, lo que permite tener un total de 2,097,142 redes, cada una de ellas con 256 computadoras. Las direcciones estarán comprendidas entre 192.0.0.0. y 223.255.255.255., y la mascara de subred será 255.255.255.0.

- La clase D se reserva todas las direcciones para multidestino (multicast), es decir, un ordenador transmite un mensaje a un grupo especifico de computadoras de esta clase. Las direcciones estarán comprendidas entre 224.0.0.0. y 239.255.255.255.

- La clase E se utiliza exclusivamente para fines experimentales. Las direcciones están comprendidas entre 240.0.0.0. y 247.255.255.255.

- **IPv6.**

  Esta es una nueva versión del protocolo IP, llamada IPv6, aunque también es conocida como IPng (Internet Protocol Next Generation). Es la versión 6, debido a que la numero 5 no paso de la fase experimental. La compatibilidad con la versión 4 es prácticamente total. Algunas de las modificaciones, están encaminadas a mejorar la seguridad en la red, que apenas existía en la versión 4.

  El motivo básico para crear un nuevo protocolo fue la falta de direcciones. IPv4 tiene un espacio de direcciones de 32 bits, en cambio IPv6 ofrece un espacio de 128 bits. El reducido espacio de direcciones de IPv4, junto al hecho de falta de coordinación para su asignación durante la década de los 80's, sin ningún tipo de optimización, dejando incluso espacios de direcciones discontinuos, generan en la actualidad, dificultades no previstas en aquel momento.

[1] Información obtenida de (http://www.dgsca.unam.mx/dtd/Telecom%20site%20folder/Pages/redunam.html).

Otro de los problemas de IPv4 es la gran dimensión de las tablas de ruteo en el backbone de Internet, que lo hace ineficaz y perjudica los tiempos de respuesta.

Debido a la multitud de nuevas aplicaciones en las que IPv4 es utilizado, ha sido necesario agregar nuevas funcionalidades al protocolo básico, aspectos que no fueron contemplados en el análisis inicial de IPv4, lo que genera complicaciones en su escalabilidad para nuevos requerimientos y en el uso simultáneo de dos o más de dichas funcionalidades. Entre las mas conocidas se pueden mencionar medidas para permitir la calidad de Servicio (QoS), Seguridad (IPsec) y movilidad.

Características principales de IPv6

- Mayor espacio de direcciones. El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar mas niveles de jerarquías de direccionamiento y mas nodos direccionables.

- Posibilidad de paquetes con carga útil (datos) de mas de 65,355 bytes contra 4096 bytes de IPv4.

- Capacidad de etiquetas de flujo. Puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo (flow) de tráfico particular, que requieren manejo especial por los routers IPv6, tal como calidad de servicio no por defecto o servicios de tiempo real. Por ejemplo video conferencia.

- Características de movilidad, la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad.

- **ICMP (Internet Control Message Protocol).**

  Internet es un sistema autónomo que no dispone de ningún control central. El protocolo ICMP, proporciona el medio para que el software de hosts y gateways intermedios se comuniquen. El protocolo ICMP tiene su propio número de protocolo (número 1), que lo habilita para utilizar el IP directamente. La implementación de ICMP es obligatoria como un subconjunto lógico del protocolo IP. Informa de los errores ocurridos en el procesamiento de los paquetes y genera algunos mensajes de administración y de estatus. Los mensajes de error de este protocolo los genera y procesa TCP/IP, y no el usuario.

- **ARP (Address Resolution Protocol)** El protocolo ARP, es el encargado de convertir las direcciones IP en direcciones de la red física.

  El funcionamiento del protocolo ARP es bastante simple. Cuando una máquina desea enviar un mensaje a otra máquina que está conectada a través de una red Ethernet se encuentra con un problema: la dirección IP de la máquina en cuestión es diferente a la dirección física de la misma. La máquina que quiere enviar el mensaje sólo conoce la dirección IP del destino, por lo que tendrá que encontrar un modo de traducir la dirección IP a la dirección física. Esto se hace con el protocolo ARP.

Este protocolo utiliza una tabla denominada Tabla de Direcciones ARP, que contiene la correspondencia entre direcciones IP y direcciones físicas utilizadas recientemente. Si la dirección solicitada se encuentra en esta tabla el proceso se termina en este punto, puesto que la máquina que origina el mensaje ya dispone de la dirección física de la máquina destino.

Si la dirección buscada no esta en la tabla el protocolo ARP envía un mensaje a toda la red. Cuando un ordenador reconoce su dirección IP envía un mensaje de respuesta que contiene la dirección física. Cuando la máquina origen recibe este mensaje ya puede establecer la comunicación con la máquina destino, y esta dirección física se guarda en la Tabla de direcciones ARP.

- **RARP (Rever Address Resolution Protocol)** Protocolo de Resolución de Dirección de Retorno. Es un Protocolo de bajo nivel que se encarga de la asignación de direcciones IP a maquinas simples desde un servidor en una red física.

  Este protocolo permite que una estación de trabajo recientemente inicializada transmita su dirección Ethernet y diga: mi dirección Ethernet de 48 bits es 14.04.05.18.01.25. "¿Alguien allá afuera conoce mi dirección IP?", el servidor RARP ve esta solicitud, busca la dirección Ethernet en sus archivos de configuración y devuelve la dirección IP correspondiente.

1.4.2.4 Capa física.

Es la responsable de poner datos en el medio físico de la red. Esta capa contiene dispositivos físicos tales como cables, adaptadores de red, etc. La capa contiene los protocolos como Ethernet y ATM, los cuales definen como los datos van a ser transmitidos sobre la red.

1.5 PALABRAS CLAVES

RED
BROADCAST
POINT TO POINT
LAN
REDES ETHERNET
TOKEN RING.
CSMA/CD.
MAN
INTERNET
INTRANET
PROTOCOLO
ANCHO DE BANDA
BANDA BASE
BANDA ANCHA
INTERFACES DE RED
SISTEMAS OPERATIVOS DE RED
SERVIDOR DE RED

CONCENTRADOR O HUB
SWITCH
RUTEADOR
TOPOLOGIAS DE RED
MODELO OSI (OPEN SYSTEM INTERCONNECTION)
TCP/IP

Elementos de conexión de

Capítulo

2

2 ELEMENTOS DE CONEXIÓN DE REDES

2.1 MEDIOS DE TRANSMISIÓN

Se entiende por medio de transmisión, el soporte físico utilizado para el envío de datos por la red. La mayor parte de las redes existentes en la actualidad utilizan como medio de transmisión cable coaxial, cable bifilar o par trenzado y cable de fibra óptica. También se utilizan medios inalámbricos como ondas de radio, microondas o infrarrojos, estos medios son más lentos que el cable o la fibra óptica.

Cualquier medio, que pueda transportar información en forma de señales electromagnéticas se puede utilizar en redes como medio de transmisión.

Los medios de transmisión son la espina dorsal de la red, por ellos se transmite la información entre los distintos nodos, como se vio en el capítulo 1, para efectuar la transmisión de la información se utilizan varias técnicas, pero las más comunes son: banda base y banda ancha.

2.1.1 Medios de transmisión guiados

Éstos medios transmiten una señal por un conducto físico. Los más comunes son: par trenzado, cable coaxial y fibra óptica.

- **Par trenzado**

  Es el medio guiado más barato y más usado. Consiste en un par de cables, cubiertos cada uno de plástico aislante y entrelazados, el uno con el otro, como se muestra en la Figura 2.1.

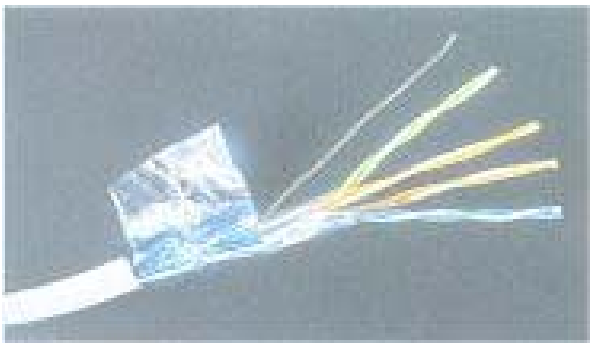


Figura 2.1 Par trenzado

Este tipo de medio es el más utilizado debido a su bajo costo pero su inconveniente principal es su poca velocidad de transmisión y su poco alcance.

Con este tipo de cable, se pueden transmitir señales analógicas o digitales. Es un medio muy susceptible a ruido y a interferencias. Para evitar estos problemas se suele trenzar el cable con distintos pasos de torsión y se suele recubrir con una malla externa para evitar las interferencias externas. La utilización del trenzado tiende a disminuir la interferencia electromagnética.

Dependiendo del número de trenzas por unidad de longitud, los cables de par trenzado se clasifican en categorías. A mayor número de trenzas, se obtiene una mayor velocidad de transferencia.

- Categoría 1 y 2, hasta 4 Mbps
- Categoría 3, hasta 10 Mbps
- Categoría 4, hasta 16 Mbps
- Categoría 5, hasta 100 Mbps
- Categoría 5-e, hasta 1 Gbps

Los cables par trenzado pueden ser a su vez de dos tipos:

- UTP (*Unshielded Twisted Pair*, par trenzado no blindado) Los cables UTP son los más utilizados debido a su bajo costo y facilidad de instalación.

- STP (*Shielded Twisted Pair*, par trenzado blindado). Los cables STP están cubiertos por una malla metálica que reduce las interferencias y mejora las características de la transmisión. Sin embargo, tienen un costo elevado y al ser más gruesos son más complicados de instalar. El cableado que se utiliza con más frecuencia en la actualidad es UTP Categoría 5-e.

- **Cable coaxial**

Consiste en un cable conductor interno separado de otro cable conductor externo por anillos aislantes o por un aislante macizo. Todo esto se recubre con otra capa aislante que es la funda del cable (Figura 2.2).

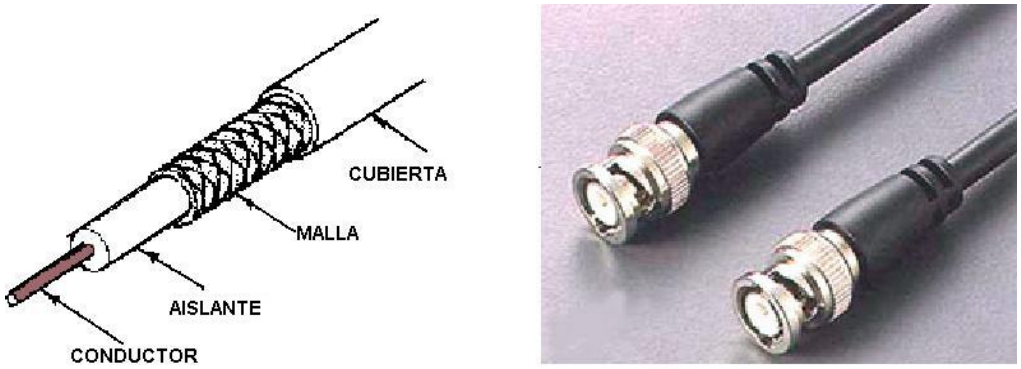


Figura 2.2 Cable coaxial

Este cable, aunque es más caro que el par trenzado, se puede utilizar a más larga distancia, con velocidades de transmisión superiores, menos interferencias y permite conectar más estaciones. Se utiliza para transmitir señales analógicas o digitales. Sus principales inconvenientes son:

- Atenuación, que se caracteriza por la pérdida de energía conforme la señal se propaga hacia su destino

- Ruido Térmico, que es el resultado del movimiento constante y aleatorio de electrones en el conductor; este representa un límite a la capacidad del canal provocando así la posible existencia de datos dañados.

- **Fibra óptica**

Es un filamento de vidrio sumamente delgado diseñado para la transmisión de la luz. Las fibras ópticas poseen enormes capacidades de transmisión, del orden de miles de bits por segundo. Además de que los impulsos luminosos no son afectados por interferencias causadas por el ambiente (Figura.2.3).

La ventaja de este medio de transmisión se basa en la frecuencia que tiene la luz, por lo que el ancho de banda es enorme, para un BIT con valor 1: un pulso de luz, para un BIT con valor 0: bastaría la ausencia de luz.

La velocidad de transmisión es muy alta, desde 45 Mbps hasta 9.6 Gbps en casos especiales. Se limitan por las conversiones entre las señales ópticas y eléctricas. Los pulsos de la luz rebotan dentro de la fibra. En una fibra de modo único (monomodo) los pulsos no pueden rebotar (el diámetro es demasiado pequeño) y se necesita menor amplificación. La longitud del cable viene limitada por las atenuaciones que recibe la señal con la distancia, pudiendo llegar a ser los segmentos de hasta 2 Km.

Su forma es cilíndrica con tres secciones radiales: núcleo, revestimiento y cubierta (Figura 2.3). El montaje de fibra óptica está compuesto por un emisor de luz, un detector y un medio transmisor. Su rango de frecuencias es todo el espectro visible y parte del infrarrojo.

Es un medio muy apropiado para largas distancias. Sus beneficios frente al cable coaxial y de par trenzado son que permite mayor ancho de banda, su tamaño y peso es menor, se produce un aislamiento electromagnético, la atenuación es menor y la separación entre los repetidores es mayor.

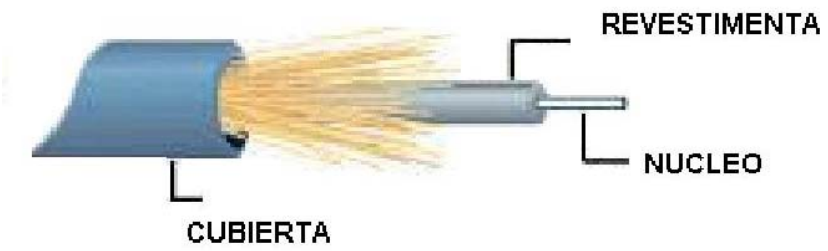


Figura 2.3 Estructura de la Fibra Óptica

Una de las desventajas es no poder empalmar fácilmente cables para conectarlos a nuevos nodos, además de que su instalación y mantenimiento tiene un costo elevado por lo que solamente son utilizados para redes con mucho tráfico.

2.1.2 Medios de transmisión no guiados

Entre los medios no guiados se encuentran:

- **Ondas de radio.**

  Son ondas omnidireccionales, es decir, se propagan en todas las direcciones. Son capaces de recorrer grandes distancias, incluso atravesando edificios. Su mayor problema es la interferencia entre usuarios.

- **Microondas terrestres.**

  Estas ondas viajan en línea recta, por lo que emisor y receptor deben estar alineados cuidadosamente. Suelen utilizarse antenas parabólicas como la que se muestra en la figura 2.4. Tienen dificultades para atravesar edificios. Debido a la propia curvatura de la tierra, la distancia entre dos repetidores no debe exceder de 80 Km de distancia. Es una forma económica para comunicar dos zonas geográficas mediante dos torres suficientemente altas para que sus extremos sean visibles. Al igual que otros medios no guiados también se ven afectadas por las condiciones atmosféricas y la atenuación aumenta con las lluvias. La interferencia es otro inconveniente de las microondas ya que al proliferar estos sistemas, puede haber solapamiento de señales.

Figura 2.4 Antena para Microondas

- **Microondas por satélite.**

  Los satélites son artefactos en órbitas geoestacionarias cuyo lanzamiento es científicamente calculado a fin de que siempre se halle cubriendo una misma porción de suelo terráqueo. La altitud promedio de un satélite es de 35,000 Km desde la superficie terrestre, con órbitas regulares de 24 horas en la mayoría de los casos al igual que nuestro planeta. Tienen capacidades para manipular de forma simultánea, de 250 a 40,000 comunicaciones.

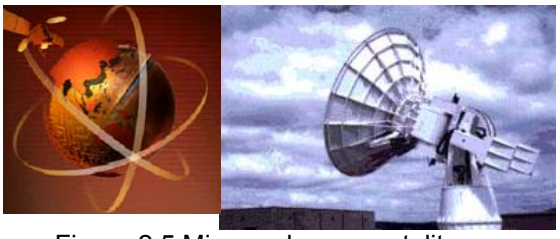


Figura 2.5 Microondas por satelite

El satélite recibe las señales y las amplifica o retransmite en la dirección adecuada, como se muestra en la figura 2.5. Para mantener la alineación del satélite con los receptores y emisores de la tierra, el satélite debe ser geoestacionario.

- **Infrarrojos.**

  Son ondas direccionales incapaces de atravesar objetos sólidos (paredes, por ejemplo) que están indicadas para transmisiones de corta distancia. Las tarjetas de red inalámbricas utilizadas en algunas redes locales emplean esta tecnología, resultan muy cómodas para computadoras portátiles; sin embargo, su velocidad es inferior a la conseguida mediante un cable par trenzado.

- **Ondas de luz.**

  Se usan rayos láser y son unidireccionales. Ofrecen un ancho de banda alto con costo bajo, pero el rayo es muy angosto y el alineamiento entre los receptores es difícil. Se pueden utilizar para comunicar dos edificios próximos instalando en cada uno de ellos un emisor láser y un foto detector.

2.2 INTERFACES DE RED (TARJETAS DE RED).

Una tarjeta de interfaz de red o Network Interfaz Card (NIC) es un dispositivo que se conecta a la computadora con el fin de ofrecer la conexión física a una red. Cada tarjeta se encuentra diseñada para trabajar en un tipo de red específico y soporta una gran variedad de cables y tipos de bus (ISA, EISA, PCI, PCMCIA y USB).

2.2.1 Direcciones MAC.

Una dirección MAC (Media Access Control) consiste en coordinar el acceso al canal de forma que la información vaya desde el origen hasta el destino a través de la misma red de difusión. Las direcciones físicas MAC se graban durante el proceso de fabricación del adaptador Ethernet y con el objeto de garantizar que no existan dos direcciones iguales, el IEEE asigna al fabricante del adaptador los primeros 24 bits de la dirección, siendo responsabilidad del fabricante la administración de los 24 bits restantes para formar la dirección completa de 48 bits.

2.2.2 Tipos de tarjetas de RED

Cada tarjeta de red tiene un conector para cada tipo de cable (coaxial, par trenzado, fibra óptica). Las tarjetas de red que funcionan para redes inalámbricas poseen una antena para comunicarse con la estación base.

En una red generalmente se usan dos clases de tarjetas; una con características especiales de configuración física para servidores de red y las tarjetas para las estaciones de trabajo o máquinas clientes.

La tarjeta del servidor puede ser capaz de recibir y transmitir datos a velocidades altas, con el fin de proporcionar un excelente rendimiento al servidor, ya que maneja un tráfico exigente para los usuarios conectados a la red (Figura 2.6).
Las tarjetas de red para las estaciones de trabajo pueden no ser tan exigentes, esto depende de la carga de trabajo de la estación.

Figura 2.6 Tarjeta de red

Los recursos utilizados por una tarjeta son:

- **Input/output Port Address** (Puerto de Dirección de entrada / salida): Estos puertos están en un rango de dirección de 200h a 3FFh, que son para uso de comandos, respuestas de lectura y la transferencia de datos.

- **Interrupt Request Line** (Solicitud de Interrupción): Es el canal requerido por la tarjeta para ser atendida por el procesador de la computadora.

- **Direct Memory Request Line** (DMA): Es una dirección fija de la memoria RAM, para ser utilizada por la tarjeta.

- **Buffers Memory Address:** Espacio en la memoria utilizado por la tarjeta de red que agiliza la entrada de datos de la red al sistema.

2.3 SISTEMAS OPERATIVOS DE RED

Al igual que un equipo no puede trabajar sin un sistema operativo, una red de equipos no puede funcionar sin un sistema operativo de red. Si no se dispone de ningún sistema operativo de red, los equipos no pueden compartir recursos.

Los sistemas operativos de red se encargan de controlar el acceso a los datos que se encuentran en las unidades de discos compartidas del servidor, de la distribución del espacio en los discos duros del servidor y de la utilización de los periféricos compartidos.

En un entorno de red, los servidores proporcionan recursos a los clientes de la red y el software de red del cliente permite que estos recursos estén disponibles para los equipos clientes. La red y el sistema operativo del cliente están coordinados de forma que todos los elementos de la red funcionen correctamente.

Los Sistemas Operativos de red pueden ser de dos tipos: multitarea y multiproceso. Un sistema operativo multitarea, como su nombre indica, proporciona el medio que permite a un equipo procesar más de una tarea a la vez. Un sistema operativo multiproceso puede

ejecutar tantas tareas como procesadores tenga. Si el número de tareas es superior al número de procesadores, el equipo debe ordenar los procesadores disponibles para dedicar una cierta cantidad de tiempo a cada tarea, alternándolos hasta que se completen estas. Con este sistema, el equipo parece que está trabajando sobre varias tareas a la vez. Existen dos métodos básicos de multitarea:

- Con prioridad. En una multitarea con prioridad, el sistema operativo puede tomar el control del procesador sin la cooperación de la propia tarea.

- Sin prioridad (cooperativo). En una multitarea sin prioridad, la propia tarea decide cuándo deja el procesador. Los programas escritos para sistemas de multitarea sin prioridad deben incluir algún tipo de previsión que permita ejercer el control del procesador. No se puede ejecutar ningún otro programa hasta que el programa sin prioridad haya abandonado el control del procesador.

El sistema multitarea con prioridad puede proporcionar ciertas ventajas dada la interacción entre el sistema operativo individual y el sistema operativo de red. Por ejemplo, cuando la situación lo requiera, el sistema con prioridad puede conmutar la actividad de la CPU de una tarea local a una tarea de red.

2.3.1 Características de los Sistemas Operativos en Red.

- Bloqueo de archivos y registros. En un sistema operativo de red, un mismo archivo o un registro de un archivo puede ser usado por más de un usuario, y por tanto es necesario establecer un mecanismo para que dos usuarios no efectúen una modificación en el registro o en el archivo al mismo tiempo.

- Distribución de espacio en los discos duros. En una red local, el disco o los discos duros pueden ser utilizados de tres maneras distintas, ya sea de forma privada, compartida o pública.

  - *En una utilización privada*, los archivos que se encuentran en ellos son personales y únicamente tiene acceso su propietario para operaciones de lectura, escritura, borrado y creación de nuevos archivos.

  - *En una utilización compartida*, los archivos que se encuentran en ellos tienen niveles de acceso distintos en función de las autorizaciones dadas por el administrador de la red.

  - *En una utilización pública*, los archivos pueden ser leídos por todos los usuarios, pero no modificados ni borrados. Esto último sólo puede ser realizado por el administrador de la red.

- Recursos compartidos: Dentro de las ventajas de una red, se encuentra la posibilidad de compartir los recursos que se encuentran en ella, como archivos e impresoras.

Los sistemas operativos se dividen en dos grupos, el modelo cliente servidor y el modelo punto a punto.

2.3.2 Modelos basados en cliente servidor

Los servidores normalmente corren los procesos que ofrecen uno o varios de los siguientes servicios: servidores de archivos, servidores de impresión, de nombres, de correo electrónico, etc.; mientras que, son las computadoras tipo clientes quienes ejecutan los programas de los usuarios y desde donde se solicitan los servicios a los servidores.

En los sistemas que utilizan el modelo cliente-servidor un servidor principal proporciona soporte a las estaciones de la red. Entre ellos tenemos NetWare de Novell, Microsoft LAN Manager, Microsoft Windows NT, LAN Server de IBM y Vines de Banyan, algunos de los cuales se muestran en la figura 2.7.

Figura 2.7 Sistemas operativos Cliente servidor

2.3.3 Modelos basados en sistemas punto a punto

Estos sistemas operativos destacan por la sencillez de su instalación y por su bajo costo, aunque no pueden llegar a competir en posibilidades con los sistemas basados en el modelo cliente-servidor.

En los sistemas que utilizan el modelo punto a punto no existe un servidor principal, sino que todas las estaciones comparten sus recursos de igual a igual. Entre los más utilizados en la actualidad son: Windows 95 y 98, Netware, LAN punto a punto de Macintosh, algunos de ellos se muestran en la figura 2.8.

Figura 2.8 Sistemas Operativos punto a punto

2.4 SERVIDORES DE RED

Los servidores son PC's de gran potencia que permiten que puedan acceder a sus recursos cada uno de los PC's de la red. Este concepto, también se refiere al uso de uno o más PC's para realizar tareas específicas.

2.4.1 Servidor de Discos en Red

Algunas de las primeras LAN usaban un servidor de disco, un disco duro con información para compartirla con las estaciones de trabajo de la red. Las estaciones de trabajo individuales manejan el servidor de discos como si fuera una unidad de disco adicional. La estación de trabajo accede la unidad de la red exactamente de la misma manera como haría con sus propias unidades de disco al almacenar archivos. Sin embargo, el procedimiento se complica cuando una estación de trabajo desea acceder a un archivo específico que se encuentra en un servidor de discos.

Las PC de IBM y sus compatibles que utilizan el DOS, emplean una tabla de asignación de archivos (FAT) para registrar donde se encuentra almacenado un archivo en particular. Sin examinar esta valiosa tabla, una estación de trabajo individual no puede tener idea de dónde están almacenados los archivos. El servidor de discos de red lleva su propia FAT y envía una copia a cada estación de trabajo. Cada una de ellas almacena la copia en RAM y cuando es necesario, el sistema operativo de la estación, utiliza la FAT de la red para tener acceso a los archivos en el servidor de discos.

Con un servidor de discos, la integridad de la FAT se mantiene al dividir (o hacer la partición de) esta unidad de disco duro en varios volúmenes de usuario. Cada volumen se reserva para uso exclusivo de una estación de trabajo específica con objeto de preservar la integridad de la FAT de ese volumen en particular. Aunque es posible que ciertos volúmenes son designados como volúmenes públicos, por lo general éstos se clasifican como de sólo lectura para garantizar su integridad; las estaciones de trabajo individuales pueden consultar esta información pero no pueden modificarla.

2.4.2 Servidor de Archivos

Los servidores de archivo son mucho más eficientes y complejos que los servidores de discos. Contienen un software que forma una protección alrededor del sistema operativo de discos normal de la computadora. Esta protección filtra los comandos hacia el servidor de archivos antes de que el sistema operativo pueda recibirlos. El servidor de archivos cuenta con un sistema de archivos propio. Cuando una estación de trabajo solicita un archivo específico, el servidor de archivos lo envía directamente a dicha estación de trabajo. La estación de trabajo individual no identifica al servidor de archivos como otra unidad de disco, sino que lleva una tabla de conexión de unidades mapeadas designadas de manera lógica que indican la ubicación de los directorios del sistema de archivos del servidor. El usuario solicita un archivo y el servidor responde enviándolo.

El servidor de archivos es más eficiente que los servidores de discos por que no necesita enviar copias de la FAT a cada estación de trabajo que solicita un archivo. Además no hay necesidad de dividir la unidad de disco duro de la red en volúmenes debido a que las

estaciones de trabajo individuales ya no necesitan preocuparse acerca de dónde reside un archivo específico.

2.4.3 Servidor de archivo distribuidos

Para la mayoría de redes de oficinas pequeñas un solo servidor de archivos es más que suficiente. A esto se le conoce como servidor centralizado, y funciona como una mini computadora: Una unidad maneja todo el servicio de archivos y cada estación espera su turno. Si la LAN está diseñada para manejar varios departamentos diferentes, o si se trata de una red más grande, entonces, resulta más eficiente añadir más servidores de archivos a la red.

Estas unidades adicionales se conocen como servidores de archivo distribuido porque dividen (o distribuyen) las tareas de servicio de archivos por toda la red. Este método también proporciona una velocidad óptima para otros usuarios de la red. La información llega con mayor rapidez debido a que el servidor de archivos está localizado justo en el departamento al que sirve.

Otra ventaja es que si un servidor deja de funcionar otro servidor puede dar servicio temporal a toda la red. Aunque también pueden dificultar las tareas de seguridad. El administrador de la red ahora tiene que asegurarse de que todas las unidades de disco de los servidores estén protegidas contra el acceso no autorizado.

2.4.4 Servidor de archivo dedicado y no dedicado

Un servidor de archivos dedicado es una mini computadora (con una unidad de disco duro) que se usa exclusivamente como servidor de archivos. Al dedicar todos sus recursos de procesamiento y de memoria al servicio de archivos, la computadora especial puede ofrecer mayor velocidad y eficiencia a la red.

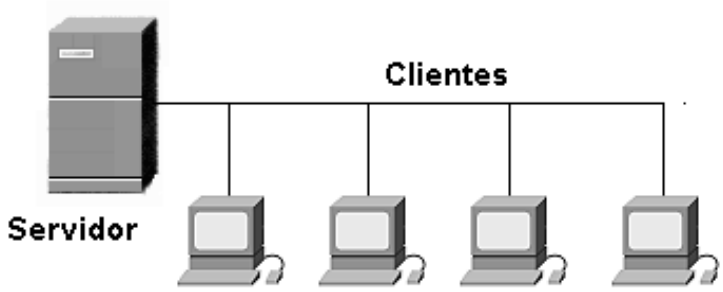


Figura 2.9 Servidor dedicado

Un servidor de archivos como el mostrado en la figura 2.9, no dedicado es aquel que se utiliza como estación de trabajo además de funcionar como servidor de archivos. Esto significa que la memoria RAM debe dividirse de manera que una parte quede disponible para ejecutar programas. También significa que una estación de trabajo de la red quizás tenga que esperar el envío de un archivo mientras el usuario del servidor de archivos carga un programa de la memoria utilizando el microprocesador de la máquina. Entre más rápido sea el microprocesador, el servidor podrá realizar sus tareas con mayor rapidez. Como los servidores de archivos son, por lo general, las computadoras más

rápidas y más caras de la red, es difícil decidir si se deberá especializar la unidad o no. El dinero que podría ahorrarse haciendo que la máquina fuera no dedicada se pierde muchas veces por la degradación de la LAN completa. Por lo general, un servidor de archivos centralizado para más de tres o cuatro estaciones de trabajo debe ser dedicado.

2.4.5 Servidor de archivo en una red punto a punto

En una red de punto a punto, los usuarios determinan qué recursos comparten con otros usuarios de la red. Un usuario podría compartir su unidad de disco duro como servidor de archivos para otros usuarios de la red.

Una red punto a punto como la que se muestra en la figura 2.10, puede estar compuesta de varias estaciones de trabajo servidores de archivo no dedicados cuyos propietarios han decidido compartir sus recursos con otros usuarios. Otros usuarios quizás prefieran compartir las Impresoras. Si un usuario permite que los demás tengan acceso a sus recursos, como a la unidad de disco duro, la memoria RAM de la computadora se divide en RAM disponible para compartir y RAM para el usuario de la máquina. Por lo general, los usuarios no comparten la ejecución de aplicaciones sino, más bien, sólo directorios con archivos de datos.

Figura 2.10 Red punto a punto

2.4.6 Servidor de impresión

Un servidor de impresión de la red hace posible que docenas de estaciones de trabajo compartan varios tipos de impresoras. Con una LAN y el software de servidor de impresión, se puede elegir cualquiera de las impresoras de la red.

Un servidor de impresión de red puede ser una PC dedicada que sólo ejecute el software del servidor de impresión, o puede ser una sección de software que se ejecute en el servidor de archivos de la red.

Es frecuente que algunos administradores de red instalen tarjetas de red en las impresoras para acelerar el proceso de impresión de la red. Estas impresoras pueden recibir datos de la red a razón de varios millones de bits por segundo. Son particularmente útiles para imprimir archivos gráficos extensos que contienen tantos datos que pueden obstruir el tráfico de la red mientras imprimen, debido a que están conectadas directamente a la red y no a la computadora, pero el uso de un servidor de impresión no significa que una estación de trabajo no pueda tener su propia impresora dedicada.

El software para compartir impresoras deben contener un integrador de impresión (prints spooler), un tipo de software que crea una memoria temporal para almacenar las tareas de impresión mientras esperan su turno (en cola de espera). Los integradores complejos tienen capacidades adicionales, incluyendo el traslado de un trabajo al inicio de la cola si requiere impresión inmediata.

2.4.7 Servidor de comunicaciones

Cuando se utilizan dos o más tipos de sistemas operativos es necesario realizar un proceso de traducción para que las computadoras se puedan comunicar entre ellas. Esta traducción puede ser manejada por cada computadora, o bien, por medio de un servidor de comunicaciones de red, también llamado compuerta (gateway).

2.4.8 Otros servidores

Otros servidores que pueden formar parte de una red incluyen a los servidores de fax. Servidores de base de datos, el cual ejecuta específicamente una base de datos y por lo general no maneja sistema de compartir archivos ni impresoras y esta configurado de diferente forma que un servidor de archivos. Existen también servidores de correo, que actúan como buzones de la red y servidores gráficos que manejan y transportan imágenes de alta calidad a lo largo de la red.

2.5 REPETIDOR

Los repetidores son el dispositivo más elemental de una red y, como su nombre indica, se limitan simplemente a regenerar la señal, sin cambiar su contenido, para ampliar el rango de distancia que se alcanza, según el medio físico de transmisión empleado (Figura 2.11). Trabajan en la capa 1 (capa física) del modelo OSI.

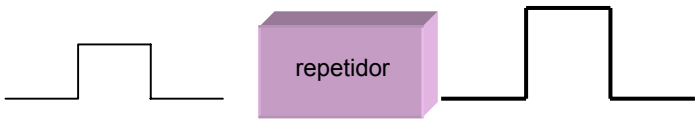


Figura 2.11 El Repetidor sólo regenera una señal

Nos permite interconectar dos o más segmentos incluso con diferentes tipos de cable, permitiéndonos, de este modo, sobrepasar el número máximo de nodos o la longitud máxima, permitida por segmento. Se encarga de regenerar las señales y volver a sincronizar los segmentos, incluso de desconectar (lo que se llama segmentar o particionar) a aquellos que funcionan inadecuadamente, permitiendo así que el resto de la red siga trabajando. Por supuesto, el uso de repetidores está limitado, ya que generan un pequeño retraso, que en caso de prolongarse por varios repetidores consecutivos impediría el adecuado funcionamiento de la red y la perdida de los paquetes que circulan por la misma; entre dos nodos cualesquiera de la red, pueden existir un máximo de cuatro repetidores lo que equivale a cinco segmentos, y además un máximo de tres de ellos pueden conectarse otros nodos (es decir, dos de los cinco segmentos solo pueden ser empleados para la interconexión). La velocidad a la que se transmiten los paquetes es siempre la misma que la de la propia red.

2.6 CONCENTRADORES O HUBS

Comúnmente conocidos como hubs, estos elementos mostrados en la figura 2.12, se basan en el principio de interconexión más básico, podemos entenderlos como un armario de conexiones donde se centralizan todas las conexiones de una red, o sea un dispositivo con entradas y salidas, que no hace nada más que centralizar conexiones, trabaja en la capa 1 (capa física) del modelo OSI, sus funciones son: sondeo de terminales, conversión de códigos, de protocolos, de velocidades, comparación de datos, administración remota, detección y corrección sencilla de problemas. Suelen utilizarse para implementar topologías físicas en estrella, pero funcionando como un anillo o un bus lógico.

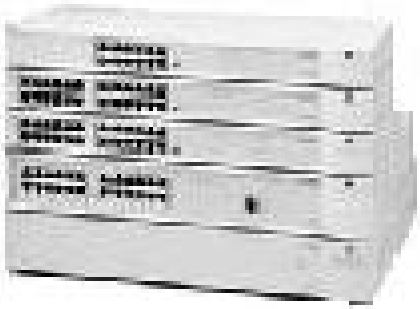


Figura 2.12 HUB

2.7 PUENTES

Sirven para enlazar dos o más LAN que empleen igual protocolo de enlace o LLC (Logical Link Control). Trabajan en la capa 2 (capa de enlace) del modelo OSI, usualmente en la subcapa MAC y no realizan control de flujo, ignorando protocolos de nivel superior, por lo que se comportan de manera transparente respecto a estos.

Así pues, varias redes físicas pueden combinarse para formar una sola red lógica, (Figura 2.13) constituyendo cada una un segmento. Su función es gestionar el tráfico de mensajes entre redes LAN. Los puentes se basan en el principio de que cada nodo de la red tiene su propia dirección, y reenvían los paquetes basándose en la dirección del nodo destino.

Figura 2.13 Unión de dos redes mediante un puente

Un puente es un dispositivo que conecta dos LAN separadas para crear lo que aparenta ser una sola LAN. Los puertos revisan la dirección asociada con cada paquete de información. Luego, si la dirección es la correspondiente al otro segmento de red, el puente pasara el paquete al segmento. Si el puente reconoce que la dirección es la correspondiente a un nodo del segmento de red actual, no pasará el paquete al otro lado.

2.8 CONMUTADORES O SWITCHES

Los switches han sido desarrollados recientemente y conjugan propiedades pertenecientes a un concentrador con las de un puente dando grandes ventajas en el funcionamiento de las redes LAN, ya que el ancho de banda deja de ser compartido para ser dedicado, estos son comúnmente conocidos como conmutadores. Algunos tienen ciertas características de un ruteador, lo que los hace aún más potentes, estos tipos de switches son conocidos como Switch WAN. (Figura 2.14).

En general, un switch conmuta paquetes desde los puertos de entrada hacia los puertos de salida, suministrando a cada puerto el ancho de banda total. Se puede repartir el ancho de banda de la red de una manera apropiada en cada segmento de red o en cada nodo, de modo transparente al usuario. Trabaja en la capa 2 del modelo OSI, dependiendo de sí cuenta con funciones de ruteo o no.

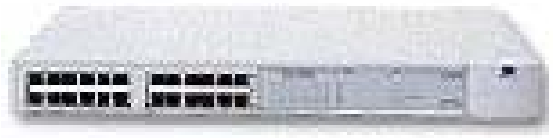


Figura 2.14 Switch

2.8.1 Diferencias entre switch y un hub

Las principales diferencia entre un switch y un Hub son:

- Los switches toman decisiones basándose en las direcciones MAC y los hubs no toman ninguna decisión.
- En un switch el ancho de banda total, está por encima del ancho de banda de cada uno de los puertos.
- Algunos switches son capaces de realizar la integración de distintos tipos de redes (Ethernet, Token Ring, FDDI, ATM, etc.), permitiéndose incluso pequeños cambios de protocolos (siempre que operen en la capa 2 del modelo OSI.

2.9 RUTEADORES

Los ruteadores (Figura 2.15) operan de una manera similar a los puentes, son dispositivos de propósito general diseñado para segmentar la red, con la particularidad de que lo hacen en la capa de 3 del modelo OSI. Incluye una dirección de red y una de dispositivo, permiten la interoperatividad de redes diferentes como pueden ser una Ethernet y una Token Ring, y permite dividir una red en varias subredes, eligiendo el mejor camino para enviar un paquete sin la necesidad de mantener extensas tablas que contengan la dirección de todos y cada uno de los dispositivos conectados, proporcionando seguridad, control y redundancia.

Los routers organizan una red grande en términos de segmentos lógicos. Cada segmento de red es asignado a una dirección, así que, cada paquete tiene tanto *dirección destino*

como *dirección fuente*.

Figura 2.15 Router o Ruteador

Los router son más inteligentes que puentes y switches, no sólo construyen tablas de enrutamiento, sino que además utilizan algoritmos para determinar la mejor ruta posible para una transmisión en particular.

Los protocolos usados para enviar datos a través de un ruteador deben ser específicamente diseñados para soportar funciones de enrutamiento. IP (Internet), IPX (Novell) y DDP (Appletalk Network layer protocol) son protocolos de transporte enrutables. NetBEUI no es un protocolo enrutable por ejemplo. Los router pueden ser de dos tipos:

- **Ruteadores estáticos**: estos router no determinan rutas. En vez de eso, se debe de configurar la tabla de enrutamiento, especificando las rutas potenciales para los paquetes.

- **Ruteadores dinámicos**: Estos router tienen la capacidad de determinar rutas (y encontrar la ruta más óptima) con base en la información de los paquetes y en la información obtenida de otros routers.

2.9.1 Funciones primarias de un ruteador

Las funciones primarias de un ruteador son:

- Segmentar la red dentro de dominios individuales de brodcast.
- Proporcionan un envió inteligente de paquetes.
- Soportar rutas redundantes.

Aislar el tráfico de la red ayuda a diagnosticar problemas, y debido que cada puerto del ruteador es una subred separada, el tráfico de brodcast no pasa a través del ruteador.

2.9.2 Beneficios del ruteador son:

- Proporcionan seguridad a través de sofisticados filtros de paquetes, en ambiente LAN y WAN.

- Permiten diseñar redes jerárquicas, que deleguen autoridad y puedan forzar el manejo local de regiones separadas de redes internas.

- Integran diferentes tecnologías de enlace de datos, tales como Ethernet, Fast Ethernet, Token Ring, FDDI y ATM.

2.10 PALABRAS CLAVES

MEDIOS DE TRANSMISIÓN
PAR TRENZADO
UTP
STP
CABLE COAXIAL
FIBRA ÓPTICA
ONDAS DE RADIO
MICROONDAS TERRESTRES.
MICROONDAS POR SATÉLITE.
INFRARROJOS.
ONDAS DE LUZ.
INTERFACES DE RED (TARJETAS DE RED).
DIRECCIONES MAC.
SISTEMAS OPERATIVOS DE RED
SERVIDORES DE RED
REPETIDOR
CONCENTRADORES O HUBS
PUENTES
CONMUTADORES O SWITCHES
RUTEADORES

Redes virtuales (VLAN)

Capítulo

3

3 REDES VIRTUALES (VLAN)

Los grupos de trabajo en una red, hasta ahora, han sido creados por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo concentrador o hub.

Como consecuencia directa, estos grupos de trabajo comparten el ancho de banda disponible y los dominios de "broadcast", además existe la dificultad de gestión cuando se producen cambios en los miembros del grupo. Más aún, la limitación geográfica que supone que los miembros de un determinado grupo deben estar situados adyacentemente, por su conexión al mismo concentrador o segmento de la red.

Los esquemas VLAN (Virtual LAN o red virtual), proporcionan los medios adecuados para solucionar esta problemática, por medio de la agrupación realizada de una forma lógica en lugar de física.

Sin embargo, las redes virtuales siguen compartiendo las características de los grupos de trabajo físicos, en el sentido de que todos los usuarios tienen conectividad entre ellos y comparten sus dominios de "broadcast".

La principal diferencia con la agrupación física, como se ha mencionado, es que los usuarios de las redes virtuales pueden ser distribuidos a través de una red LAN, incluso situándose en diferentes switches de la misma.

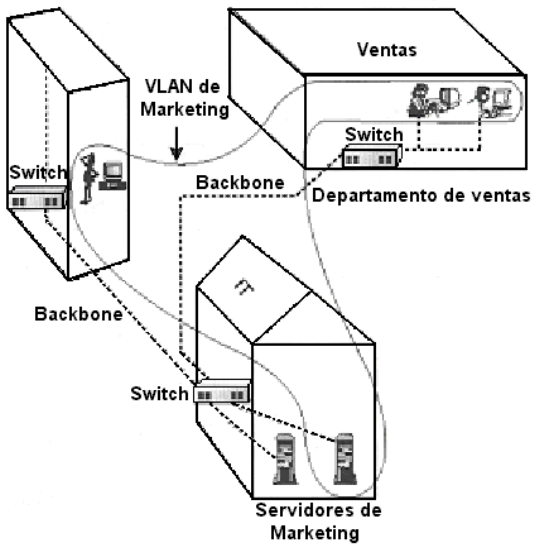


Figura 3.1 Ejemplo de VLAN

Los usuarios pueden, así, "moverse" a través de la red, manteniendo su pertenencia al grupo de trabajo lógico, como se muestra en la Figura 3.1, la VLAN se extiende por toda la empresa desde un edificio donde se localizan los servidores centralizados hasta la oficina donde se encuentran los vendedores pasando por un edificio hacia donde pretende extenderse la oficina de ventas.

Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, logramos, como consecuencia directa, el incremento del ancho de banda en dicho grupo de usuarios.

Además, al poder distribuir a los usuarios en diferentes segmentos de la red, podemos situar puentes y ruteadores entre ellos, separando segmentos con diferentes topologías y protocolos. Así por ejemplo, podemos mantener diferentes usuarios del mismo grupo, unos con FDDI y otros con Ethernet, en función tanto de las instalaciones existentes como del ancho de banda que cada uno precise, por su función específica dentro del grupo.

Todo ello, por supuesto, manteniendo la seguridad deseada en cada configuración por el administrador de la red: Se puede permitir o no que el tráfico de una VLAN entre y salga desde o hacia otras redes.

Pero aún se puede llegar más lejos. Las redes virtuales nos permiten que la ubicación geográfica no se limite a diferentes concentradores o plantas de un mismo edificio, sino a diferentes oficinas intercomunicadas mediante redes WAN o MAN, a lo largo de países y continentes, sin limitación ninguna más que la impuesta por el administrador de dichas redes.

Para comprender los beneficios de las redes VLAN comenzaremos examinando los problemas de una red de área local (LAN) y las posibles soluciones que pueden mejorar su rendimiento.

Hablaremos sobre la congestión y sus efectos sobre el rendimiento de las redes y las ventajas de las segmentación LAN en una red, así como las ventajas e inconvenientes del uso de puentes, switches y ruteadores para la segmentación LAN y los efectos de la conmutación, el bridging y el enrutamiento en una estructura de red .

3.1 PROBLEMÁTICA DE LAS REDES LAN ACTUALES

Hoy en día, las redes están cada vez más congestionadas. Al margen de una población siempre creciente de usuarios de red, se han combinado otros factores para ampliar las posibilidades de las LANs tradicionales:

- CPU más rápidas: A mediados de los ochenta, la mayoría de los PC podían realizar un millón de instrucciones por segundo (MIPS). Actualmente, es habitual ver estaciones provistas de una potencia de procesamiento de 50 a 75 MIPS, y las velocidades de entrada/salida (E/S) han aumentado en la misma medida. Como resultado de ello, dos estaciones de trabajo que estén en la misma LAN pueden saturar fácilmente la red.

- Sistemas operativos más rápidos: El entorno multitarea presente en los sistemas operativos de PC actuales (Windows, UNIX y Mac) permite que haya transacciones de red simultáneas. Esta capacidad integrada ha supuesto un incremento de una demanda mayor de recursos de red.

- Aplicaciones intensivas de red: El uso de aplicaciones cliente/servidor están aumentando. Este tipo de aplicaciones permite a los administradores centralizar la

información, facilitando así su mantenimiento y protección. Las aplicaciones cliente/servidor liberan a los usuarios de la tarea de mantener la información siempre que se disponga del suficiente espacio de disco duro para almacenarla. Dada la ventaja que ofrecen estas aplicaciones, cada vez son más utilizadas.

Problemática de las LAN Ethernet

La arquitectura LAN más común es Ethernet 802.3, Ethernet se usa para transportar datos entre los dispositivos de red como computadoras, impresoras y servidores. En ésta arquitectura, todos los dispositivos se encuentran conectados al mismo medio de transmisión, por lo que el rendimiento se puede ver afectada negativamente por todos o alguno de los factores que se describen a continuación.

- **Diseño semidúplex**

  Ethernet es una tecnología semiduplex, es decir, cada estación Ethernet comprueba la red para ver si se están transmitiendo datos antes de transmitir más datos. Si la red ya está en uso, la transmisión se retrasará. A pesar del retraso de transmisión, dos o más estaciones pueden transmitir a la vez, lo que acaba en una colisión.

  Cuando se produce una colisión, la estación que primero detecte la colisión enviará una señal de atasco. Al “oírla”, todas las demás estaciones esperarán un periodo de tiempo aleatorio antes de tratar de transmitir de nuevo. Cuantas más estaciones se añadan a la red y empiecen a transmitir, más probabilidad habrá de que haya colisiones.

  Las LAN Ethernet se saturan, porque los usuarios ejecutan software intensivo de red, como por ejemplo, aplicaciones cliente/servidor, lo que hace que las estaciones de trabajo transmitan con más frecuencia y durante periodos más prolongados.

- **Latencia**

  La latencia o retraso de propagación, es el tiempo que tarda una trama, o paquete de datos, en viajar desde la estación de origen hasta su destino final en la red. Dado que las LAN Ethernet utilizan CSMA/CD para ofrecer el máximo esfuerzo de entrega, debe haber un cierto grado de latencia en el sistema para detectar colisiones y negociar derechos de transmisión en la red, ya que el objetivo de Ethernet consiste en permitir que todos los dispositivos que comparten el medio transmitan sobre una base de igualdad.

  La latencia no depende exclusivamente de la distancia y del número de dispositivos. Por ejemplo, si tres switches separan dos estaciones de trabajo, éstas, experimentarán menor latencia que si las separaran dos routers. Esto se debe a que los routers realizan una toma de decisiones más compleja y prolongada. Los dispositivos de intermediación, es decir, los switches, mejoran mucho el rendimiento de la red.

- **Congestión y ancho de banda**

  Los avances técnicos están creando computadoras y estaciones de trabajo más rápidas e inteligentes. La combinación de esto, junto con las aplicaciones de red más intensivas ha originado una necesidad de mayor capacidad de red, o ancho de banda.

  Las redes actuales están experimentando un crecimiento en la transmisión de archivos gráficos grandes, vídeo de movimiento completo y aplicaciones multimedia, así como, un aumento en el número de usuarios por red. Todos estos factores ejercen mucha presión en el ancho de banda.

  Cuanta más gente utilice una red para compartir archivos grandes, acceder a servidores de archivos y conectarse a Internet, más congestión habrá. Esto puede suponer que los tiempos de respuesta sean más prolongados, que las transferencias de archivos sean más largas y que los usuarios de las redes se vuelvan menos productivos por causa de los retrasos de la red. Para aliviar la congestión de red, es necesario que haya más ancho de banda disponible y sobre todo que se use de forma más eficaz.

- **Uso de repetidores**

  La distancia que una LAN puede cubrir está limitada por causa de la atenuación, la atenuación significa que la señal se debilita mientras viaja por la red.

  La atenuación es causada por la resistencia del cable, o medio de transmisión. Como se mencionó anteriormente, un repetidor Ethernet es un dispositivo de capa física que regenera la señal de una LAN Ethernet. Cuando se usa un repetidor Ethernet para ampliar la distancia de una LAN, una sola red puede recorrer una distancia muy grande y más usuarios pueden compartir la misma red. Sin embargo, el uso de repetidores y repetidores multipuerto o Hubs también conlleva el tema del efecto de las difusiones y las colisiones sobre el rendimiento general de la red LAN.

3.2 USO DE SEGMENTACIÓN PARA MEJORAR EL RENDIMIENTO DE UNA LAN

Una red se puede dividir en unidades más pequeñas llamadas segmentos. Al dividir la red en segmentos se puede reducir la congestión, pues cada segmento utiliza el método de acceso CSMA/CD y mantiene el tráfico sólo entre los usuarios de dicho segmento, es decir cada segmento es un dominio de colisión.

Por ejemplo, como se muestra en la Figura 3.2, al segmentar una red a 10 Mbps, se reduce el número de dispositivos que comparten esos 10 Mbps, y como consecuencia de esto se reduce el numero de colisiones por segmento.

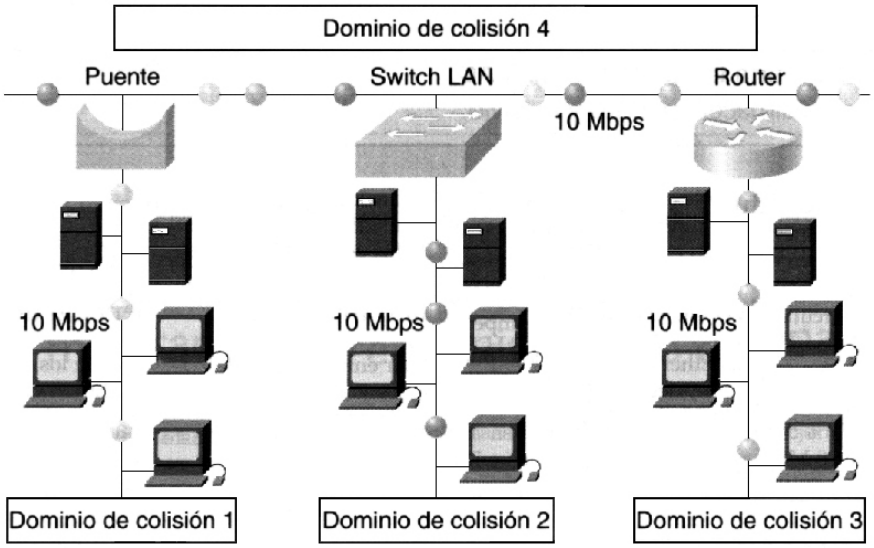


Figura 3.2 Segmentación

3.2.1 Segmentación con puentes

Los puentes fueron diseñados, según la norma IEEE802.1d, para la conexión de redes diferentes. La filosofía de los puentes impide que las colisiones se propaguen entre diferentes segmentos de la red, algo que los repetidores son incapaces de hacer.

Como se muestra en la figura 3.3, los puentes "aprenden" la segmentación de una red al observar el tráfico de cada segmento o pueden usar filtros definidos por el administrador de red, construyendo una tabla con la dirección MAC de cada dispositivo de red, lo cual les permite saber qué segmento utilizar para alcanzar dicho dispositivo. Los puentes son dispositivos que reenvían tramas de datos en función de las direcciones MAC de las tramas.

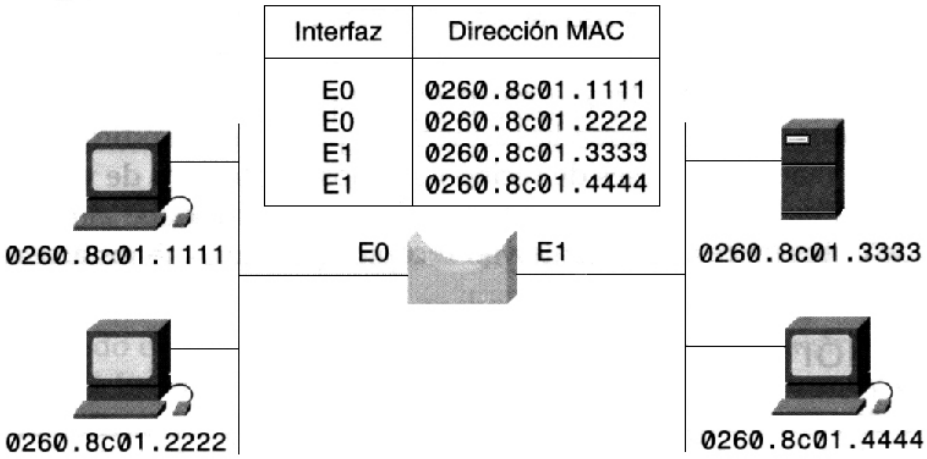


Figura 3.3 Segmentación con puente

Con el uso de puentes, cada segmento dispone del 100% del ancho de banda, o en otras palabras, el ancho de banda total de la red se multiplica por el número de puertos con que

cuenta el puente. Por ejemplo en el caso de una red Ethernet a 10 Mbps, con un puente de dos puertos, el ancho de banda total disponible entre dos segmentos seria de 20Mbps. Un puente transmite paquetes de un segmento a su destino en otro segmento. Cuando se activa un puente y empieza a operar, examina la dirección MAC de los paquetes de entrada y construye una tabla de destinos conocidos. Si el puente sabe que el destino de un paquete está en el mismo segmento que el origen lo descarta, ya que no es necesario transmitirlo. Si el puente sabe que el destino está en otro segmento, transmitirá el paquete únicamente a ese segmento. Si el puente no conoce el segmento de destino, transmitirá el paquete en todos los segmentos a excepción del de origen (una técnica que se conoce como inundación). La ventaja principal de los puentes es que limitan el tráfico a ciertos segmentos de red.

Los puentes incrementan la latencia de una red de un 10 a un 30%. Esta latencia se debe a la toma de decisiones necesaria para que el puente o puentes transmitan los datos. Si el puerto de destino está ocupado, el puente almacenará la trama temporalmente, hasta que el puerto esté disponible. El tiempo que se tarda en llevar a cabo estas tareas disminuye la velocidad de transmisiones de red, originando más latencia.

3.2.2 Segmentación con routers

Un router funciona en la capa de red y basa todas sus decisiones acerca del reenvío entre segmentos en la dirección del protocolo de capa de red. Un router toma decisiones de reenvío con respecto a los segmentos, examinando la dirección IP de destino del paquete de datos y su tabla de enrutamiento para decidir las instrucciones de reenvío.

Los routers impiden la propagación de colisiones de unos segmentos a otros en la red; es más, en realidad separan totalmente los segmentos convirtiéndolos en redes lógicas totalmente diferentes denominadas subredes, como se muestra en la Figura 3.4, y pueden llegar a transmitir los paquetes a la misma velocidad a la que circulan por la red.

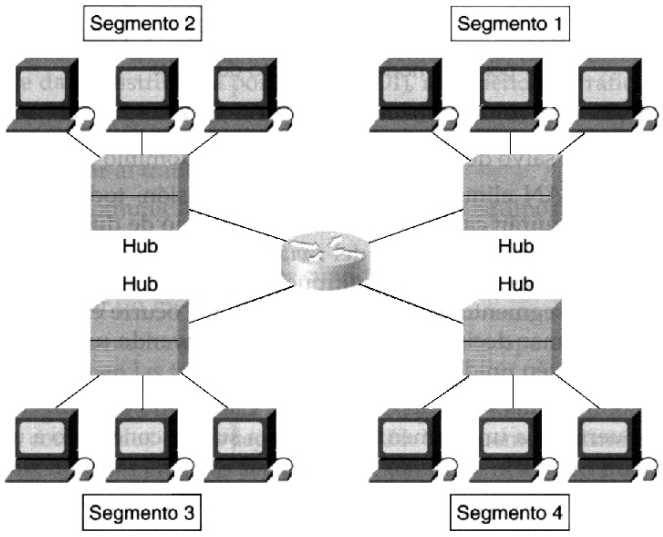


Figura 3.4 Segmentación con routers

Un router debe examinar un paquete para determinar la mejor ruta para reenviarlo a su

destino. Este proceso lleva tiempo. Los protocolos que requieren un acuse de recibo del receptor al remitente tras la recepción de cada paquete (que se conocen como protocolos orientados al acuse de recibo) tienen una pérdida de rendimiento del 30 al 40%. Los protocolos que requieren acuses de recibo mínimos (protocolos de ventana deslizante) sufren una pérdida del 20 al 30% en su rendimiento. Esto se debe al hecho de que hay menos tráfico de datos entre el remitente y el receptor, es decir, menos acuses de recibo.

3.2.3 Segmentación con switches LAN

Un switch LAN es un puente multipuerto de muy alta velocidad, provisto de un puerto para cada nodo o segmento de la red. Al igual que ocurre en los puentes, los switches también pueden tomar decisiones de reenvío construyendo una tabla de direcciones MAC de las estaciones que estén unidas a cada puerto.

Un switch puede segmentar una red en microsegmentos, los cuales son, una sola estación conectada a un puerto del switch. Esto crea dominios a salvo de colisiones a partir de un dominio de colisión más grande.

Aunque el switch LAN elimina los dominios de colisión, todas las estaciones conectadss al switch seguirán estando en el mismo dominio de broadcast. La figura 3.5 representa una LAN segmentada mediante switches, como podemos ver cada puerto del switch constituye un segmento de red formado por cada uno de los hubs y es, a su vez, un dominio de colisión separado, el total de los puertos del switch integran un dominio de broadcast.

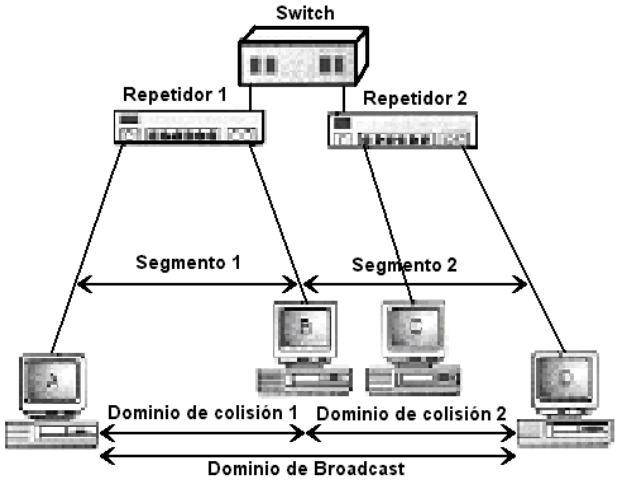


Figura 3.5 Ejemplo de segmentación

En una LAN Ethernet a 10 Mbps, una estación que está conectada directamente a un switch Ethernet es su propio dominio de colisión y accede a la totalidad de los 10 Mbps, es decir, si cada nodo está directamente conectado a uno de los puertos o a un segmento que está a su vez conectado a uno de los puertos del switch, se crea una conexión con un ancho de banda de 10Mbps entre cada nodo y cada segmento del switch.

Los conmutadores o switches tiene la funcionalidad de los concentradores a los que se añade la capacidad principal de dedicar todo el ancho de banda de forma exclusiva a

cualquier comunicación entre sus puertos. Esto se consigue debido a que el conmutador no actúa como repetidor multipuerto, si no que únicamente envía paquetes de datos hacia el puerto al que van dirigidos.

Como se vera a continuación, la conmutación LAN aligera la falta de ancho de banda y los cuellos de botella en las redes, como los que se producen entre varias PC y un servidor de archivos remoto; ya que teóricamente, la diferencia fundamental entre puentes y switches (conmutadores) es que los puentes reciben el paquete completo antes de proceder a su envío al puerto destinatario, mientras que un conmutador puede iniciar su reenvío antes de haberlo recibido por completo, ello redunda en una mejora de prestaciones.

3.2.4 Seleccionando Switches o un Routers para Segmentar

Al trabajar un ruteador en la capa 3 del modelo OSI, puede también ejecutar funciones de la capa 2, es decir el ruteador crea dominios de broadcast y de colisiones separados en cada interface. Esto significa que tanto el switch como el ruteador pueden usarse para segmentar una LAN y adicionar ancho de banda.

Entonces, ¿cual es la selección más óptima para el diseño de la red?

- Si la aplicación requiere soporte para rutas redundantes, envío inteligente de paquetes o acceso a una WAN, se debe seleccionar un ruteador.
- Si la aplicación sólo requiere incrementar ancho de banda para descongestionar el tráfico, un switch probablemente es la mejor selección.

Dentro de un ambiente de grupos de trabajo, el costo interviene en la decisión de instalar un switch o un ruteador, y como el switch es de propósito general, tiene un bajo costo por puerto en comparación con el ruteador.

Además el diseño de la red determina cuales son otros requerimientos (redundancia, seguridad o limitar el tráfico de broadcast) que justifique el gasto extra y la complejidad de instalar un ruteador dentro de dicho ambiente.

3.3 CONMUTACIÓN PARA MEJORAR EL RENDIMIENTO DE UNA LAN

La conmutación es el proceso de tomar una trama de entrada por medio de un puerto o interfaz y enviarla por otro. La conmutación es una tecnología que reduce la congestión en las redes Ethernet, Token Ring e Interfaz de datos distribuida por fibra (FDDI), reduciendo el tráfico e incrementando el ancho de banda.

Una LAN que utiliza una topología Ethernet conmutada crea una red que se comporta como si sólo tuviera dos nodos: el nodo de envío y el nodo de recepción. Estos dos nodos comparten el mismo ancho de banda entre ellos, lo cual significa que casi todo el ancho de banda está disponible para la transmisión de los datos. Dado que una LAN Ethernet conmutada utiliza el ancho de banda muy eficientemente, puede ofrecer más rendimiento que las LAN Ethernet conectadas por puentes o hubs. En una implementación LAN Ethernet conmutada, el ancho de banda disponible puede llegar a ser el 100%.

La conmutación Ethernet crea segmentos de red dedicados (es decir, conexiones punto a punto) y conectan estos segmentos a una red virtual dentro del switch. Este circuito de red virtual sólo tiene lugar cuando dos nodos necesitan comunicarse. Ésta es la razón por la que se denomina circuito virtual, sólo existe en caso de necesidad, y se establece dentro del switch. Una de las desventajas de los switches es que son más caros que los hubs.

Hoy en día, en las comunicaciones de datos, todos los equipos de conmutación llevan a cabo dos operaciones básicas:

- Conmutar tramas de datos. Ocurre cuando una trama llega a un medio de entrada y se transmite por un medio de salida.

- Mantener las operaciones de conmutación. En esta operación se construyen y mantienen las tablas de conmutación.

Hay dos formas de conmutar tramas de datos: la conmutación de capa 2 con switches y de capa 3 con routers.

La diferencia entre la conmutación de Capa 2 y la de Capa 3 es el tipo de información que hay dentro de la trama que se usa para determinar el puerto de salida correcto. Con la conmutación de capa 2, las tramas son conmutadas en base a la información de la dirección MAC. Con la conmutación de Capa 3, las tramas son conmutadas en base a la información de la capa de red. Las direcciones de la Capa 2 permanecen fijas en un dispositivo, mientras que sí es posible cambiar las direcciones de Capa 3. Además, las direcciones de capa 2 son universalmente únicas.

Los switches de capa 2 emplean la microsegmentación para satisfacer la demanda de más ancho de banda y de rendimiento mejorado, pero los diseñadores de redes se enfrentan ahora con la demanda creciente de comunicación intersubred. Por ejemplo, cada vez que un usuario accede a servicios y a recursos que se encuentren en distintas subredes, el tráfico deberá pasar por un dispositivo de capa 3. Potencialmente, existe un cuello de botella que puede amenazar el rendimiento de la red. Para evitarlo, los diseñadores de redes pueden incorporar opciones de capa 3 a lo largo de la red, con lo que se alivia la presión sobre los routers centralizados.

3.3.1 Conmutación con switches

Tanto los puentes como los switches conectan segmentos LAN, y utilizan una tabla de direcciones MAC para determinar el segmento donde hay que transmitir un paquete, reduciendo el tráfico. Los switches son más funcionales que los puentes, ya que operan a velocidades mucho más altas y pueden soportar funcionalidades nuevas, como las LAN virtuales (VLAN). Los puentes suelen conmutar utilizando software, mientras que los switches lo suelen hacer por medio de hardware

La conmutación de la capa 2 no mira en el interior de un paquete para ver si éste contiene información de capa de red, sino que busca una dirección MAC de destino y envía la información a la interfaz apropiada si conoce la ubicación de la dirección de destino. La conmutación de la capa 2 construye y mantiene una tabla de conmutación que controla las direcciones MAC que pertenecen a cada puerto o interfaz. Si el switch no sabe dónde

enviar la trama, la difundirá a todos sus puertos de la red para conocer el destino correcto. Cuando la respuesta de la trama es devuelta, el switch conoce la ubicación de la nueva dirección y añade la información a la tabla de conmutación.

- **Reconocimiento de direcciones por un switch**

  Un switch Ethernet puede conocer la dirección de cada dispositivo de la red leyendo la dirección de origen de cada paquete transmitido y anotando el puerto donde accedió al switch. A continuación, el switch añade esta información a su base de datos de reenvío.

  Las direcciones se aprenden de forma dinámica. Esto significa que a medida que se van leyendo las nuevas direcciones, se van aprendiendo y almacenando en la CAM (memoria direccionable por contenido). Cuando se lee un origen que no se encuentra en la CAM, se aprende y almacena para su uso futuro.

  Cada vez que se almacena una dirección, se le añade un nuevo timestamp. Esto permite almacenar las direcciones un determinado periodo de tiempo. Cada vez que se hace referencia o se encuentra una dirección en la CAM, ésta recibe un nuevo timestamp. Las direcciones a las que no se haga referencia durante un periodo de tiempo determinado se eliminan de la lista. Al eliminar direcciones antiguas, la CAM mantiene funcional la base de datos.

3.3.2 Conmutación con routers

La conmutación de capa 3 examina la información del paquete y los reenvía con base a sus direcciones de destino de la capa de red. La conmutación de capa 3 también soporta la funcionalidad del router. Durante casi todo el proceso, el administrador de red es quien determina las direcciones de capa 3. Protocolos como IP, IPX y AppleTalk utilizan el direccionamiento de capa 3. Al crear direcciones de capa 3, un administrador de red crea áreas locales que actúan como unidades de direccionamiento únicas (parecidas a las calles, ciudades, estados y países) y asigna un número a cada entidad local. Si los usuarios se trasladan a otro edificio, sus estaciones finales obtendrán nuevas direcciones de capa 3, pero sus direcciones de capa 2 seguirán siendo las mismas.

Dado que los routers funcionan en la capa 3 del modelo de referencia OSI, pueden adherirse y crear una estructura de direccionamiento jerárquica. Por tanto, una red enrutada puede unir una estructura de direccionamiento lógica a una infraestructura física, por ejemplo, a través de subredes TCP/IP o redes IPX en cada segmento. El flujo de tráfico de una red conmutada (es decir, plana) es diferente del flujo de tráfico de una red enrutada (es decir, jerárquica). Las redes jerárquicas ofrecen un flujo de tráfico más flexible, ya que pueden usar la jerarquía de red para determinar las rutas óptimas y contener dominios de broadcast.

3.3.3 Tipos de Conmutación

- **Conmutación simétrica**

  La conmutación simétrica es una forma de caracterizar un switch LAN en función

del ancho de banda asignado a cada puerto del switch. Como se muestra en la Figura 3.6, un switch simétrico proporciona conexiones entre puertos con el mismo ancho de banda, como todos los puertos de 10 Mbps o todos los puertos de 100 Mbps.

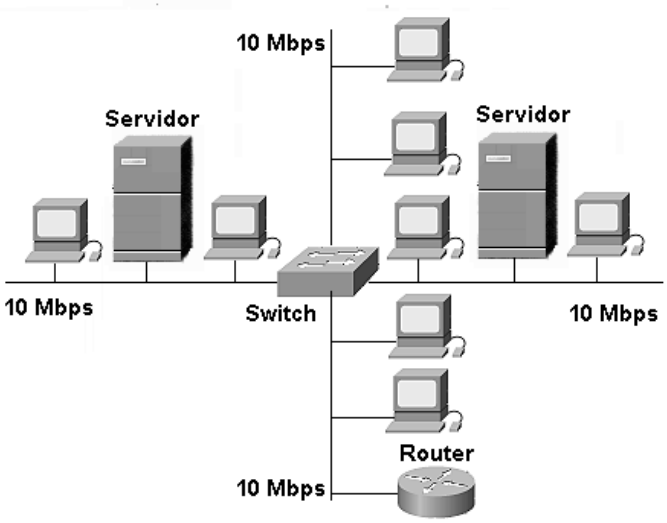


Figura 3.6 Conmutación simétrica

- **Conmutación asimétrica**

Un switch LAN asimétrico ofrece conexiones conmutadas entre puertos de ancho de banda diferente, como una combinación de puertos de 10 Mbps y 100 Mbps. Como se muestra en la Figura 3.7, la conmutación asimétrica saca el máximo partido a los flujos de tráfico de una red cliente/servidor, donde múltiples clientes se comunican con un servidor a la vez, requiriendo más ancho de banda dedicado al puerto del switch al que está conectado el servidor, con el fin de evitar un cuello de botella en ese puerto.

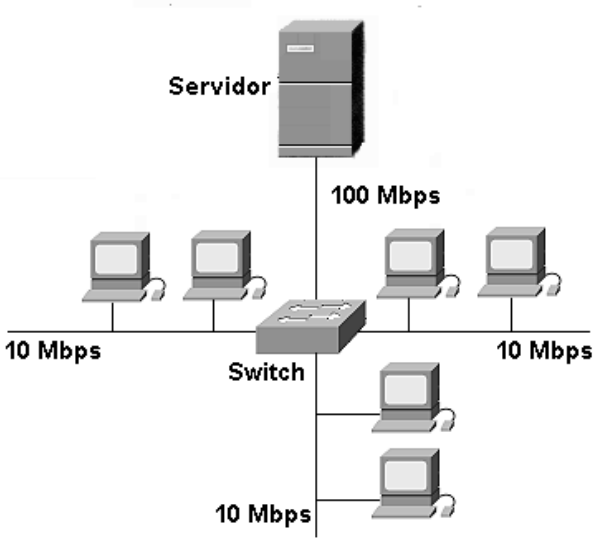


Figura 3.7 Conmutación Asimetríca

Como veremos a continuación, el buffering de memoria de un switch asimétrico es necesario para permitir que se envíe el tráfico desde un puerto de 100 Mbps hasta un puerto de 10 Mbps sin causar demasiada congestión en el puerto de 10 Mbps.

Un switch Ethernet puede usar una técnica de buffering para almacenar y reenviar paquetes al puerto o puertos correctos. El buffering también se puede utilizar cuando el puerto de destino está ocupado. El área de memoria en la que el switch almacena los datos de destino y de transmisión se denomina buffer de memoria, éste puede utilizar dos métodos para reenviar paquetes:

- **Buffering de memoria basado en el puerto**

  En este método los paquetes se almacenan en colas que están vinculadas a puertos de entrada específicos. Un paquete sólo se transmite al puerto de salida cuando todos los paquetes que estén delante de él en la cola se hayan transmitido con éxito.

  Es posible que un solo paquete retrase la transmisión de todos los paquetes de la memoria, a causa de un puerto de destino ocupado. Este retraso se produce aunque los otros paquetes puedan ser transmitidos a puertos de destino abiertos.

- **Buffering de memoria compartida**

  Este método deposita todos los paquetes en un búfer de memoria común que está compartido por todos los puertos del switch. La cantidad de memoria asignada a un puerto esta determinada por la necesidad de cada puerto. A esto se le denomina asignación dinámica de memoria de buffer. Los paquetes del buffer son vinculados dinámicamente al puerto de transmisión; el paquete se vincula a la asignación de memoria de ese puerto de transmisión. Esto permite recibir el paquete por un puerto y que se transmita por otro, sin moverlo a una cola diferente.

  El switch mantiene un mapa de los puertos a los que el paquete necesita ser transmitido. El switch sólo despeja este mapa de puertos de destino cuando el paquete ha sido transmitido con éxito. Dado que el búfer de memoria está compartido, el paquete está restringido por el tamaño total del buffer de memoria, y no sólo por la asignación a un solo puerto. Esto implica que los paquetes más grandes pueden ser transmitidos liberando menos paquetes, lo cual es relevante para la conmutación 10/100, donde un puerto de 100 Mbps puede reenviar un paquete a un puerto de 10 Mbps.

3.3.4 Métodos de conmutación

Es posible usar dos métodos de conmutación para reenviar una trama por un switch:

- **Almacenamiento y reenvío.**

  En este método se recibe la totalidad de la trama antes de que tenga lugar el reenvío. Se aplican las direcciones de destino y de origen y se aplican los filtros antes de que se reenvíe la trama. La latencia tiene lugar durante la recepción de la trama, es decir, la latencia es mayor con tramas más grandes, ya que la lectura de toda la trama es más lenta. La detección de errores es alta, debido al tiempo que tiene el switch para detectar errores en espera de la recepción de la totalidad de la trama.

- **Por método de corte.**

  En éste método el switch lee la dirección de destino antes de recibir la totalidad de la trama. La trama es reenviada antes de que llegue la totalidad de la misma, de este modo se reduce la latencia de la transmisión, pero la detección de errores es mínima. Hay dos formas de conmutación por método de corte:

  - **Conmutación de reenvío rápido.**

    Este tipo de conmutación ofrece el nivel más bajo de latencia reenviando de forma inmediata un paquete después de recibir la dirección de destino. Dado que esta conmutación empieza reenviando antes de recibir la totalidad del paquete, es posible que haya veces en que los paquetes se retransmitan con errores. Aunque esto no suele ocurrir y el adaptador de red de destino descarta el paquete erróneo tras su recepción, el tráfico superfluo puede ser inaceptable en ciertos entornos. Utilice la opción sin fragmentos para reducir el número de paquetes que se reenvía con errores. En el modo de reenvío rápido, la latencia se calcula desde el primer bit que se recibe hasta el primero que se transmite, o primero en entrar, primero en salir (FIFO).

  - **Conmutación sin fragmentos.**

    Este tipo de conmutación filtra los fragmentos de colisión, que constituyen la mayoría de los paquetes con errores, antes de que empiece el reenvío. En una red que funcione bien, los fragmentos de colisión deben ser menores de 64 bytes. Cualquiera de ellos que exceda de los 64 bytes es un paquete válido, por lo que se suele recibir sin errores. La conmutación sin fragmentos espera hasta que el paquete recibido haya determinado no ser un fragmento de colisión antes de reenviar el paquete. En este modo, la latencia se calcula como FIFO.

La latencia de cada modo de conmutación depende de cómo el switch reenvía las tramas. Cuanto más rápido sea el modo de conmutación, menor será la latencia del switch.
Para llevar a cabo el reenvío rápido de tramas, el switch emplea menos tiempo en comprobar los errores. Esto tiene como resultado una menor comprobación de errores, lo que puede conducir a un número más alto de retransmisiones.

En caso de diferencia de velocidades entre las subredes interconectadas al conmutador, necesariamente ha de operar con el método de almacenamiento y reenvío. Esta tecnología proporciona una serie de facilidades como son:

- **Filtrado Inteligente**

  Posibilidad de hacer filtrado de trafico no sólo basado en direcciones MAC, sino considerando parámetros adicionales, tales como el tipo de protocolo o la congestión de tráfico dentro del switch o en otros switches de la red.
- **Soporte de redes VLAN**

  Las VLAN segmentan lógicamente la infraestructura física de una LAN en distintas subredes o dominios de difusión, de forma que las tramas de difusión sólo son conmutadas entre puertos de la misma VLAN. De esta forma se simplifican también los movimientos o cambios , permitiendo a los usuarios ser reubicados fácilmente.

Lo que podemos observar después de haber tratado los temas de conmutación y segmentación, es que ambos conceptos van unidos, es decir, la segmentación se encarga de reducir el número de estaciones conectadas a una red o subred (segmento) mientras que la conmutación, se encarga de establecer conexiones punto a punto dentro de cada uno de los segmentos de red.

Otra forma en la que podrías ver la relación entre estos dos conceptos es la siguiente: la segmentación de una red implica la redistribución física de los dispositivos en dicha red, mientras que la conmutación solo implica el cambio de hubs por puentes o switches en los armarios o closets de comunicaciones, es decir, para reorganizar una red mediante segmentación además de sustituir hubs por puentes o switches, habría que reorganizar las PC de modo que los usuarios con recursos compartidos en común queden en el mismo segmento de la red para que no tengan que estar realizan consultas entre segmentos. El empleo de conmutación, facilita la comunicación entre segmentos permitiendo que una máquina de un determinado segmento acceda directamente a los recursos que necesita en algún dispositivo de otro segmento diferente, evitando así la congestión de la red.

Después de analizar los beneficios de la segmentación y la conmutación en cuanto a la mejora del rendimiento de las redes de área local, veremos a continuación el uso de redes virtuales de área local (VLAN), donde unimos los beneficios de estas dos técnicas (conmutación y segmentación), para disminuir el trafico de broadcast en la red mediante la segmentación lógica de la misma, este tipo de redes son posibles gracias a las características de conmutación que ofrecen algunos switches.

3.4 VLAN

Una de las grandes virtudes de puentes y switches es su sencillez de manejo. Debido a su funcionamiento transparente es posible realizar una compleja red, incluso con enlaces WAN si se utilizan puentes remotos, sin tener que configurar ningún router. A fines de los 80’s se puso de moda la idea de desarrollar grandes redes, incluso a nivel nacional,

basadas únicamente en el uso de puentes transparentes. Sin embargo pronto se vio que esta estrategia tenía dos inconvenientes serios:

- Los puentes propagan el tráfico broadcast y multicast. Generalmente los protocolos orientados a redes LAN hacen un uso exhaustivo de este tipo de frames, especialmente los broadcast, para anunciar todo tipo de servicios. Incluso el protocolo de red IP, emplea broadcasting para la resolución de direcciones. La proliferación de tráfico broadcast en una red es especialmente grave más que por el ancho de banda desperdiciado por el consumo de ciclos de CPU que se produce en todos los nodos de la red. Este no es el caso con los frames multicast, ya que cuando un frame multicast no incumbe a una estación es descartado por la interfaz.

- La transparencia de los puentes hace difícil establecer mecanismos de control, protección y filtrado de tráfico, por lo que las redes muy grandes basadas en puentes se hacen inmanejables. Además, en los casos en que se requieren controles o mecanismos de administración se han de utilizar direcciones MAC que no tienen ningún prefijo común que permita referirse o identificar una parte de la red, ya que la asignación no ha seguido ningún criterio geográfico ni corresponde con la topología de la red.

Como consecuencia de esto la creación de grandes redes locales está desaconsejada y es práctica habitual en estos casos separar mediante routers las diversas partes de la red. Este es el caso en un campus o gran edificio. Los routers, son equipos de comunicaciones que actúan a nivel de red, aislando los frames broadcast y multicast (es decir, no los retransmite por sus otras interfases como lo hace un puente o un switch) y facilitan la administración al agregar las direcciones de nivel de red y un ordenamiento lógico de más alto nivel. Se puede observar entonces que un router, por el hecho de aislar los broadcast, genera tantos dominios de broadcast como interfases tenga.

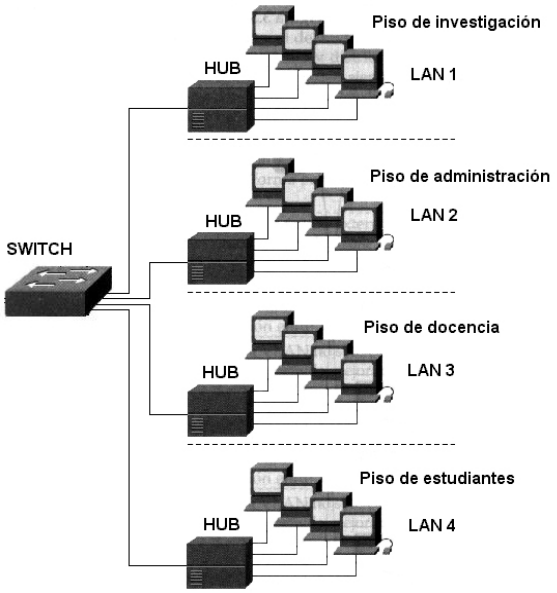


Figura 3.8 Organización por piso para los grupos de trabajo.

Dividir una red local con criterios geográficos resulta relativamente sencillo, ya que normalmente la topología del cableado permite realizar esa división de manera directa. Como se muestra en la Figura 3.8, una red LAN típica está configurada en función de la infraestructura física que la conecta. Los usuarios están agrupados con base a las conexiones con el hub compartido y los puertos de router que hay entre los hubs. Esta topología proporciona únicamente una segmentación entre los hubs, que suelen estar ubicados en pisos separadas, y no entre usuarios conectados al mismo hub. Esto impone limitaciones físicas en la red y limita el modo en que se pueden agrupar los usuarios.

Un switch segmenta físicamente una LAN en dominios de colisión individuales. No obstante, cada segmento sigue formando parte de un dominio de broadcast. El número total de segmentos de un switch equivale a un dominio de broadcast.

Por ejemplo, si se quiere dividir en varias una red local que abarca el campus de una universidad, se puede crear una LAN por edificio con switches en cada edificio e interconectar cada edificio a una interfaz diferente de un router que interconecte todo el campus, para así aislar los dominios de broadcast y mantener comunicadas todas las LAN. Sin embargo, a menudo se requiere realizar una división lógica de acuerdo a criterios funcionales, que no siempre coinciden con la ubicación física. Por ejemplo, en el caso de una universidad se podría pensar por razones de eficiencia y seguridad en crear una red para investigación, otra para docencia, otra para estudiantes y una última para tareas administrativas.

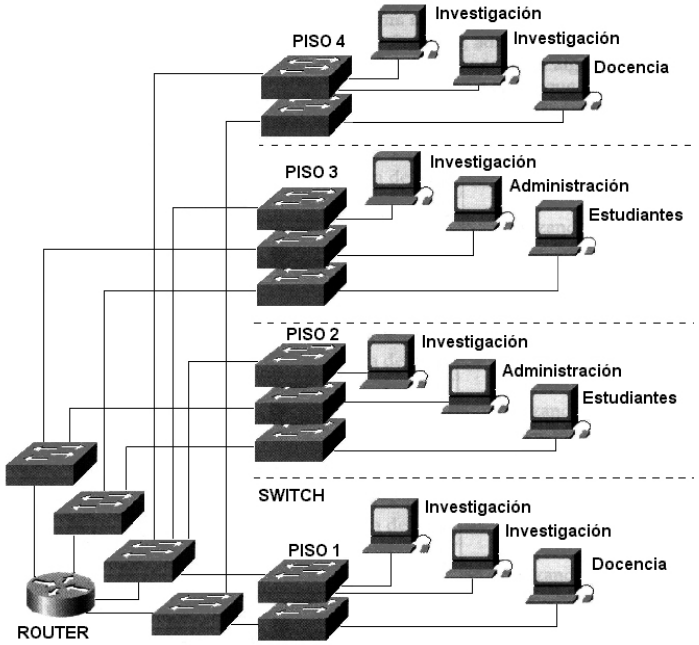


Figura 3.9 Organización utilizando múltiples switches para los grupos de trabajo

Normalmente habrá varios edificios en los que habrá que dotar una serie de puestos de cada una de las cuatro redes mencionadas, en cuyo caso, como se muestra en la Figura 3.9, habría que instalar en los correspondientes armarios de cableado switches independientes e interconectarlos entre sí por separado. Esto provoca una red compleja y muy cara, ya que en muchos casos habrá equipos subutilizados.

El problema que se presenta es simple, se desea tener redes aisladas, a nivel de enlace, para los cuatro grupos de trabajo mencionados. La solución es sencilla si se dispone de espacios físicos contiguos para todos los miembros de un mismo grupo, como por ejemplo un edificio o piso para administración, otro para alumnos, etc. Pero, generalmente esto no sucede y existe una mezcla de usuarios en un mismo edificio y/o piso. La solución pasará entonces por la mencionada opción de tener por cada piso y/o edificio un switch para cada grupo de trabajo, con el fin de nunca mezclar los tráficos, y lograr la conectividad entre las cuatro LAN usando un router de cuatro interfases que permita comunicarlas a un nivel superior (nivel de red).

La solución actual a este problema es la creación de redes locales virtuales, o VLANs. Las VLANs son una forma de realizar una partición lógica de un switch en otros más pequeños, de forma que aunque se trata de un solo equipo, se dividen los puertos en grupos que son completamente independientes entre sí como se muestra en la Figura 3.10. Un switch que tiene la capacidad de generar VLANs se puede considerar como un switch que, por software, se convertirá en tantos switches como VLANs se creen, es decir, si se crean las cuatro VLANs necesarias para el ejemplo en un switch, esto se puede ver como si se hubieran comprado cuatro switches y cada uno de ellos genera una LAN para cada grupo de trabajo, y los tráficos, a nivel de enlace, nunca se mezclarán entre las VLANs, pues la única forma de hacerlo es utilizando un router que comunique, a nivel de red, las cuatro VLANs generada. Un switch con capacidades de VLANs es entonces un generador de diversos dominios de broadcast. La funcionalidad o soporte de VLANs está disponible hoy en día en la mayoría de los switches del mercado.

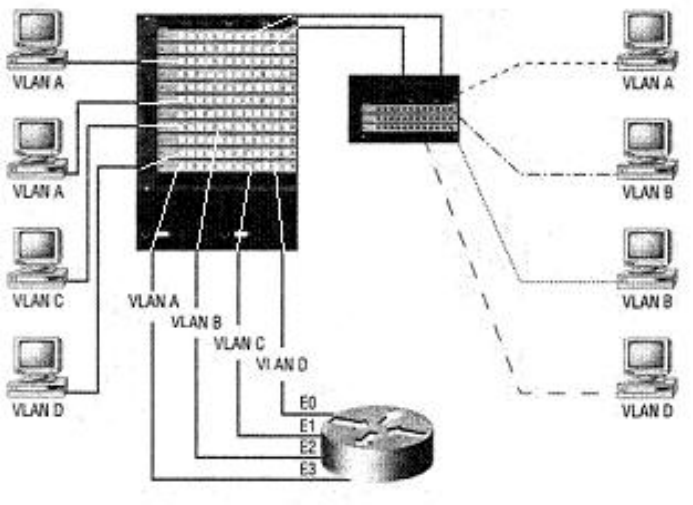


Figura 3.10 Asignación de puertos de uno mas switches a una VLAN

Suponiendo el caso anterior, en que se ha decidido dividir la red de campus en cuatro VLANs: I (de investigación), D (de docencia), E (de estudiantes) y A (de administración). Si se tiene un switch de 24 puertas en un closet de cableado y se plantea la necesidad de suministrar servicio a 8 equipos de la VLAN I, 4 de la D, 4 de la E y 4 de la A. Se podría asignar, por ejemplo, los puertos 1 a 8 a la VLAN I, 9 a 12 a la VLAN D, 13 a 16 a la VLAN E y 17 a 20 a la VLAN A, dejando los puertos 21 a 24 libres para futuras ampliaciones o para conectar las interfases de un router, etc. A partir de ese momento, el switch se

comportará como cuatro switches virtuales de 4 puertos cada uno, los correspondientes a las tres VLANs y un cuatro correspondiente a los puertos no asignados. De esta forma, se pueden asignar puertos a una u otra VLAN de forma flexible en función de las necesidades.

Queda por resolver aún la conexión de las cuatro VLANs con el resto de la red. Una posibilidad sería asignar los puertos 21 a 24 a cada una de las cuatro VLANs y conectarlas a cuatro interfases físicas diferentes del router como se muestra en la Figura 3.8. Aunque físicamente las cuatro VLANs comparten los switches, sigue habiendo cuatro redes separadas en el cableado, ya que nunca viajan por un mismo cable frames de VLANs diferentes. Cabe también pensar en un nivel adicional de optimización, en el que se compartiera un mismo cable para diferentes VLANs. Esto permitiría un ahorro considerable en el número de puertos consumidos mediante el uso de enlaces troncales, especialmente cuando se manejan muchas VLANs. Por ejemplo, se podría emplear sólo un puerto, por ejemplo el 21, para conectar las cuatro VLANs, liberando así los puertos 22 a 24 para otros usos. Esta situación se denomina configurar un enlace trunk o troncal. Debiera ser lógico entonces que los enlaces Trunk suelan ser de mayor capacidad que los puertos normales del switch ya que soportan un tráfico más elevado. Por ejemplo, en un switch de puertos a 10 Mbps el enlace trunk típicamente será de 100 Mbps y en uno con puertos de 100 Mbps será de Gigabit Ethernet.

Los enlaces Trunk, mostrados en la Figura 3.11, suponen un cambio importante en el funcionamiento de los switches, ya que al mezclar frames de diferentes VLANs por el mismo cable es preciso marcarlas o etiquetarlas de alguna manera a fin de poder entregarlas a la VLAN adecuada en el otro extremo. El marcado se hace añadiendo un campo nuevo en el header del frame MAC, lo que hace que el tamaño del frame Ethernet supere ligeramente la longitud máxima de 1500 bytes en algunos casos, ya que un switch puede recibir un frame de 1500 bytes y si lo ha de enviar por un enlace trunk tendrá que incorporarle la etiqueta correspondiente, pues en ningún caso está permitido fragmentar el frame original. Hoy en día existe un formato estándar para colocar las etiquetas de VLAN que es el conocido como IEEE 802.1q que es el que utilizan prácticamente la totalidad de los equipos actuales. De esta forma es posible diseñar complejas redes con VLANs utilizando equipos de diferentes fabricantes.

Una propiedad interesante de las VLANs es la posibilidad de configurar interfases virtuales en los hosts. Suponiendo que en el caso analizado con las cuatro VLANs, I, D, E y A, se tiene un servidor que se desea esté accesible de forma directa en las cuatro VLANs, de forma que cualquier host de cualquiera de las VLANs pueda acceder a él sin necesidad de pasar por un router. Una posible solución sería conectar al servidor mediante cuatro interfases de red y conectar cada una de ellas a un puerto del switch asignado a cada una de las VLANs. Cada interfaz recibiría una dirección de red correspondiente a la VLAN en la que se encuentra. Sin embargo, esta solución se hace inmanejable si aumenta el número de VLANs. Otra posibilidad, más interesante, sería configurar una interfaz de red del servidor como tres interfaces virtuales y conectarla a un puerto trunk del switch. Para esto se necesita disponer de drivers con soporte de IEEE 802.1q para la interfaz de red.

Las LAN se dividen cada vez más en grupos de trabajo formados por topologías VLAN. Las VLAN segmentan lógicamente la infraestructura física de una LAN en distintas

subredes (o dominios de broadcast), por lo que, las tramas de difusión sólo son conmutadas entre los puertos de la misma VLAN, sin embargo una VLAN puede abarcar varios segmentos de red.

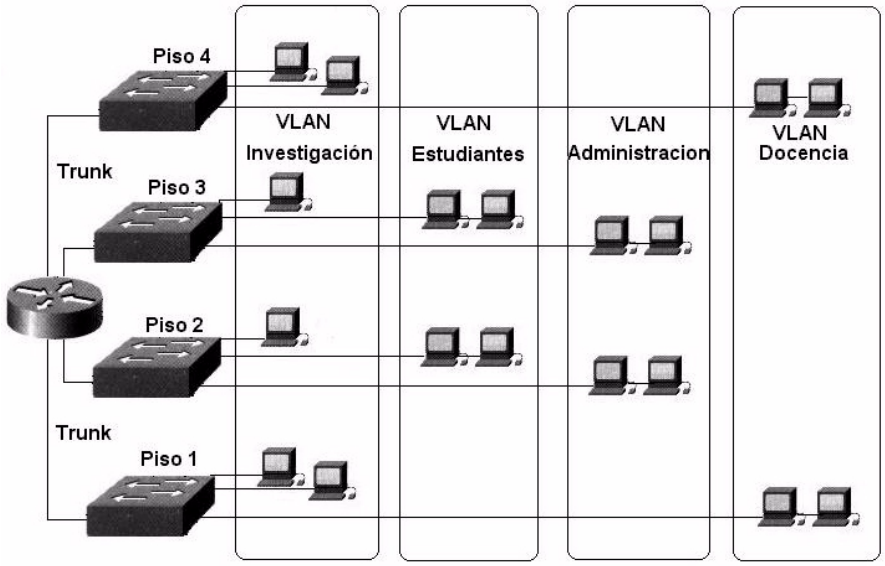


Figura 3.11 Organización usando VLANs y enlaces Trunk para los grupos de trabajo

Las implementaciones VLAN iniciales ofrecían una opción de asignación de puerto que establecía un dominio de broadcast entre un grupo de dispositivos predeterminado. Los requisitos de red actuales exigen una funcionalidad VLAN que cubra toda la red. Esta solución a las VLAN permite agrupar geográficamente usuarios separados en topologías virtuales de red.

En una LAN que utilice dispositivos de conmutación, la tecnología VLAN es una forma muy eficaz de agrupar usuarios en grupos de trabajo virtuales, independientemente de su ubicación física en la red. La Figura 3.12 muestra las diferencias entre la segmentación LAN tradicional y la segmentación VLAN. Algunas de estas diferencias son las siguientes:

- Las VLAN funcionan en las Capas 2 y 3 del modelo de referencia OSI.
- La comunicación entre VLAN la proporciona el enrutamiento de Capa 3.
- Las VLAN ofrecen un método de controlar las difusiones de red.
- El administrador de red asigna usuarios a una VLAN.
- Las VLAN pueden incrementar la seguridad de una red definiendo qué nodos de la red pueden comunicarse entre sí.

Por medio de la tecnología VLAN es posible agrupar puertos de switch y sus usuarios conectados, en grupos de trabajo definidos lógicamente, como los siguientes:

- Compañeros del mismo departamento.

- Un equipo de producto multidisciplinar.
- Distintos grupos de usuarios que comparten la misma aplicación o software de red.

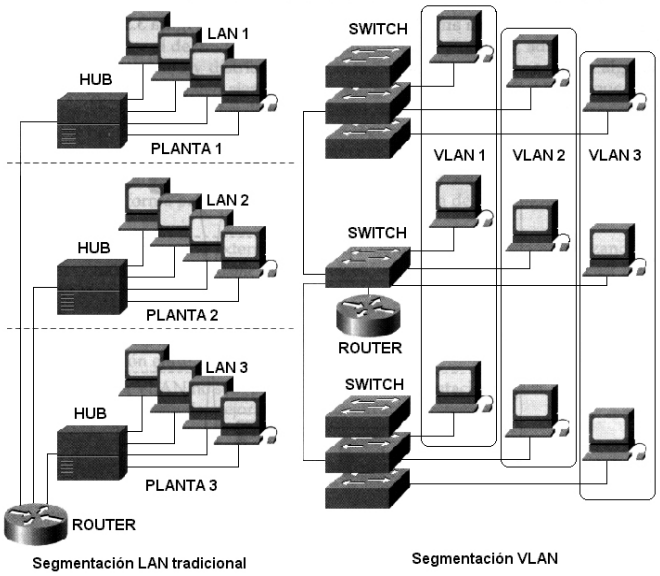


Figura 3.12 Diferencia entre Segmentación LAN y Segmentación VLAN.

Estos puertos y usuarios se pueden agrupar en grupos de trabajo de un solo switch o en varios switches Interconectados. Al agrupar puertos y usuarios en múltiples switches, las VLAN pueden abarcar infraestructuras de construcción individual, construcciones interconectadas o, incluso, redes de área amplia (WAN), como se ve en la Figura 3.13.

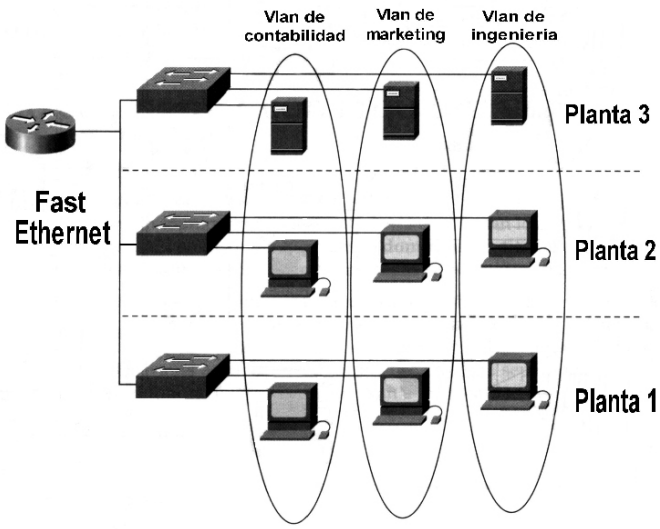


Figura 3.13 Red VLAN agrupadas por grupo de trabajo

3.4.1 Transporte de las VLAN a través de los backbones.

El backbone suele actuar como punto de encuentro de grandes volúmenes de tráfico.

También transporta información VLAN de los usuarios finales e identificación entre switches, routers y servidores conectados directamente. En el backbone, los enlaces de ancho de banda alto y de gran capacidad son los elegidos para transportar el tráfico de la empresa.

- **Los routers de las VLAN**

  El papel tradicional del router consiste en proporcionar firewalls, administración de la difusión y procesamiento y distribución de ruta. Si bien los switches asumen algunas de estas tareas, los routers siguen siendo vitales en las arquitecturas VLAN, ya que proporcionan rutas conectadas entre las distintas VLAN. También se conectan con otras partes de la red que, o bien están segmentadas de forma lógica con la solución de subred más tradicional, o bien requieren acceso a sitios remotos a través de enlaces de área amplia.

  La comunicación de Capa 3 que, o bien está incorporada en el switch, o bien es ofrecida externamente, forma parte integral de toda arquitectura de conmutación de alto rendimiento, ya que puede integrar routers externos en la arquitectura de conmutación utilizando una o más conexiones de backbone de alta velocidad. Suelen ser conexiones Fast Ethernet o ATM, y ofrecen ventajas al aumentar el rendimiento entre los switches y los routers.

  La arquitectura VLAN no sólo proporciona una segmentación lógica, además con una planificación cuidadosa, puede mejorar mucho la eficacia de una red.

3.5 CLASIFICACION DE LAS VLANs

Los problemas asociados con las LAN compartidas y la consolidación de los switches están haciendo que las configuraciones LAN tradicionales sean sustituidas por configuraciones de VLAN conmutada. Las configuraciones VLAN conmutadas se diferencias de las configuraciones LAN tradicionales en lo siguiente:

- Los switches eliminan las restricciones físicas impuestas por una arquitectura de hub compartido, ya que los usuarios y puertos de la empresa se agrupan lógicamente. Los switches sustituyen a los hubs en el recinto de cableado, se instalan fácilmente sin hacer prácticamente ningún cambio en el cableado, y pueden sustituir completamente a un hub compartido con servicio de puerto para cada usuario.

- Los switches pueden ser utilizados para crear VLAN con el fin de proporcionar servicios de segmentación (que suelen ser proporcionados por los routers en las configuraciones LAN tradicionales).

Los switches constituyen uno de los componentes centrales de las comunicaciones VLAN. Como se ve en la Figura 3.14, llevan a cabo funciones VLAN criticas, actuando como punto de entrada para los dispositivos finales en la red conmutada y para las comunicaciones de la empresa.

Todo switch tiene la inteligencia necesaria para filtrar y reenviar las decisiones por trama,

en base a la métrica VLAN definida por los administradores de la red. El switch también puede comunicar esta información a los demás switches y routers de la red.

Las soluciones más habituales para el agrupamiento lógico de los usuarios en VLAN distintas son el filtrado de trama y la identificación de trama. Ambas técnicas examinan la trama cuando se recibe o reenvía por el switch. En base al conjunto de reglas que defina el administrador, estas técnicas determinan dónde va a ser enviada, filtrada o difundida la trama. Estos mecanismos de control pueden administrarse centralmente (por medio de software de administración de redes) y se implementan fácilmente en la red.

El filtrado de trama examina la información concreta de cada trama. En cada switch se desarrolla una tabla de filtrado; esto proporciona un alto nivel de control administrativo, ya que se pueden examinar muchos atributos de cada trama. En función de la sofisticación del switch LAN, es posible agrupar a los usuarios en base a las direcciones MAC o el tipo de protocolo de la capa de red. El switch compara las tramas que filtra con las entradas de la tabla, y toma la acción oportuna en base a las entradas.

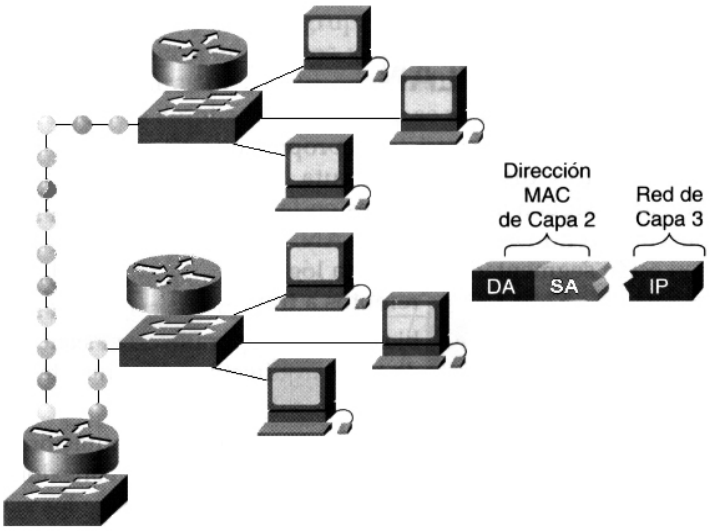


Figura 3.14 Puertos y direcciones lógicas

En sus primeros días, las VLAN estaban basadas en filtros y agrupaban a los usuarios en base a una tabla de filtrado. Este modelo no escalaba bien, ya que había que hacer referencia a cada trama con arreglo a una tabla de filtrado.

El etiquetado de trama VLAN es una solución que ha sido desarrollada específicamente para las comunicaciones conmutadas, y coloca un identificador único en la cabecera de cada trama cuando es reenviada por el backbone de red.

El identificador es entendido y examinado por cada switch, con antelación a las difusiones o transmisiones a otros switches, routers o dispositivos finales. Cuando la trama sale del backbone de red, el switch elimina el identificador antes de que se transmita la trama a la estación final de destino. La identificación de trama de Capa 2 requiere algo de procesamiento o estructura administrativa.

El etiquetado de trama asigna un ID de VLAN a cada trama. Esta técnica fue la elegida por el IEEE (Instituto de ingenieros eléctricos y electrónicos), debido a su escalabilidad. El etiquetado de trama está ganando aceptación como mecanismo normal de trunking (enlace troncal); en comparación con el filtrado de trama, puede proporcionar una solución más escalable al despliegue VLAN que puede implementarse en todo un campus. La IEEE 802.1q establece que el etiquetado de trama es la forma de implementar las VLAN.

Una VLAN conforma un red conmutada que está segmentada lógicamente por funciones, equipos de proyecto o aplicaciones, sin tener en cuenta la ubicación física de los usuarios. A continuación se examinan los métodos de implementación VLAN.

3.5.1 VLAN Estáticas

Las VLAN estáticas son puertos de un switch que se asignan estáticamente a una VLAN. Los puertos asignados a la misma VLAN comparten difusiones. Los puertos que no pertenezcan a esa VLAN no comparten estas difusiones. Con esto se mejora el rendimiento general de la red. Aunque las VLAN estáticas exigen que el administrador haga cambios, son seguras, fáciles de configurar y de controlar. Las VLAN estáticas funcionan bien en redes en las que se controlan y administran los movimientos.

- **VLAN de puerto central**

  En las VLAN de puerto central, a todos los nodos conectados a los puertos de la misma VLAN se les asigna el mismo ID de VLAN. La Figura 3.15 muestra la calidad de miembro de VLAN por puerto de router, lo cual facilita la tarea del administrador y hace que la red sea más eficaz, ya que los usuarios son asignados por puerto, las VLAN se administran más fácilmente, proporciona una mayor seguridad entre las VLAN y los paquetes no se filtran a otros dominios.

  En esta figura se puede ver la dirección 192.20.21.0 esta asignada a todos los nodos de la VLAN de Ingeniería, así como la dirección 192.20.24.0 esta asignada a los nodos de la VLAN marketing.

  - **Ventajas:**

    Facilidad de movimientos y cambios: Un movimiento supone que la estación cambia de ubicación física, pero sigue perteneciendo a la misma VLAN. Requiere reconfiguración del puerto al que se conecta la estación, salvo si se utilizan técnicas de asignación dinámica a VLAN. Un cambio implica pertenencia a una nueva VLAN sin movimiento físico.

    El puerto del switch ha de configurarse como perteneciente la nueva VLAN y la estación puede precisar reconfiguración, lo cual no será necesaria si la subred (IP, IPX, etc.) a la que pertenece está totalmente contenida en la VLAN. Cualquier operación de añadir, mover o cambiar un usuario se traduce normalmente en la reconfiguración de un puerto y algunas aplicaciones gráficas de gestión de VLANs automatizan totalmente está reasignación.

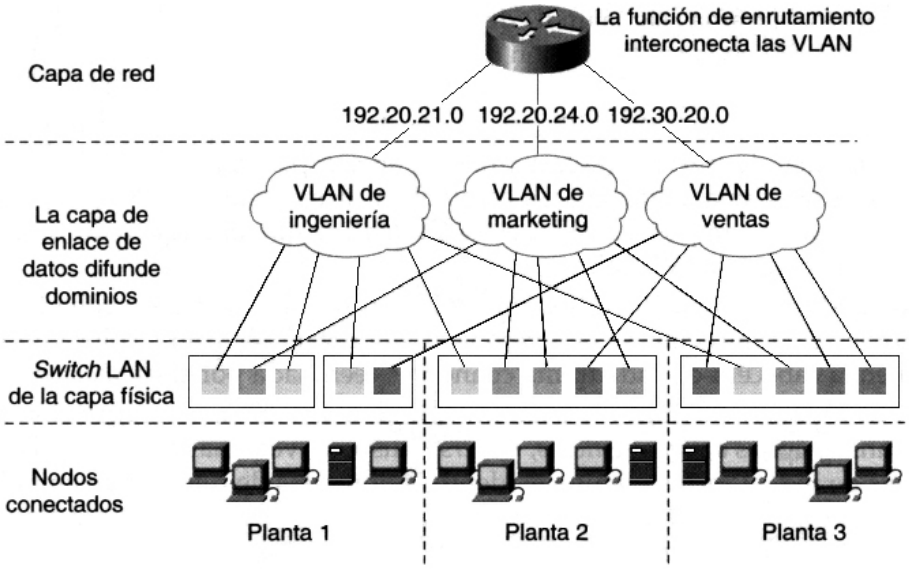


Figura 3.15 Redes VLAN de puerto central

Microsegmentación y reducción del dominio de broadcast: Aunque los switch permiten dividir la red en pequeños segmentos, el tráfico broadcast sigue afectando el rendimiento de las estaciones y se precisan routers o VLANs para aislar los dominios de broadcast. La definición de VLAN por puerto implica que el tráfico broadcast de una VLAN no afecta a las estaciones en el resto de las VLANs, puesto que es siempre interno a la VLAN en la que se origina.

Multiprotocolo: La definición de VLAN por puerto es totalmente independiente del protocolo o protocolos utilizados en las estaciones.

- **Desventajas:**

Administración: Los movimientos y cambios implican normalmente una reasignación del puerto del switch a la VLAN a la que pertenece el usuario. Aunque las aplicaciones de gestión facilitan esta tarea es recomendable combinar dichas aplicaciones con mecanismos de asignación dinámica de VLAN de forma que se asignan los puertos a la VLAN en función de la dirección MAC o de otros criterios como la dirección de nivel 3.

3.5.2 VLAN Dinámicas

Las VLAN dinámicas son puertos de un switch que pueden determinar automáticamente sus tareas VLAN. Las funciones VLAN dinámicas están basadas en el direccionamiento MAC, el direccionamiento lógico o el tipo de protocolo de los paquetes de datos.

Cuando una estación se conecta inicialmente a un puerto de switch no asignado, el switch apropiado comprueba la entrada de dirección MAC en la base de datos de administración VLAN y configura dinámicamente el puerto con la configuración VLAN correspondiente.

Las ventajas principales de esta solución son que hay una menor administración en el recinto de cableado cuando se añade o traslada un usuario y una notificación centralizada cuando se añade a la red un usuario no reconocido.

Normalmente, es necesario que haya más administración para configurar la base de datos dentro del software de administración de la VLAN y mantener una base de datos exacta de todos los usuarios de la red.

- **VLAN por dirección MAC**

  Se basa en direcciones MAC, por lo que se realiza un mapeo para que el usuario pertenezca a una determinada VLAN. Este tipo de VLAN ofrece mayores ventajas pero es complejo porque la pertenencia a la VLAN se basa en una tabla contenida en el switch que relaciona la dirección MAC del dispositivo y la VLAN asignada.

  - **Ventajas:**

    Facilidad de movimientos. Las estaciones pueden moverse a cualquier ubicación física perteneciendo a la misma VLAN sin que se necesite ninguna reconfiguración del switch.

    Multiprotocolo. No presenta ningún problema de compatibilidad con los diversos protocolos y soporta incluso la utilización de protocolos dinámicos tipo DHCP.

  - **Desventajas:**

    Problemas de rendimiento y control de broadcast. Este método de definición de VLAN implica que en cada puerto del conmutador coexisten miembros de distintas VLANs por lo que cualquier trafico de VLANs afecta al rendimiento de todas las estaciones. El trafico multicast y broadcast se propaga por todas las VLANs.

    Complejidad en la administración. Todos los usuarios deben configurarse inicialmente en una VLAN. El administrador de la red introduce de forma manual en la mayoría de los casos, todas las direcciones MAC de la red. Cualquier cambio o nuevo usuario precisa modificación de la base de datos. Todo ello puede complicarse en redes con gran numero de usuarios. Existen soluciones alternativas para automatizar esta definición y normalmente se utiliza un servidor de configuración de forma que las direcciones MAC se copian en las tablas de direcciones de los conmutadores a la base de datos del servidor.

- **VLAN por protocolo.**

  La asignación de las VLANs se basa en información de protocolos de red. La pertenencia a la VLAN se basa en la utilización de filtros que se aplican a las tramas para determinar su relación de pertenencia a la VLAN. Los filtros han de aplicarse por cada trama que entre por uno de sus puertos del switch.

- **Ventajas:**

  Segmentación por protocolo. Es el método apropiado solo en aquellas redes en las que el criterio de agrupación de usuarios este basado en el tipo de protocolo de nivel 3 y la segmentación física existente sea muy diferente a los patrones de direccionamiento.

  Asignación dinámica. Tanto la definición de VLANs por dirección MAC como por protocolo de nivel 3 ayuda a automatizar la configuración del puerto del switch en una VLAN determinada.

- **Desventajas:**

  El problema de rendimiento y control de broadcast. La utilización de VLANs de nivel 3 requiere búsquedas en las tablas de pertenencia que afectan el rendimiento global del switch. Los retardos de transmisión pueden aumentar en un 50 y un 80%. El problema de control de broadcast surge con las estaciones multiprotocolo o sistemas multistack (por ejemplo: estaciones con stacks TCP/IP, IPX y APPLE TALK) que pertenecen a tantas VLANs como protocolos utilizan por lo tanto recibirán todos los broadcast provenientes de las diversas VLANs en las que están incluidas .

  No soportan protocolos de nivel 2 ni protocolos dinámicos. La estación necesita una dirección de nivel 3 para que el switch la asigne a una VLAN. Las estaciones que utilicen protocolos de nivel 2 como Net Bios y LAT no podrán asignarse a una VLAN. Si existen protocolos dinámicos como DHCP y la estación de trabajo no tiene configurada su dirección IP ni su router por defecto el switch no podrá clasificar la estación de trabajo dentro de una VLAN.

Una premisa esencial en la definición de VLAN es que el rendimiento del switch no debe degradarse debido a la existencia de VLAN. Las técnicas de marcado (identificación de paquetes pertenecientes a cada VLAN) utilizadas en la definición de VLAN por puerto permite mantener una velocidad de transmisión según el ancho de banda disponible y por ello a prevalecido dicha solución en la definición del estándar 802.1Q . Esta técnica permiten además la asignación de un mismo puerto o tarjeta de red a varias VLANs (routers o servidores pueden aprovechar esta ventaja evitándose la utilización de tantas interfaces o tarjetas de red como VLANs).

ISL(Inter Switch Link) para interfase Token Ring y 82.10 para FDI son dos técnicas de marcado. El ISL es un protocolo no propietario de CISCO que se utiliza para interconectar múltiples switches, conservando al información de trafico que pasa a través de una VLAN entre los switches Esta tecnología es muy parecida al 802.10 y se define solo en fast ethernet.

3.6 PALABRAS CLAVES

REDES VIRTUALES DE AREA LOCAL (VLANs)
SEGMENTACIÓN

SEGMENTACIÓN CON PUENTES
SEGMENTACIÓN CON ROUTERS
SEGMENTACIÓN CON SWITCHES LAN
CONMUTACIÓN
CONMUTACIÓN CON SWITCHES
CONMUTACIÓN CON ROUTERS
CONMUTACIÓN SIMÉTRICA
CONMUTACIÓN ASIMÉTRICA
ENLACES TRUNK
VLAN ESTÁTICAS
VLAN DINÁMICAS
VLAN POR PUERTO CENTRAL
VLAN POR DIRECCIÓN MAC
VLAN POR PROTOCOLO

Principios de configuración y aplicaciones de VLANs

Capítulo

4

4. PRINCIPIOS DE CONFIGURACIÓN Y APLICACIONES DE VLANs

Hoy en día existen una gran cantidad de compañías fabricantes de switches, entre los más importantes se encuentran 3Com, CISCO, DELL, e INTEL por citar algunas. Para mostrar el funcionamiento y configuración de una VLAN, se utilizará el switch Ethernet Catalyst 1900 de CISCO, por lo cual conoceremos sus componentes claves e introduciremos otros aspectos funcionales que influyen en su entorno.

4.1 CONSECUENCIAS DEL USO DE SWITCHES

Los switches Ethernet operan en la capa 2 del modelo OSI y proporcionan las siguientes funcionalidades:

- Un switch Ethernet **aprende las direcciones MAC** de los dispositivos conectados a cada uno de sus puertos, estas direcciones son almacenadas en una tabla de direcciones MAC la cual se utiliza para rastrear las ubicaciones de los dispositivos conectados (Figura 4.1).

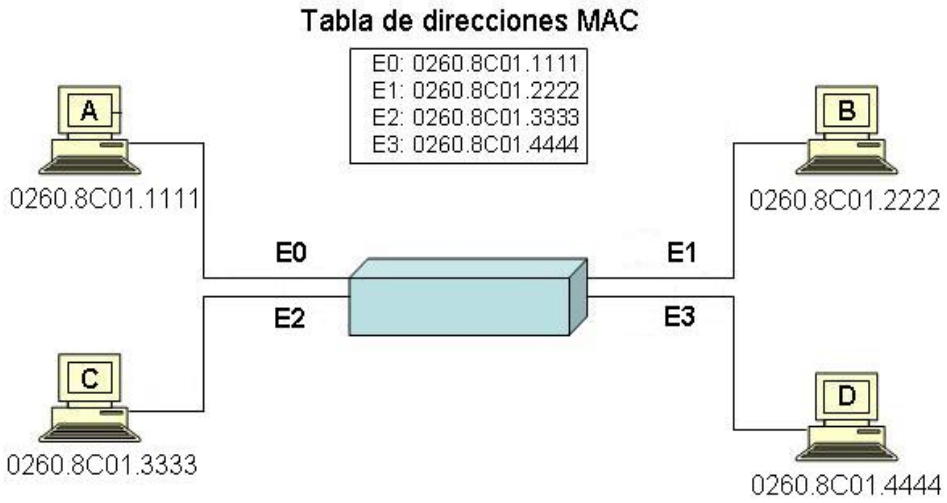


Figura 4.1 Tabla de direcciones MAC

Inicialmente, cuando enciende el switch, la tabla de direcciones MAC esta vacía, con una tabla de direcciones MAC vacía no hay filtrado de direcciones, por lo que el switch envía cada frame a todos los puertos, este proceso de enviar un frame a todos los puertos conectados, es llamado desbordamiento o inundación (flooding); la inundación es la manera menos eficiente para transmitir datos ya que se desperdicia ancho de banda.

- Cuando un switch Ethernet recibe un frame, este consulta su tabla de direciones MAC para determinar en que puerto puede alcanzar el dispositivo identificado como el destino del frame. Si la dirección es encontrada, el frame es retransmitido solamente hacia ese puerto, esto es conocido como **filtrado de frames**.
  Para el ejemplo mostrado en la Figura 4.2, si la estación A envía un frame a la estación C, cuando la dirección MAC de la estación C existe en la tabla de

direcciones MAC, el switch retransmite el frame solamente hacia el puerto indicado.

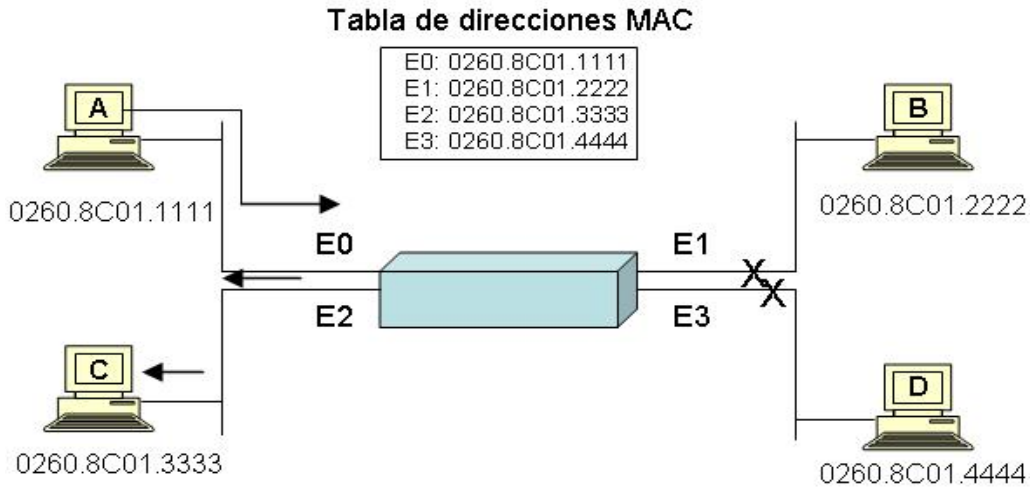


Figura 4.2 Transmisión de paquete por dirección MAC

Cuando el frame llega al switch, la dirección MAC de destino 0260.8C01.3333, es comparada con las entradas de la tabla de direcciones MAC, si el switch determina que la dirección MAC destino puede ser alcanzada a través de alguno de los puertos, E2 en este caso, retransmite el frame solamente hacia este puerto, el switch no retransmite el frame a los puertos E1 o E3 con lo que preserva el ancho de banda en estos enlaces.

Cabe mencionar que los frames de broadcast y multicast constituyen un caso especial. Puesto que los frames de broadcast y multcast pueden ser de interés a todas las estaciones, el switch normalmente difunde estos frames a todos los puertos.

- Las redes Ethernet son diseñadas comúnmente con enlaces y dispositivos redundantes, como se muestra en la Figura 4.3, una **topología redundante** permite establecer un enlace principal y un enlace de respaldo para todos los switches de la red, con lo que se eliminan los puntos de falla únicos que pueden resultar en la perdida de la funcionalidad total de la red.

  Mientras los diseños redundantes eliminan el problema de tener un solo punto de falla, introducen otros que deben tomarse en cuenta y que se trataran a continuación.

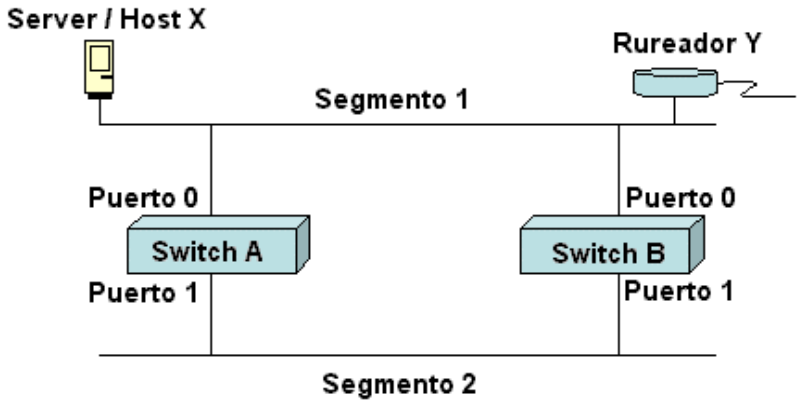


Figura 4.3 Topología redundante

- **Tormentas de broadcast**

  Este problema tiene lugar por que los switches inundan o desbordan los frames de broadcast hacia todos los puertos excepto en el que fue recibido el frame. Una tormenta de broadcast puede rápidamente obstruir la red con tráfico innecesario y evitar el switcheo de paquetes.

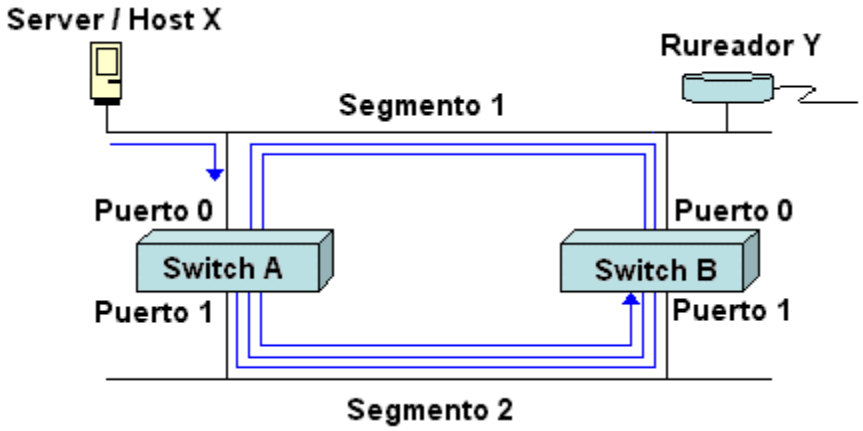


Figura 4.4 Tormenta de broadcast

De la figura 4.4 podemos observar que cuando el host X envía un frame de broadcast, por ejemplo un ARP por su default gateway hacia el ruteador Y, el frame será recibido por el switch A, el switch A examina el campo de la dirección destino en el frame y determina que el frame debe ser desbordado hacia la parte baja del enlace Ethernet (segmento 2).

Cuando esta copia del frame llega al switch B, el proceso se repite y una copia del frame es transmitida hacia la parte alta de la red (segmento 1).

Puesto que la copia original del frame llega al switch B via la parte alta del segmento 1, estos frames viajan alrededor del loop en ambas direcciones aun

después de que la estación destino ha recibido una copia del frame.

Una solución para evitar los loops podría eliminar este problema previniendo que una de las cuatros interfases transmita o reciba frames durante la operación normal.

- **Mútiples copias de frame.**

Otro problema que surge a causa del uso de topologías redundantes es que muchos protocolos están diseñados de modo que no se pueden enfrentar con las transmisiones duplicadas. En general, los protocolos que hacen uso de un mecanismo de secuenciación numérica asumirán que muchas transmisiones han fallado y el número de secuencia se ha reciclado. Otros protocolos intentarán manejar la transmisión duplicada hacia el protocolo apropiado de capa superior con resultados impredecibles. Para ver como pueden ocurrir transmisiones múltiples consideremos la Figura 4.5.

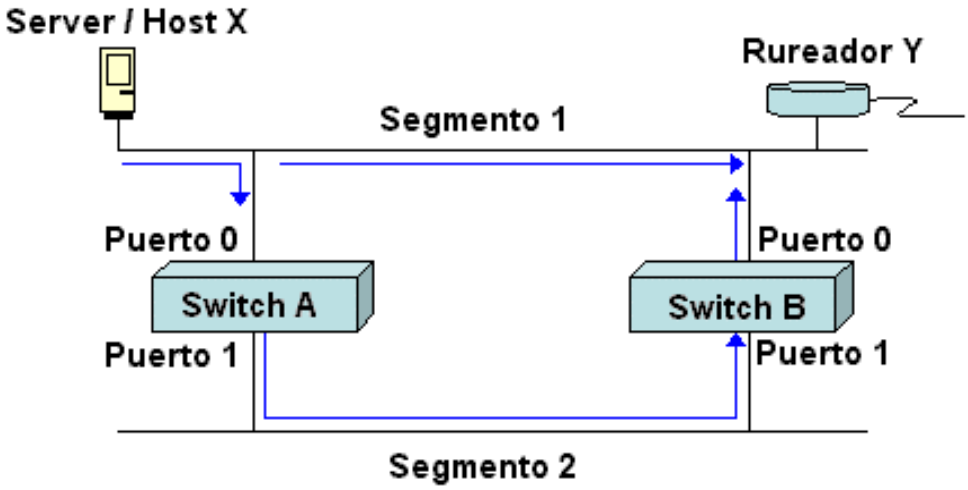


Figura 4.5 Transmisión múltiple

Cuando un host X envía un frame unicast hacia el ruteador Y, una copia es recibida sobre la conexión ethernet directa (segmento 1), mientras que al mismo tiempo el switch A recibe una copia y pone este dentro de sus buffers.

Si el switch A examina el campo de dirección destino en el frame y encuentra que no hay entrada en la tabla de direcciones MAC para el ruteador Y, el switch A desborda el frame hacia todos los puertos excepto por el puerto que lo origina, en este caso, es desbordaos hacia el segmento 2, cuando el switch B recibe una copia del frame también transmite una copia del frame dentro del segmento 1 si no hay entrada en la tabla de direcciones MAC para el ruteador Y, como resultado de este proceso, el ruteador Y recibe una copia del mismo frame por segunda vez.

Nuevamente, una solución para evitar los loops podría eliminar este problema

previniendo que una de las cuatros interfases transmita o reciba frames durante la operación normal.

- **Inestabilidad en la base de datos MAC**

  Un tercer problema relacionado con las topologías redundantes es la inestabilidad de la base de datos o tabla MAC que resulta cuando múltiples copias de un frame llegan en diferentes puertos de un switch. En la figura 4.6 el switch B instala un mapeo entre el host X y el puerto 0 hacia el segmento 1 cuando el primer frame llega. Algún tiempo mas tarde, cuando la copia del frame transmitido a través del switch A llega, el switch B debe remover la primera entrada e instalar una que mapea la dirección MAC del host X hacia el puerto 1 en el segmento 2. Dependiendo de la arquitectura interna del switch en cuestión, podrá o no enfrentar los rápidos cambios en su base de datos MAC.

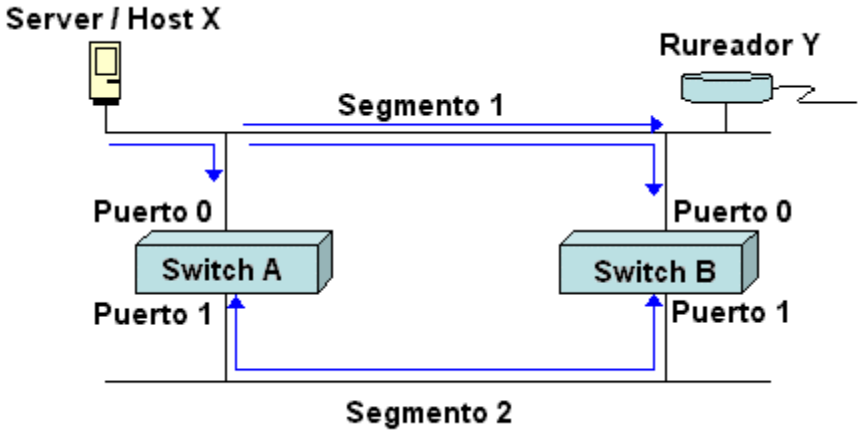


Figura 4.6 Inestabilidad en la base de datos MAC

- **Problemas múltiples de loops**

  Una larga y compleja red de switches con enlaces redundantes puede causar múltiples loops. (Figura 4.7), un loop puede existir dentro de otro loop.

  Protocolos de capa 2 como Ethernet carecen de un mecanismo para reconocer y eliminar los paquetes en un loop sin fin. Algunos protocolos de capa 3 implementan un mecanismo llamado TTL (Time To Live) que limita el número de veces que un paquete puede ser retransmitido por el dispositivo de red de capa 3. A falta de tal mecanismo, los dispositivos de capa 2 continuarán retransmitiendo tráfico en loop de forma indefinida.

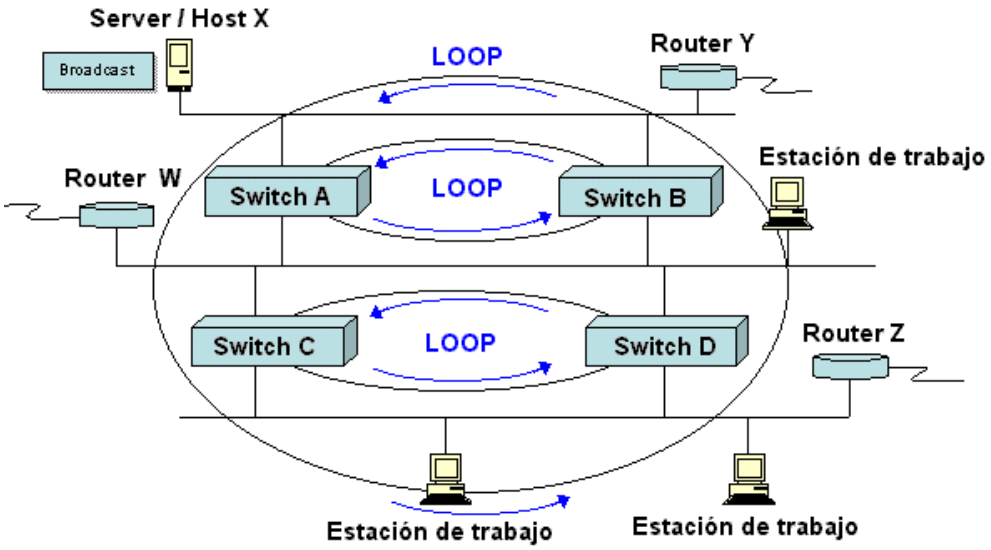


Figura 4.7 Múltiples Loops

Cuando una red de switches incluye loops por redundancia o forma una topología redundante, un swicth Ethernet puede prevenir que frames duplicados viajen sobre trayectorias redundantes mediante la configuración del protocolo spanning tree, el cual se trata a continuación.

4.1.1 Protocolo Spanning-Tree (STP)

Debido a la problemática que se presenta por loops dentro de una red de switches con topología redundante, el protocolo Spanning-Tree permite tener una topología redundante libre de loops, colocando ciertos puertos en estado de bloqueo como se muestra en la Figura 4.8.

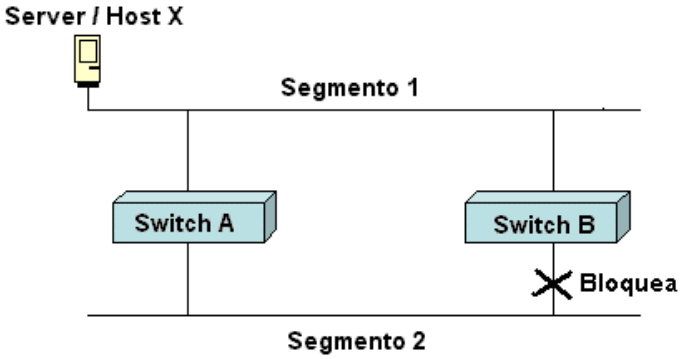


Figura 4.8 Puertos en estado de bloqueo

El problema de los loops fue resuelto por el comité 802 del IEEE en el estándar 802.1d con un algoritmo inteligente conocido como protocolo de árbol de extensión (Spanning Tree Protocol o STP). El STP se basa en la teoría de grafos y convierte un lazo cerrado en una topología de árbol, deshabilitando algunos enlaces. Esta acción asegura que

existirá una única ruta entre dos switches.

El propósito del STP es mantener una red libre de loops esto se logra cuando un dispositivo reconoce un loop en la topología y bloquea uno o mas puertos redundantes.

El STP continuamente explora la red por lo que una falla o la adición de un nuevo enlace en el switch es descubierta rápidamente. Cuando la topología de red cambia, el STP reconfigura los puertos del switch para evitar la perdida de conectividad o la creación de nuevos loops. El STP esta habilitado por default en los switches Catalyst de la serie 1900.

Operaciones Spanning-Tree

El protocolo Spanning-Tree convierte una topología de red con loops (Figura 4.9-a) en una topología de red libre de loops (Figura 4.9-b), mediante las siguientes operaciones:

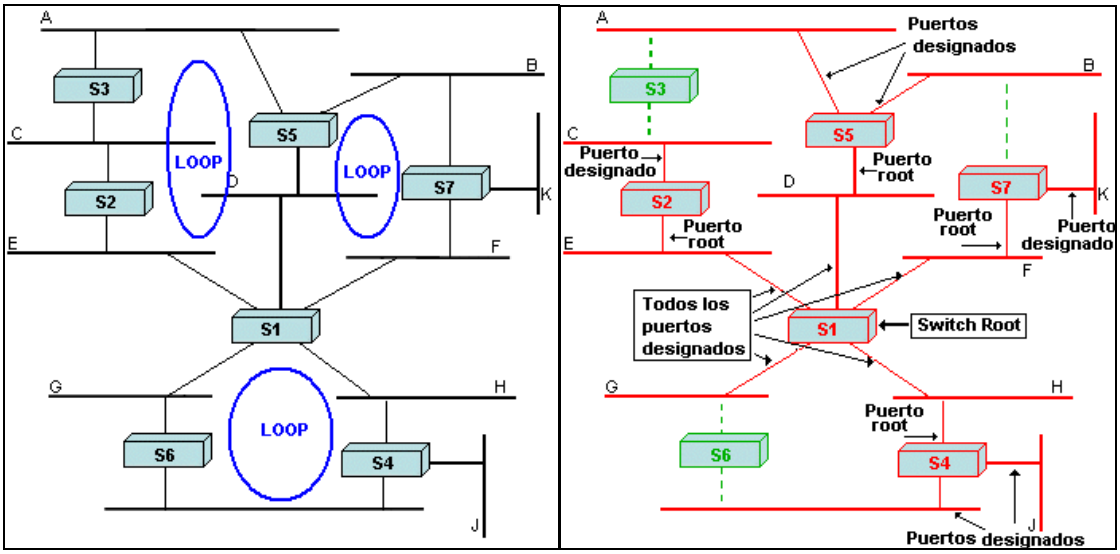


Figura 4.9 a y b Protocolo Spanning-Tree

- **Selección del switch Root**

  Los switches que ejecutan el algoritmo de Spanning-Tree intercambian mensajes de configuración con otros switches a intervalos de tiempo regulares usando un frame multicast llamado BPDU (Bridge Protocol Data Unit). Una de las piezas de información incluida en el BPDU es el Bridge ID. El Spanning Tree le asigna a cada switch un identificador único (Bridge ID).

  Típicamente, el Bridge ID esta formado por una prioridad (2 bytes) mas la dirección MAC (6 bytes) del switch. La prioridad por default según el estándar IEEE 802.1d, es 32768, el valor de rango medio. El switch root es el switch con menor Bridge ID. Cada switch selecciona una de sus direcciones MAC para usarse como Bridge ID en el Spanning-Tree. Un switch con múltiples VLANs usa un incremento de su dirección MAC base para cada VLAN.

- **Costo de trayectoria**

  El costo de trayectoria en el Spanning-Tree es un costo de trayectoria total acumulado basado en los anchos de banda de todos los enlaces de la trayectoria. En la tabla 4.1 se muestran algunos de los costos de trayectoria especificados en el estándar IEEE 802.1d.

Velocidad de enlace	Costo (re-ratificado IEEE spec)	Costo (re-ratificado IEEE spec)
10Gbps	2	1
1Gbps	4	1
100Mbps	19	10
10Mbps	100	100

Tabla 4.1 Costos de trayectoria

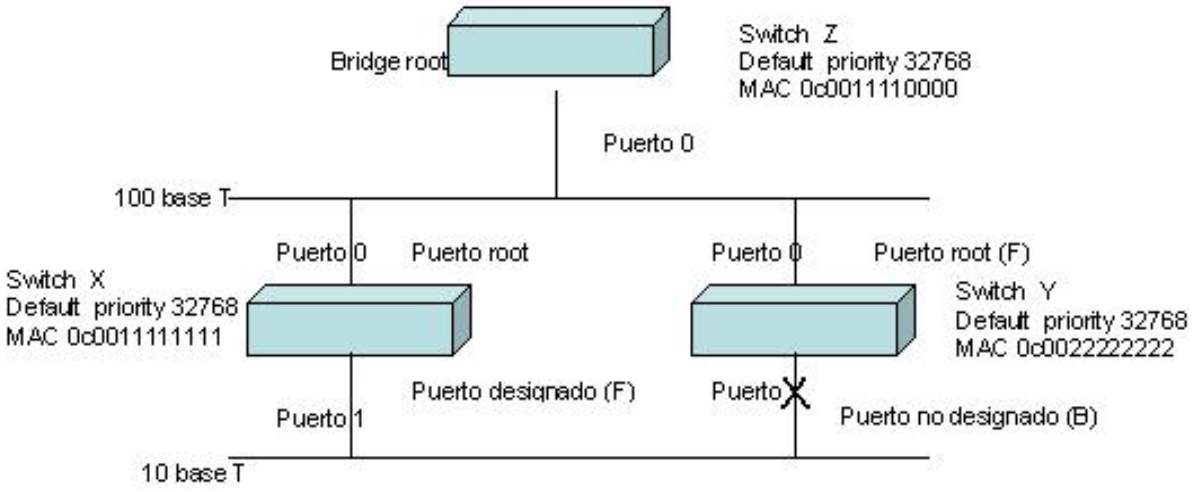


Figura 4.10 Spanning Tree

Como un ejemplo, consideremos la figura 4.10, en la cual el Bridge root es el switch Z, ya que tiene el menor Bridge ID, el puerto root es el Puerto 0 del switch X y Y, pues esta es la trayectoria de menor costo, el puerto designado es el puerto 0 del switch Z. Todos los puertos en el switch root son puertos designados.

El puerto 1 del switch X es un puerto designado puesto que ambos switches X y Y tienen el mismo costo de trayectoria hacia el Bridge root, el puerto designado es seleccionado para estar en el switch X porque este tiene el menor Bridge ID.

El puerto 1 del switch Y esta en estado Blocking ya que es el puerto no designado en el segmento y todos los puertos designados y los puertos root, están en estado forwarding.

- **Estados de los puertos en Spanning-Tree**

  Como ya se menciono, durante la operación normal un puerto esta en estado forwarding o blocking. Los puertos forwarding proporcionan la trayectoria de menor costo hacia el switch root, pero ocurren también dos estados transitorios cuando un dispositivo reconoce un cambio en la topología de la red, durante un cambio en la topología, un puerto temporalmente implementa los estados listening y learning; la duración y secuencia de dichos estados se muestra en la Figura 4.11.

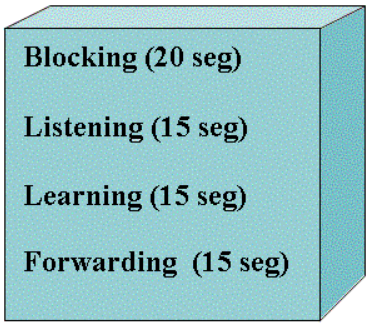


Figura 4.11 Estados de los puertos en el Spanning Tree

Todos los puertos inician en estado blocking para prevenir loops. El puerto permanece en estado bloqueado si el Spanning-Tree determina que hay otra trayectoria hacia el Switch root que tiene un menor costo. Los puertos blocking aun pueden recibir BPDUs.

Cuando el puerto esta en el estado de transición listening, es capaz de checar BPDUs, este estado es usado para indicar que el puerto esta escuchando todos los frames.

Cuando el puerto esta en estado learning, es capaz de modificar su tabla de direcciones MAC con base en las direcciones MAC escuchadas, pero no transmite frames.

En el estado forwarding, el puerto es capaz de enviar y recibir frames. El tiempo normal que toma al puerto para transitar del estado blocking al forwarding es 50 segundos aproximadamente. El tiempo que toma un puerto para transitar del estado listening al estado learning o del estado learning al estado forwarding es llamado retardo de transmisión (forward delay).

Re-cálculo del Spanning-Tree

Cuando hay un cambio topológico debido a la falla de un enlace o de un switch, el protocolo Spanning-Tree reajusta la topología de red para asegurar la conectividad colocando los puerto bloqueados en estado forwarding.

En la figura 4.12, si el Switch X (el bridge root) falla, el switch Y detectará el BPDU perdido proveniente del bridge root. Los temporizadores del Spanning-Tree son para

ajustar el tiempo y normalmente deben ajustarse al valor por default, uno de estos temporizadores es llamado MAXAGE. Cuando el temporizador MAXAGE expira y un nuevo BPDU no ha sido recibido del switch vecino, se inicia el re-calculo Spanning-Tree.

Después que la red ha convergido, el Switch Y se convierte en el Bridge root y transmite el trafico entre los dos segmentos cuando sus puertos transitan hacia los estados de forwarding.

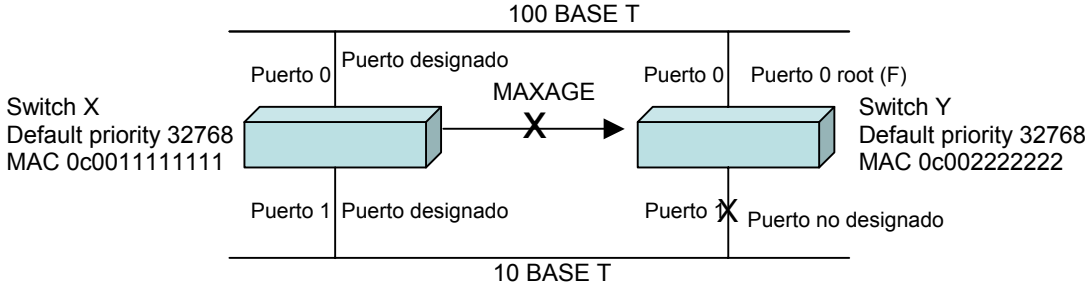


Figura 4.12 Spanning Tree recálculo

La convergencia es necesaria para la operación normal, en una red de switches un problema clave es el porcentaje de tiempo requerido para la convergencia cuando la topología de red cambia. La convergencia en el protocolo de Spanning-Tree significa un estado donde todos los puerto de switches han transitado al estado forwarding o blocking.

Una convergencia rápida es una característica de red deseable ya que esto reduce el periodo de tiempo que los switches tienen puertos en estados de transición y por lo tanto no envían trafico. Cuando la topología de la red cambia los switches deben re-calcular el protocolo Spanning-Tree, lo cual rompe el tráfico de usuario.

4.1.2 Operación VLAN (LAN Virtual)

La LAN virtuales (VLANs) permiten a un grupo de usuarios compartir un dominio de broadcast común independientemente de su localización física en la red (Figura 4.13). La creación de VLANs mejora el desempeño y la seguridad en una red switcheada mediante el control de la propagación de broadcast.

Una VLAN es un dominio de broadcast lógico que puede abarcar múltiples segmentos de LAN físicos. Una VLAN puede ser utilizada para proporcionar a las estaciones una segmentación lógica por funciones, equipos de proyecto o aplicaciones sin tener en cuenta la ubicación física de los usuarios. Cada puerto de switch puede ser asignado únicamente a una VLAN, los puertos en una VLAN comparten los broadcast, los puertos que no pertenecen a la misma VLAN no comparten los broadcast, esto mejora el desempeño global de la red.

Dentro de una interconectividad de switches, las VLANs proporcionan segmentación y flexibilidad organizacional. Usando tecnología VLAN, se pueden agrupar puertos de uno o más switches y sus usuarios conectados dentro de comunidades definidas lógicamente, tales como, colaboradores en el mismo departamento, equipo de producto o grupos de usuarios compartiendo la misma aplicación de red.

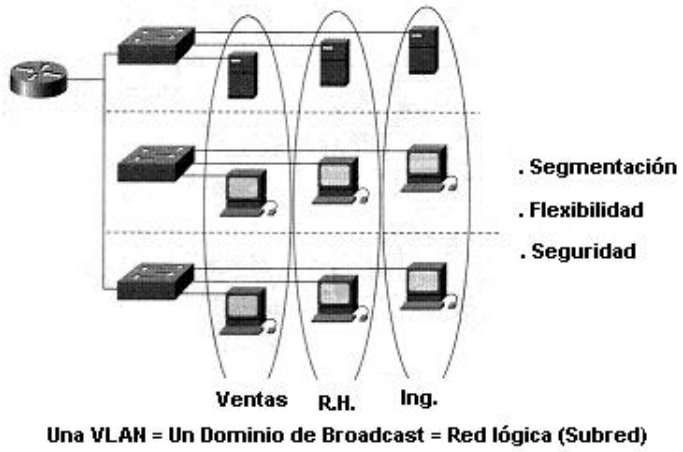


Figura 4.13 Vista global de una VLAN

Una VLAN puede existir en un solo switch o abarcar múltiples switches. Las VLANs pueden incluir estaciones en mismo edificio o infraestructuras de múltiples edificios, e incluso pueden conectarse a través de WANs.

En un switch Catalyst, cada VLAN configurada implementa un aprendizaje de direcciones, decisiones de transmisión/Filtraje y mecanismos para evitar loops.

Internamente, el switch Catalyst implementa VLANs restringiendo la transmisión de datos hacia puertos destino en la misma VLAN que los puertos de origen, esto es, cuando un frame llega en un puerto del switch, el Catalyst debe re-transmitir el frame solamente hacia un puerto que pertenece a la misma VLAN, la implicación es que una VLAN operando en un switch Catalyst limita la transmisión de tráfico de unicast, multicast y broadcast. El tráfico de origen desbordado desde una VLAN particular solamente se desbordará hacia los puertos que pertenecen a dicha VLAN.

Normalmente, un puerto solo transporta tráfico de la VLAN a la cual pertenece, para que una VLAN abarque a múltiples switches, se requiere una troncal o trunk para conectar dos switches juntos; una trocal puede transportar tráfico de múltiples VLANs. Un puerto de troncal puede ser configurado en puertos Fast Ethernet en los switches Catalyst 1900.

Los puertos que pertenecen a una VLAN son configurados en modo membership (membresía) que determina a cual VLAN pertenece (Figura 4.14) estos modos son:

- Static: La asignación de la VLAN hacia el puerto es estáticamente configurado por un administrador.

- Dynamic: El Catalyst 1900 soporta VLANs dinámicas usando VPMS (VLAN membership policy server), este switch no puede operar como VPMS. Un VPMS contiene una base de datos que mapea direcciones MAC a una asignación de VLAN. Cuando un frame llega a un puerto dinámico en el Catalyst 1900 este pregunta al VPMS por la signación de VLANs basándose en la dirección MAC fuente del frame que está llegando.

Un puerto dinámico puede solamente pertenecer a una sola VLAN, pero pueden estar activos múltiples host en un puerto dinámico solo si pertenecen a la misma VLAN.

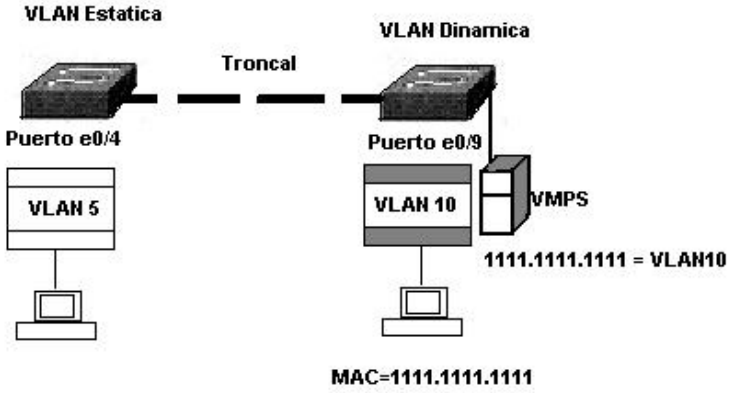


Figura 4.14 Modos de membresía

4.1.3 Inter-Switch Link (ISL)

ISL, es un protocolo propietario de Cisco para interconectar múltiples switches y para el mantenimiento de información VLAN como trafico que viaja entre switches.

El ISL frame tagging usado por los switches de la serie Catalyst es un mecanismo de baja latencia para multiplexar tráfico desde múltiples VLAN en una sola trayectoria física. Este protocolo ha sido implementado para la conexión entre switches, ruteadores y tarjetas de interfase de red usadas en nodos tales como servidores. Para soportar ISL, cada dispositivo conectado debe contar con esta capacidad. Un ruteador que es configurado para ISL es usado para permitir una comunicación entre VLANs. Un dispositivo no ISL que recibe los frames Ethernet encapsulados, puede considerarlos como errores de protocolo si el tamaño del encabezado mas el frame de datos excede el tamaño del MTU.

ISL funciona en la capa 2 encapsulando el frame de datos con un nuevo encabezado y CRC (Cyclic Redundancy Cheek), es un protocolo independiente del frame de datos que puede transportar cualquier protocolo de capa superior.

Encapsulamiento ISL

Los puertos configurados como tróncales ISL, encapsulan cada frame con un encabezado de 26 bytes (Figura 4.15) donde viene una identificación de la VLAN a la que pertenece y también se adiciona al final un segundo campo de chequeo de frame (CRC de 4 bytes) antes de enviarlo hacia fuera de la troncal. Puesto que la tecnología ISL esta implementada el ASICs, los frames son etiquetados a velocidad del alambre. El número de VLANs soportadas por un switch depende del hardware del switch. El Catalyst 1900 soporta 64 VLANs con una instancia separada de Spanning-Tree por VLAN.

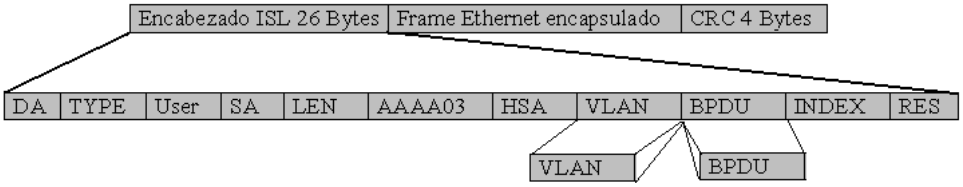


Figura 4.15 Encapsulamiento ISL

El encabezado del frame ISL contiene la siguiente información de los campos

- **DA**: Dirección de destino multicast de 48 bits.
- **Type:** Descriptor de 4 bits de los tipos de frame encapsulado: Ethernet (0000), Token Ring (0001), FDDI (0010), y ATM (0011).
- **User:** Descriptor de 4 bits como extensión del campo Type o para definir prioridades Ethernet, la prioridad mas baja es un valor binario de 0, y 3 la mas alta.
- **SA:** Dirección MAC fuente de 48 bits del switch Catalyst transmitiendo.
- **LEN:** Descriptor de 16 bits de longitud de frame menos DA, type, user, SA, LEN y CRC.
- **AAAA03:** Encabezado estándar SNAP 802.2 LLC.
- **HSA:** Primeros 3 bytes de SA (ID del fabricante o ID único organizacional).
- **VLAN ID:** 15 bits de VLAN ID. Solamente los 10 bits mas bajos son usados para 1024 VLANs.
- **BPDU:** Descriptor de 1 bit que identifica si el frame es un spanning-tree. Este también es ajustado si el frame encapsulado es un frame CDP**.**
- **INDEX:** Descriptor de 16 bits que identifica el ID del puerto transmitiendo. Usado para diagnostico.
- **RES:** Campo reservado de 16 bits usado para información adicional tal como el campo FC de un frame FDI.

4.1.6 VTP (VLAN Trunking Protocol)

Es un protocolo usado para distribuir y sincronizar información de identificación acerca de las VLANs configuradas a través de una red switcheada. Las configuraciones hechas hacia un solo servidor VTP son propagados a través de los enlaces hacia todos los switches conectados en la red (Figura 4.16). VTP permite a la red switcheada escalar a tamaños mayores mediante la reducción manual de configuraciones necesarias en la red.

VTP es un protocolo de mensajería de capa 2 que mantiene la consistencia de la configuración VLAN mediante el manejo de adiciones, borrados y cambio de nombres de las VLANS a través de las redes, también minimiza las fallas e inconsistencias de configuración que pueden causar problemas, tales como, nombres duplicados de VLANs o especificaciones incorrectas del tipo de VLAN.

Un dominio VTP es uno o varios switches interconectados compartiendo el mismo ambiente, un switch puede estar solamente en un dominio VTP

Por default, un switch Catalyst esta en un estado dominio-no-administración hasta que este recibe un anuncio para un dominio sobre un enlace troncal o hasta que se configura un dominio de administración. VTP opera en uno de tres modos: modo servidor, modo cliente y modo transparente. El modo VTP por default es modo servidor pero las VLANs no son propagadas sobre la red hasta que el nombre de un dominio de administración es especificado o aprendido.

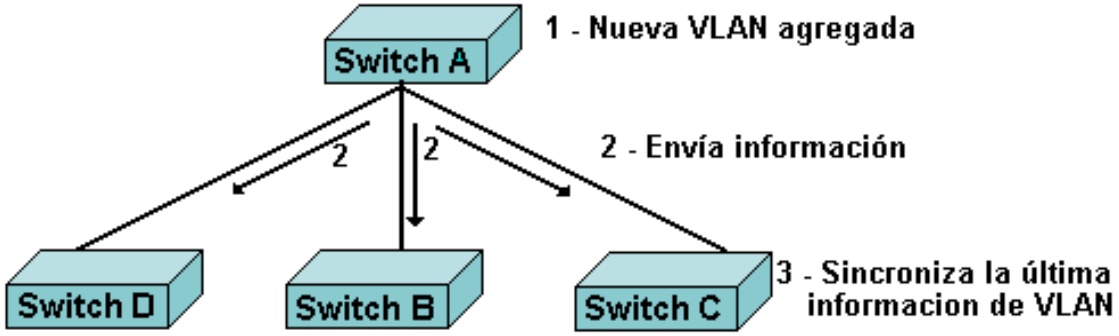


Figura 4.16 VLAN Trunking Protocol

Modos VTP

Un switch Catalyst operando en modo VTP servidor puede crear, modificar y borrar VLANs y otros parámetros de configuracion para el dominio VTP completo (Figura 4.17). En este modo las configuraciones VLAN son guardadas en la memoria no volátil del switch, cuando se hace un cambio a la configuración de una VLAN en el modo VTP servidor, el cambio es propagado a todos los switches en el dominio. Mensajes VTP son transmitidos hacia todas las conexiones tróncales (trunk) tales como ISL.

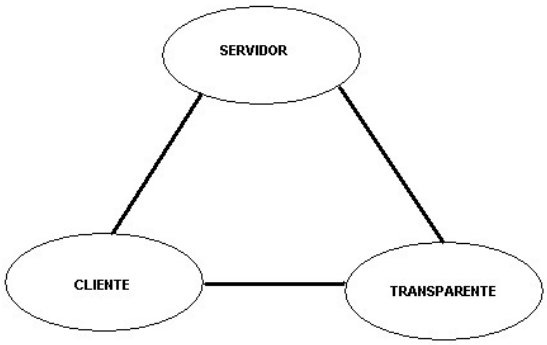


Figura 4.17 Modos VTP

Un dispositivo operando como un VTP cliente no puede crear cambiar o borrar VLANs tampoco guarda la configuración VLAN en memoria no volátil.

En ambos modos, cliente y servidor, los switches sincronizarán sus configuraciones de VLAN con la ultima información recibida desde otros switches en el dominio administrado.

Un switch operando en modo VTP transparente no crea anuncios VTP ni sincroniza su configuración VLAN con la información recibida de otros switches en el dominio, sino que sólo transmite los anuncios VTP recibidos de otros switches que son parte del mismo dominio de administración, además puede crear, borrar y modificar VLANs, pero los cambios afectarán solamente al switch local, no se transmitirán a otros switches en el dominio, las funciones de cada modo se muestran en la figura 4.17.

Como trabaja VTP

Los anuncios VTP son desbordados a través del dominio administrado, son enviados cada cinco minutos o cada vez que ocurre un cambio en las configuraciones VLAN (Figura 4.18); son enviados sobre la VLAN por default (VLAN1) usando un frame multicast; Incluido en el anuncio VTP esta un número de revisión de configuración, un número alto indica que la información VLAN que esta siendo anunciada es mas actual que la que esta almacenada.

Un dispositivo que recibe anuncios VTP puede revisar varios parámetros antes de incorporar la información VLAN recibida, primero, el nombre del dominio de administración y la contraseña en el anuncio deben ser iguales a los configurado en el switch local, a continuación, si el numero de revisión de configuración indica que el mensaje fue creado después de la configuración actual, el switch incorpora la información del anuncio VLAN.

Para reiniciar el numero de revisión de configuración en el Catalyst 1900 se utiliza el comando EXEC privilegiado **delete vtp**.

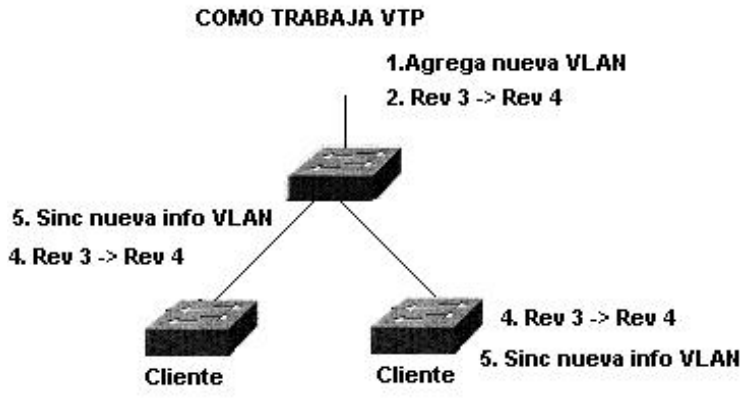


Figura 4.18 Forma de operar de un VTP

Uno de los componentes mas críticos del VTP es el numero de revisión de configuración.,

cada vez que un VTP servidor modifica su información VLAN, este incrementa el número de revisión de configuración en uno, entonces envía un anuncio VTP con el nuevo número de revisión de configuración, si el número anunciado es mayor que el numero almacenado en los otros switches en el dominio, estos sobre-escribirán sus configuraciones VLAN con la nueva información.

Nota: El proceso de sobre-escritura debería significar que si el VTP servidor borra todas las VLANs y tiene el numero de revisión mas alto, los otros dispositivos en el dominio VTP deberían también borrar sus VLANs.

4.1.7 VTP Pruning

VTP pruning usas los anuncios VLAN para determinar cuando una conexión troncal esta innecesariamente desbordando trafico.

Por default, una conexión troncal transporta tráfico para todas las VLAN en el dominio de administración VTP, comúnmente, algunos switches en una red empresarial no tienen puertos locales configurados en cada VLAN. En el ejemplo de red mostrado en la figura 4.19, los switches 1 y 4 soportan puertos estáticamente configurados en la VLAN 1.

VTP pruning incrementa el ancho de banda disponible restringiendo el tráfico desbordado sólo en aquellos enlaces troncales que el tráfico debe usar para acceder a los dispositivos de red apropiados.

La Figura 4.19 muestra una red switcheada con VTP pruning habilitado, en esta red el tráfico de broadcast de la estación A no es transmitido a los switches 3,5 y 6 porque el trafico para una VLAN 1 ha sido "recortado" en los enlaces indicados en los switches 2 y 4.

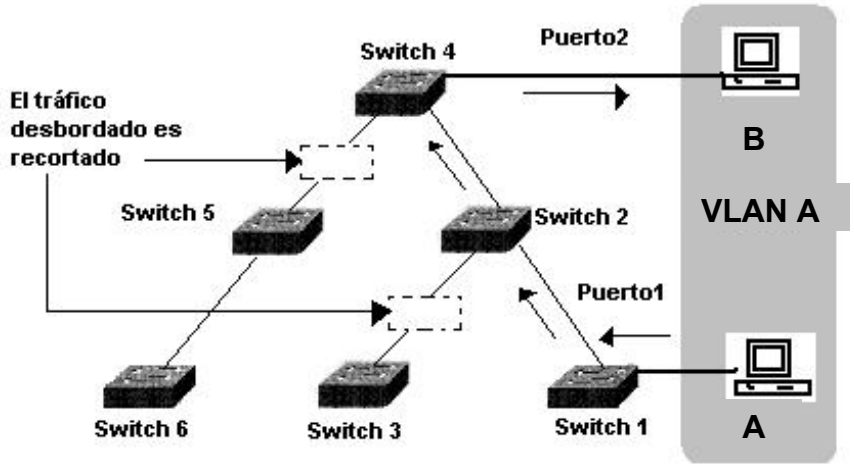


Figura 4.19 VTP pruning

en ambas direcciones (10 Mbps en la transmisión y 10 Mbps en la recepción).

4.2 PRINCIPIOS DE CONFIGURACIÓN DE VLANs

En el switch Catalyst 1900 hay tres métodos diferentes de configuración, el método basado en Web usando el VSM (Visual Switch Manager), el método a base de menús desde el puerto de consola y el método de IOS CLI. Cada método lleva a cabo las mismas tareas. El uso de VSM requiere que el switch tenga una dirección IP configurada y conectividad de red para comunicarse con un navegador Web tal como Netscape o Internet Explorer.

Una dirección IP también debe ser asignada si se planea conectar al switch vía una sesión Telnet o si se planea usar SNMP para administrar el switch.

En este apartado nos enfocaremos a usar el CLI para configurar el switch.

Catalyst 1900 configuraciones por default

El switch Catalyst 1900 viene con ajustes por default. Sin embargo, se pueden cambiar para ajustarlos a las necesidades especificas de cada red. Los valores por default varían dependiendo de las características del switch.

A continuación se mencionan algunos de los ajustes por default en el switch Catalyst 1900.

- IP address: 0.0.0.0
- CDP: Habilitado.
- Switching mode : fragment free.
- 100baseT port: Auto-negociación modo duplex.
- 10baseT port: Half duplex.
- Spanning Tree: Habilitado.
- Consolé password: ninguno.

Puertos en el Catalyst 1900

El switch 1912 y el switch 1924 pertenecen a la familia de switches Catalyst 1900, como se muestra en la Figura 4.20, el 1912 y el 1924 tienen:

- Un puerto AUI (e0 25)
- Dos puertos uplink 100baseT (FastEthernet 0/26 y FastEthernet 0/27)

Los puertos uplink son también referidos como: Port A (FastEthernet 0/26) y port B(FastEthernet 0/27)

En adición a los puertos AUI y uplinks 100baseT:

- El 1912 tiene 12 puertos 10baseT (e0/1 a e0/12)
- El 1924 tiene 24 puertos 10baseT (e0/1 a e0/24)

	Catalyst 1912	Catalyst 1914
Puertos 10 base T	e0/1 a e0/12	e0/1 a e0/24
Puertos AUI	e0/25	e0/25
Puertos Uplink 100 base T	fa0/26(Port A) fa0/27(Port B)	fa0/26(Port A) fa0/27(Port B)

Figura 4.20 Switch Catalyst serie 1900

Los puertos en el Catalyst 1900 son refenciados como puerto o interfases. Por ejemplo, para el puerto 1 (Figura 4.21):

- La salida del comando **show run** se refiere a e0/1 como Interfase e0/1
- La salida del comando **show spantree** se refiere a e0/1 como puerto Ethernet0/1.
- La salida del comando **show vlan-membership** se refiere a e0/1 como solamente puerto 1.

```
wg_sw_d# show run

Building configuration…
!
!
Interfase Ethernet 0/1
!
!
Interfase Ethernet 0/2
```

```
wg_sw_d# show span

Port Ethernet 0/1: of VLAN 1 is forwarding
   Port path cost 100,Port priority 128
   Designate root has priority 32768, address 0090.8673.3340
   Designed port is Ethernet 0/1, path cost 0
   Timers: message age 20, forward delay 15, hold 1
```

Port	VLAN	Membership Type	Port	VLAN	Membership Type
1	5	static	13	1	static
2	1	static	14	1	static
3	1	static	15	1	static

Figura 4.21Comandos para el manejo de puertos

Modos de configuración el switch.

El switch Catalyst 1900 tiene varios modos de configuración, para configurar los parámetros globales del switch, como el nombre del switch o la dirección IP, se utiliza el modo de configuración global; para configurar un puerto o interfase en particular, se utiliza el modo de configuración de interfase (Figura 4.22).

Modos de configuración global	wg_sw_a# conf term wg_sw_a(config)#
Modos de configuración interface	wg_sw_a(config)# interface e0/1 wg_sw_a(config-if)#

Figura 4.22 Modos de configuración global

- **Configurando la dirección IP del switch.**

  Para configurar una dirección IP y una mascara de subred al switch se utiliza el comando en modo de configuración global **ip address**, cabe mencionar que se requiere una dirección IP en el switch para propósitos de administración.

Por ejemplo, para poder emplear el VSM, se requiere que el switch tenga una dirección IP configurada y conectividad IP para comunicarse con un navegador web tal como Netscape o Microsoft Internet Explorer. Una dirección IP debe ser asignada también, si se planea conectar al switch vía Telnet o si se planea usar SNMP para administrar el switch.

Se usa el comando de configuración global **no ip address** para restaurar la dirección IP a su valor default que es 0.0.0.0.

- **Configuración del default gateway del switch.**

El default gateway es la dirección IP del ruteador usado para enviar tráfico entre diferentes redes, se ndebe configurar uno en el switch, pues si el switch necesita enviar tráfico hacia una red IP diferente a la que pertenece, éste envía el tráfico hacia el default gateway.

Se utiliza el comando de configuración global **ip defalult-gateway** para configurar el default gateway y el comando **no ip default-gateway** para restaurar la dirección del gateway (Figura 4.23) al valor por default 0.0.0.0, por ejemplo:

```
wg_sw_a(config)#

ip default-gateway {ip adrress}

wg_sw_a(config)# ip default-gateway 10.5.5.3
```

Figura 4.23 Configuración del default gateway

Se utiliza el comando **show ip** (Figura 4.19) desde el modo EXEC privilegiado para verificar la dirección IP, la mascara de subred y el default gateway, por ejemplo (Figura 4.24):

```
wg_sw_a(config)#show ip

IP address:                     10.5.5.11
Subnet mask:    255.255.255.0
Default gateway:        10.5.5.3
Management VLAN:            1
Domain name:
Name server 1:          0.0.0.0
Name server 2:          0.0.0.0
HTTP server:            Enabled
HTTP port:                              80
RIP:                        Enabled
wg_sw_a#
```

Figura 4.24 Comando Show ip

- **Ajuste de las opciones Duplex**

Se utiliza el comando de configuración de interfase **duplex** para habilitar el modo duplex para una interfase.

- **Auto:** ajusta la auto-negociación del modo duplex
- **Full:** ajusta el modo full-duplex.
- **Full-flow-control:** ajusta el modo full-duplex con control de flujo.
- **Half:** ajusta el modo half-duplex.

Para puertos 100 Mbps TX el default es **auto**, para puertos 10 Mbps TX el default es **half**, para verifica los ajustes de duplex se utiliza el comando **show interfase** (Figura 4.25).

```
wg_sw_a(config)#interface e0/1
wg_sw_a(contig-if)#

duplex {auto | full | full-flow-control | half}

wg_sw_a(config-if)#duplex half
```

Figura 4.25 Configuración de las opciones duplex

Se usa el comando en modo EXEC privilegiado **show interfaces** para desplegar las estadísticas y el estado de todas las interfaces especificadas. Una de las piezas de información mostrada es el ajuste de duplex de una interface (Figura 4.26).

```
wg_sw_a# show interfaces

Ethernet 0/1 is Enable
Hardware is Built-in 10base-T
Address is 00E0.1EA2.FBC1
MTU 1500 bytes, BW 10000 Kbits
802-1d STP State: Blocking        Forward Transitions       : 2
Port monitoring: Disabled
Unknown unicast flooding: Enabled
Unregistered multicast flooding: Enabled
Description:           ests
Duplex settings: Half duplex
Back pressure: Disabled
```

Figura 4.26 Opciones Duplex

La auto-negociación puede producir a veces resultados impredecibles. Si un dispositivo conectado no soporta auto-negociación y esta operando en modo full-duplex por default, el switch Catalyst ajusta el puerto correspondiente al modo half-duplex.

Esta configuración, half-duplex en un extremo y full-duplex en el otro, origina errores de colisiones tardías en el extremo half-duplex. Para evitar esta situación, se deben ajustar manualmente los parámetros duplex del switch para igualar al dispositivo conectado.

```
wg_sw_a# show interfaces

Ethernet 0/1 is Enabled
Hardware is Built-in 10Base-T
Address is 00E0.1EA2.FBC1
MTU 1500 bytes, BW 10000 Kbits
802.1d STP State:  Blocking       Forward Transitions:  2
Port monitoring: Disabled
Unknown unicast  flooding: Enabled
Unregistered multicast flooding:  enabled
Description:  ests
Duplex setting: Half duplex
Back pressure: Disabled
```

Figura 4.27 a) Errores FCS

Receive Statistics		**Transmit Statistics**	
Total good Frames:	44841	Total frames	404502
Total octets:	4944550	Total octets	29591574
Broadcast/multicast frames	31011	Broadcast/multicast frames	390913
Broadcast/multicast octets	3865029	Broadcast/multicast octets	28478154
Good frames forwarded	9	Deferrals	0
Frames filtered	0	Single collisions	0
Runt frames	0	Multiple collisions	0
No buffer discards	0	Excessive collisions	0
Errors :		Queue full discards	0
FCS errors	0	Errors:	
Alignment errors	0	Late collisions	0
Giant frames	0	Excessive deferrals	0
Address violations	0	Jabber	0
		Other transmit errors	0

Figura 4.27 b) Errores FCS y late collision

Si el puerto del switch esta en modo full-duplex y el dispositivo conectado esta en modo half-duplex, se debe revisar por errores FCS en el puerto del switch full-duplex. Se utiliza el comando **show interfaces** para revisar los FCS o los errores de colisiones tardías (Figura 4.27).

- **Manejo de la tabla de direcciones MAC**

Los switches utilizan tablas de direcciones MAC para transmitir el tráfico entre sus puertos. Estas tablas incluyen direcciones dinámicas, permanentes y estáticas.

Las direcciones MAC dinámicas son aprendidas por el switch y después desechadas cuando no estan en uso. El switch proporciona direccionamiento dinámico aprendiendo la dirección fuente de cada paquete que recibe en cada uno de sus puertos y agregando la dirección y el número de puerto asociado a la tabla. Como las estaciones son agregadas o removidas de la red, el switch actualiza la tabla de direcciones agregando nuevas entradas y sacando las obsoletas, o sea, aquellas que no están actualmente en uso.

Un administrador puede específicamente asignar direcciones permanentes para ciertos puertos, a diferencia de las direcciones dinámicas las direcciones permanentes no se vuelven obsoletas. El Catalyst 1900 puede almacenar hasta un máximo de 1024 direcciones MAC en su tabla. Una vez que la tabla de direcciones

MAC esta llena, todas las nuevas direcciones desconocidas son difundidas (Figura 4.28 a y b). Por ejemplo:

```
wg_sw_a# sh-mac-address-table

Number of permanent address : 0
Number of restricted static addresses  0
Number of dynamic addresses  6
```

Address	Dest Interface	Type	Source interface List
00E0.1E5D.AE2F	Ethernet 0/2	Dynamic	All
00D0.588F.B604	FastEthernet 0/26	Dynamic	All
00E0.1E5D.AE2B	FastEthernet 0/26	Dynamic	All
0090.273B.87A4	FastEthernet 0/26	Dynamic	All
00D0.586F.B600	FastEthernet 0/26	Dynamic	All
00D0.5892.38C4	FastEthernet 0/27	Dynamic	All

Figura 4.28 a y b) Manejo de la direcciones MAC

- **Ajuste de direcciones MAC permanentemente**

Se utiliza el comando de configuración global **mac-address-table permanent** para asociar una dirección MAC permanente a un puerto del switch (especificado por type y module/port). Usa el comando **no mac-address-table permanent** para borrar una dirección MAC permanente.

Una dirección permanente en la tabla de direcciones MAC no se desechada por envejecimiento y todas las interfases pueden enviar tráfico a esta. En el ejemplo mostrado en la Figura 4.29 a y b, el comando especifica que lols frames con la dirección MAC 2222.2222.2222 deben ser transmitidos hacia la interfase Ethernet e0/3 por lo que todas las interfaces pueden enviar tráfico hacia esta dirección.

```
wg_sw_a(config)#mac-address-table permanent  2222.2222.2222 e0/3

wg_sw_a#sh mac-address-table
Number of permanent address : 1
Number of restricted static addresses:  0
Number of dynamic addresses:  4
```

Address	Dest Interface	Type	Source interface List
00E0.1E5D.AE2F	Ethernet 0/2	Dynamic	All
2222.2222.2222	Ethernet 0/3	Permanent	All
00E0.1E5D.AE2B	FastEthernet 0/26	Dynamic	All
0090.273B.87A4	FastEthernet 0/26	Dynamic	All
00D0.586F.B600	FastEthernet 0/26	Dynamic	All
00D0.5892.38C4	FastEthernet 0/27	Dynamic	All

Figura 4.29 a y b) Ajuste de dirección MAC permanente

- **Ajuste de direcciones MAC estáticas restringidas**

Se utiliza el comando de configuración global **mac-address-table restricted static** para asociar una dirección estática restringida a un puerto del switch, y el comando **no mac-address-table restricted static** para borrarla.

En el ejemplo de la Figura 4.30 a y b, el switch permite tráfico, hacia la dirección estática restringida 1111.1111.1111 en e0/4 únicamente desde e0/1.

```
wg_sw_a(config)#mac-address-table restricted static  1111.1111.1111 e0/4 e0/1

wg_sw_a#sh mac-address-table
Number of permanent address : 1
Number of restricted static addresses:  1
Number of dynamic addresses:  4
```

Figura 4.30 a) Ajuste de dirección MAC estática restringida

Address	Dest Interface	Type	Source interface List
1111.1111.1111	Ethernet 0/4	Static	Et0/1
00E0.1E5D.AE2B	Ethernet 0/2	Dynamic	All
2222.2222.2222	Ethernet 0/3	Permanent	All
0090.273B.87A4	FastEthernet 0/26	Dynamic	All
00D0.586F.B600	FastEthernet 0/26	Dynamic	All
00D0.5892.38C4	FastEthernet 0/27	Dynamic	All

Figura 4.30 b) Ajuste de dirección MAC estática restringida

- **Configuración de la seguridad en el puerto**

Se utiliza el comando de configuración de interfase **port secure** para habilitar la seguridad de direccionamiento (Figura 4.31). Se utiliza también el comando **no port secure** para deshabilitar la seguridad de direccionamiento o ajustar el máximo número de direcciones permitidas en la interfase hacia el valor por default (132).
Los puertos asegurados restringen el uso de un puerto hacia un grupo de estaciones definido por el usuario. El número de dispositivos en un puerto asegurado puede estar en el rango de 1 a 32. Las direcciones MAC para los dispositivos en un puerto seguro son asignadas estadísticamente asignados por un administrador o sticky-learned. Sticky-learned toma lugar cuando la tabla de direcciones para un puerto asegurado no contiene un complemento total de direcciones estáticas. El puerto sticky aprende la dirección fuente de los frames que ingresan y automáticamente las asigna como direcciones permanentes.

Se utiliza el comando EXEC en modo privilegiado **show mac-address-table security** para desplegar y verificar la configuración de seguridad del puerto.

```
wg_sw_(config-if)#

port secure [max-mac_count count]

-  Configura una interfase a ser un puerto seguro.
-  Define un máximo numero de direcciones MAC permitidas en la tabla de dirección para este puerto.
-  Count puede ser de 1 a 132.
-  El default  es132.

wg_sw_a(config)# interface e014
wg-sw_a(config-if)# port secure
wg_sw_a(config-if)# port secure max-mac-count 1
```

Figura 4.31 a) Configuración de la seguridad en puerto

Una violación de dirección ocurre cuando un puerto seguro recibe una dirección fuente que ha sido asignada a otro puerto asegurado o cuando un puerto trata de aprender una dirección que excede el tamaño límite de su tabla de direcciones, cuando una violación de seguridad ocurre, la acción a seguir puede ser suspendido (suspended), ignorada (ignored) o deshabilitada (desable). Cuando un puerto esta suspendido, es rehabilitado hasta que se recibe un paquete conteniendo una dirección válida. Cuando un puerto esta deshabilitado, deberá ser habilitado manualmente. Si el switch ignora la violación de seguridad, éste mantiene el puerto habilitado.

Usa el comando de configuración global **addres-violation** para especificar la acción para una violación de dirección de puerto. Usa el comando no **address-violation** para ajustar el switch a su valor por default (suspendido) (Figura 4.32 a, b, c y d).

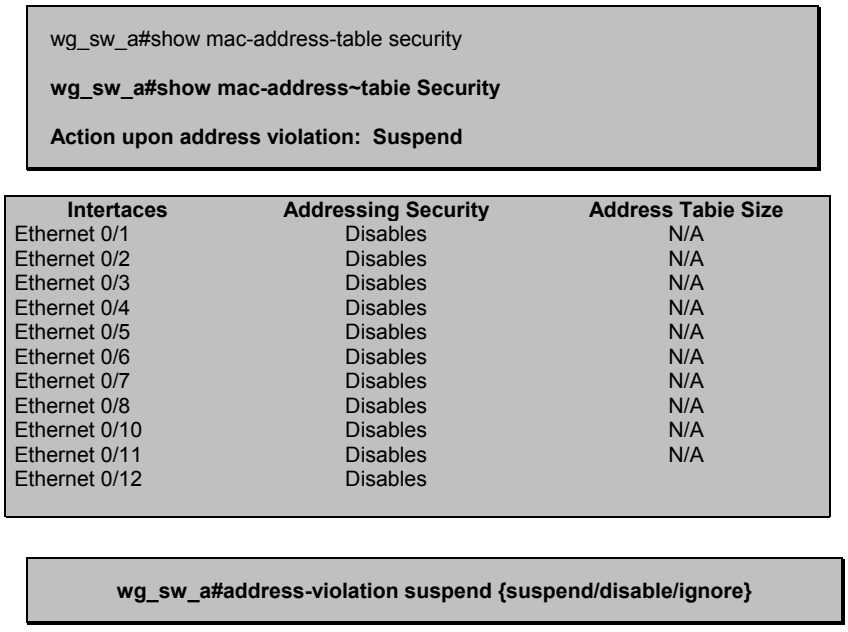


Figura 4.32 b, c y d) Configuración de la seguridad en puerto

- **Show version**

Usa el comando EXEC en modo usuario **show version** para desplegar la información básica acerca del hardware y versión del software IOS (Figura 4.33).

```
wg_sw_a# show version

Cisco Catalyst 1900/2820 Enterprise Edition Software
Version V9.00.00(12) written from 171.071.114.222
Copyright (c) Cisco Systems, Inc. 1993-1999
uptime is 2 day(s) 22 hour(s) 50 minute(s) 2l second(s)
Cisco Catalyst 1900 (486sxl) processor with 2048K/1024K bytes of memory Hardware board revision is 1
Upgrade Status: No upgrade currently in progress.
Config File Status: File wgswd.cfg downloaded from 10.1.1.1
27 Fixed Ethernet/IEEE 802.3 interface(s)
Base Ethernet Address: 00-E0-IE-7E-BE-80

wg_sw_a#
```

Figura 4.33 Show versión

- **Manejo del archivo de configuración**

  Se utiliza el comando EXEC en modo privilegiado **copy nvram tftp** para cargar la configuración en la NVRAM hacia el servidor TFTP (Figura 4.34).

  Usa el comando EXEC en modo privilegiado **copy tftp nvram** para descargar una configuración desde el servidor TFTP a la NVRAM (Figura 4.35).

  Nota: En el Catalyst 1900, la configuración running es guardada automáticamente hacia la NVRAM si se produce un cambio en la configuración running.

  Para enviar la configuración hacia un servidor TFTP:

  wg_sw_a#

  ```
  copy nvram tftp://host/dst_file
  ```

  Figura 4.34 Configuración hacia un servidor TFTP

  Para descargar la configuración desde un servidor TFTP:

  wg_sw_a#

  ```
  copy  tftp://host/src_file nvram
  ```

  ```
  wg_sw_a#copy nvram tftp://10.1.1.1/wgswd.cfg
  Configuration upload is sucessfully completed

  wg_sw_a#copy tftp://10.1.1.1/wgswd.cfg nvram
  TFTP succesfully downloades configuration file
  ```

  Figura 4.35 Configuración desde un servidor TFTP

- **Limpiando la NVRAM**

  Usa el comando EXEC en modo privilegiado **delete nvram** para restaurar la

configuración del switch a los valores por default (Figura 4.36).

```
wg_sw_d$delete nvram

Re-inicializa la configuración del sistema a los defaults de fábrica
```

Figura 4.36 Limpiando la NVRAM

4.2.1 Directrices de configuración VLAN

En un switch Catalyst 1900 se pueden activar como máximo 64 VLANs. En la configuración por default de estos switches (figura 4.37), hay varias VLANs pre-configuradas. Una de las VLANs por default es la VLAN 1. Los anuncios CDP y VTP son enviados sobre la VLAN 1. La dirección IP del switch esta en el dominio de broadcast de la VLAN 1. Como recordará, el switch requiere una dirección IP para propósitos de administración.

- El máximo número de VLANs depende del switch.
- El Catalyst 1900 soporta 64 VLANs con un spanning tree separado por VLAN.
- VLAN1 es la default.
- Los anuncios CDP y VTP son enviados sobre la VLAN1.
- La dirección IP del Catalyst 1900 esta en el dominio de broadcast de la VLAN1.
- Debe estar en modo servidor o transparente en VTP para crear, agregar o borrar VLANs.

Figura 4.37 Configuración de VLAN

Antes de que se pueda crear una VLAN, el switch debe de estar en modo VTP servidor o en modo VTP transparente.

Antes de crear VLANs debe decidir si va utilizar VTP para mantener sincronizada la información de configuración global en la red. Por default, un switch esta en modo VTP servidor.

Para permitir que las VLAN se extiendan a través de múltiples switches se deben configurar las tróncales Fast Ethernet para interconectar los switches (Figura 4.38).

- Habilitar VTP (opcional).
- Habilitar Trunking.
- Crear VLANs.
- Asignar una VLAN hacia los puertos.

Figura 4.38 Pasos de configuración

La membresía de los puertos del switch en una VLAN determinada, se asigna manualmente .

La configuración default para el switch Catalyst es:

- VTP domain name None
- VTP mode Server
- VTP pruning None
- VTP password Disable
- VTP trap Enable

El nombre del dominio VTP puede ser especificado o aprendido, por default el dominio no tiene nombre, también se debe asignar una contraseña para el dominio de administración VTP, la contraseña introducida debe ser las misma para todos los switches en el dominio ya que si se configura una contraseña diferente, el dominio VTP no funciona adecuadamente.

Habilitando o deshabilitando VTP pruning en el servidor VTP, se propagan los cambios a través de todo el dominio, es decir, se afecta al dominio de administración completo.

Se utiliza el comando en modo de configuración global **vtp** para especificar el modo de operación, nombre del dominio, contraseña y capacidades de VTP pruning. En el nombre del dominio se deben respetar las letras mayúsculas y minúsculas.

Para verificar un cambio de configuración reciente o para ver la información de configuración VTP, se utiliza el comando EXEC privilegiado **show vtp** (Figura 4.39)**.** También es desplegada la dirección IP del último dispositivo que modifico la configuración y el tiempo en que la modificación fue hecha. VTP tiene dos versiones: VTP versión 1 solamente soporta Ethernet , VTP versión 2 soporta Ethernet y Token Ring.

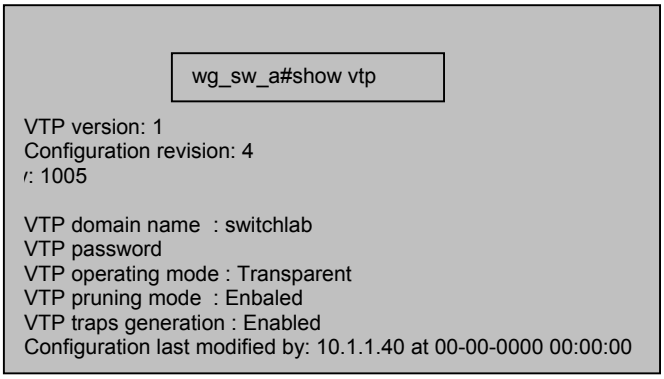


Figura 4.39 Configuración VTP

Definiendo una Troncal (Trunk)

Se utiliza el comando **trunk** en modo de configuración de interfase para establecer un puerto Fast Ethernet en modo troncal. El Catalyst 1900 soporta el DISL (Dynamic Inter-Switch Link), DISL maneja automáticamente la negociación de troncal ISL.

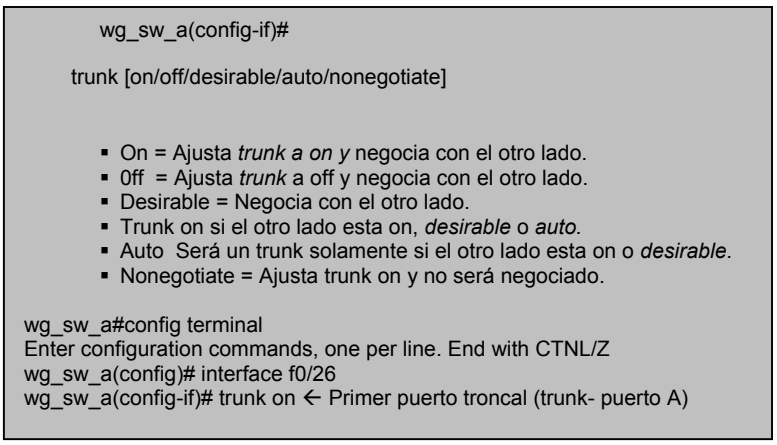


Figura 4.40 Comando Trunk

En el Catalyst 1900, los dos puertos Fast Ethernet son las interÍases fa0/ 26 y fa0/27, el comando **trunk** tiene cinco opciones: ***on, off, auto, desirable y negotiate*** los cuales se muestran en la Figura 4.40.

On = Configura el puerto dentro del modo de troncal ISL permanente y negocia con el dispositivo conectado para convertir el enlace en modo trunk.

Off = Deshabilita el modo *tnuk* del puerto y negocia con el dispositivo conectado para convertir al enlace a no *trunk.*

Desirable = Permite al puerto negociar el tipo de enlace Trunk. El puerto se establece como T*runk* si el dispositivo conectado esta en estado **on, desirable** o **auto**. De otra manera, el puerto será no Tru*nk.*

Auto = Habilita a un puerto como *trunk* solamente si el dispositivo conectado tiene el estado ajustado a **on** o **desirable**.

Nonegotiate = Configura el puerto a modo Trunk ISL permanente y ninguna negociación toma lugar con el "socio".

Para verificar la configuración de una troncal, se usa el comando EXEC privilegiado **show trunk** para desplegar los parámetros de la trocal (Figura 4.41).

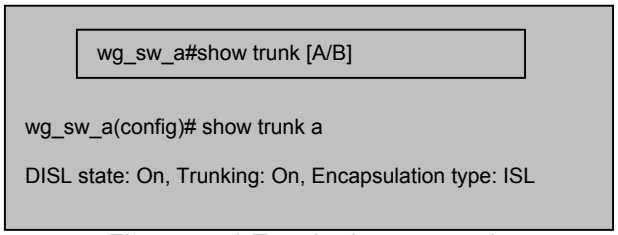


Figura 4.41 Estado de un troncal.

Agregando una VLAN

Usa el comando **vlan** en modo de configuración global para configurar VLANs en un switch Catalyst 1900, (Figura 4.42).

Cada VLAN tiene un único ID de cuatro dígitos que puede ser un numero entre 0001 y 1005. Para agregar una VLAN, se le debe asignar un número y nombre. Las VLAN por default son VIAN1, VLAN1002, VLAN1003, VLAN1004 y VLAN1005.

Para agregar una VLAN Ethernet, se debe especificar al menos un número de VLAN. Si ningún nombre de VLAN es introducido, por default es agregar el número de VLAN a la palabra VLAN, por ejemplo, VLAN0004.

Recordemos que para agregar, cambiar o borrar VLANs el switch debe estar en modo VTP servidor o en modo transparente.

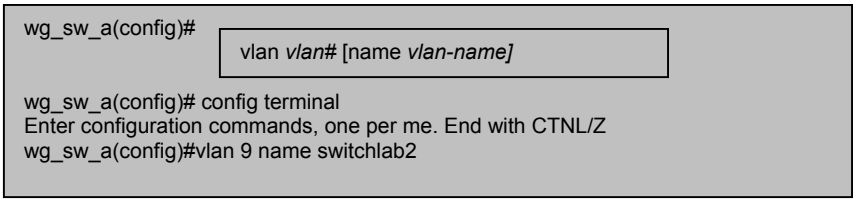


Figura 4.42 Agregando una VLAN

Una vez que la VLAN esta configurada, se deben confirmar los parámetros para asegurar su validez. Para verificar los parámetros de una VLAN se usa el comando EXEC privilegiado **show vlan *vlan#*** el cual despliega la información acerca de una VLAN y se usa el comando **show vlan** para mostrar todas las VLANs configuradas parea un switch (Figura 4.43), este comando también muestra que puertos del switch estan asignados a cada una de las VLANs, así como, el type (el default es Ethernet), SAID (usado por tróncales FDI), MTU (el default es 1500 para una VLAN Ethemet), el protocolo spanning-tree (el switch Catalyst 1900 solamente soporta el protocolo spanning-tree 802.1d) y otros parámetros usados para las VLANs Token Ring o FDI.

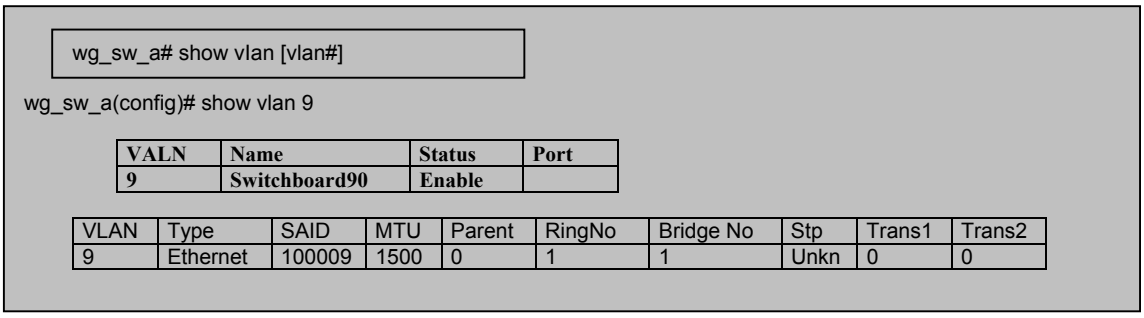


Figura 4.43 Comando show vlan

Modificando el nombre de una VLAN

Para modificar un parámetro existente en una VLAN tal como su nombre, se utiliza la

sintaxis del mismo comando usado para agregar una VLAN.

En el ejemplo mostrado en la figura 4.44, el nombre de la VLAN9 es cambiado a switchlab9 y posteriormente se utiliza el comando **show vlan 9** para verificar el cambio.

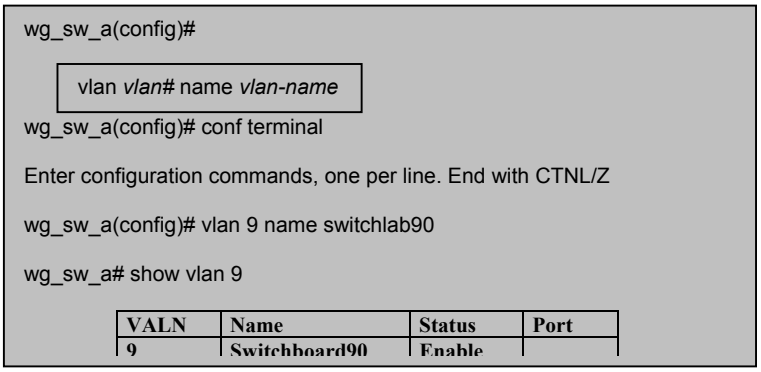


Figura 4.44 Modificación del nombre de VLAN

Asignando puertos de switch hacia una VLAN

Después de crear una VLAN se pueden asignar puertos estáticamente a esa VLAN. Un puerto puede solamente pertenecer a una VLAN a la vez (Figura 4.45).

La asignación de puertos a una VLAN se hace desde el modo de configuración de interfase, usando el comando **vlan-membership**, **Dynamic** significa que el Catalyst 1900 pregunta a un VMPS por la información del la VLAN basada en una dirección MAC. Por default todos los puertos son miembros de la VLAN1 por default.

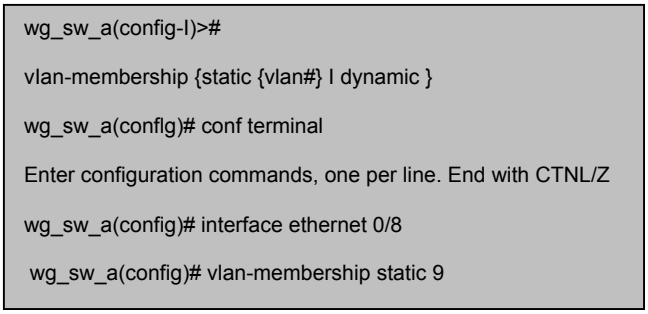


Figura 4.45 Modificación del nombre de VLAN

Verificando los miembros de una VLAN

Usa el comando EXEC privilegiado **show vlan-membership** para desplegar la asignación y tipo de membresía para todos los puertos del switch (Figura 4.46).

El port 1 se refiere al Ethernet 0/1, el port 2 se refiere al Ethernet 0/2 y así sucesivamente.

wg_sw_a# show vlan-membership

Port	VLAN	Membership Type	Port	VLAN	Membership Type
1	5	Static	13	1	Static
2	1	Static	14	1	Static
3	1	Static	15	1	Static
4	1	Static	16	1	Static
5	1	Static	17	1	Static
6	1	Static	18	1	Static
7	1	Static	19	1	Static
8	9	Static	20	1	Static

Nota: port 1 = e0/1, port 2 = e0/2 . . .

Figura 4.46 Miembros de una VLAN

Verificando el Spanning Tree

Se usa el comando EXEC privilegiado **show spantree** para desplegar el estado de la configuración del protocolo de spanning-tree del switch, en el ejemplo de la Figura 4.47, se muestra diversa información sobre el spanning-tree para la VLAN1.

Recuerde que el switch Catalyst puede soportar un spanning-tree por cada VLAN, esto permite el balance de la cargas entre los switches. Por ejemplo. un switch puede ser root para la VI AN1 mientras que otro switch puede ser root para la VLAN2.

```
wg_sw_a(config)#  show spantree {vlan number}

wg_sw_a(config)#  show spantree1


VLAN1 is executing the IEEE compatible Spanning Tree protocol

        Bridge Identifier has priority 32768, address 0050.F037.DA00
        Configured hello time 2, max age 20, forward delay 15
        Current root has priority 0, address 00D0.588F.B600
        Root port is Fast Ethrnet 0128, Cost of root path is 10
        Topology change flag not set, detected flag not set
        Topology changes 53, last topology change occurred 0d00h17m14s ago Times:
        hold 1,  topology change 8960
       hello 2, max age 20, forward delay 15
        Timers: hello 2, topology change 35, notification 2

Port Ethernet 0/1 of VLAN1 is Forwarding
Port path cost 100, Port priority 128
Designated root has priority 0, address 00D0.588F.B600
Designated bridge has priority 32768, address 0050.F037.DA00
Designated port is Ethernet 0/1,  path cost 10
Timers: message age 20, forward delay 15, hold 1
```

Figura 4.47 Comando Show spantree

4.3 APLICACIONES

4.3.1 Aplicación de VLANs a un red de campus universitario

Como primer ejemplo de aplicación tomaremos el caso de un campus de una universidad o un gran edificio. Supongamos que se quiere dividir en varias una red local que abarca el campus de una universidad, inicialmente se puede pensar en crear una LAN por edificio con switches en cada edificio e interconectar cada edificio a una interfaz diferente de un router que interconecte todo el campus, para así aislar los dominios de broadcast y mantener comunicadas todas las LANs. Sin embargo, a menudo se requiere realizar una división lógica de acuerdo a criterios funcionales, que no siempre coinciden con la ubicación física. En este caso se podría pensar por razones de eficiencia y seguridad en crear una red para investigación, otra para docencia, otra para estudiantes y una última para tareas administrativas.

Normalmente habrá varios edificios en los que habrá que dotar una serie de puestos de cada una de las cuatro redes mencionadas, en cuyo caso habría que instalar en los correspondientes armarios de cableado switches independientes e interconectarlos entre sí por separado. Esto provoca una red compleja y muy cara, ya que en muchos casos habrá equipos subutilizados.

El problema que se presenta es simple, se desea tener redes aisladas, a nivel de enlace, para los cuatro grupos de trabajo mencionados. La solución es sencilla si se dispone de espacios físicos contiguos para todos los miembros de un mismo grupo, como por ejemplo un edificio o piso para administración, otro para alumnos, etc. Pero, generalmente esto no sucede y existe una mezcla de usuarios en un mismo edificio y/o piso. La solución pasará entonces por la mencionada opción de tener por cada piso y/o edificio un switch para cada grupo de trabajo, con el fin de nunca mezclar los tráficos, y lograr la conectividad entre las cuatro LAN usando un router de cuatro interfases que permita comunicarlas a un nivel superior (nivel de red).

La solución que proponemos a este problema, es el uso de Redes Virtuales de Área Local o VLANs. Las VLANs son una forma de realizar una partición lógica de un switch en otros más pequeños, de forma que aunque se trata de un solo equipo, se dividen los puertos en grupos que son completamente independientes entre sí. Un switch que tiene la capacidad de generar VLANs se puede considerar como un switch que, por software, se convertirá en tantos switches como VLANs se creen, es decir, si se crean las cuatro VLANs necesarias para el ejemplo en un switch, esto se puede ver como si se hubieran comprado cuatro switches y cada uno de ellos genera una LAN para cada grupo de trabajo, y los tráficos, a nivel de enlace, nunca se mezclarán, pues la única forma de hacerlo es utilizando un router que comunique, a nivel de red, las cuatro VLANs generadas. Un switch con capacidades de VLANs es entonces un generador de diversos dominios de broadcast. La funcionalidad o soporte de VLANs está disponible hoy en día en la mayoría de los switches del mercado, como por ejemplo el switch que analizamos en el primer apartado de este capitulo (Switch Catalyst 1900 de CISCO).

Analizando el caso anterior, en que se ha decidido dividir la red de campus en cuatro VLANs: I (de investigación), D (de docencia), E (de estudiantes) y A (de administración).

Si se tiene un switch de 24 puertos en un closet de cableado y se plantea la necesidad de suministrar servicio a 8 equipos de la VLAN I, 4 de la D, 4 de la E y 4 de la A. Se podría asignar, por ejemplo, los puertos 1 a 8 a la VLAN I, 9 a 12 a la VLAN D, 13 a 16 a la VLAN E y 17 a 20 a la VLAN A, dejando los puertos 21 a 24 libres para futuras ampliaciones o para conectar las interfases de un router. A partir de ese momento, el switch se comportará como cuatro switches virtuales de 4 puertos cada uno, los correspondientes a las tres VLANs y un cuarto correspondiente a los puertos no asignados. De esta forma, se pueden asignar puertos a una u otra VLAN de forma flexible en función de las necesidades (Figura 4.48).

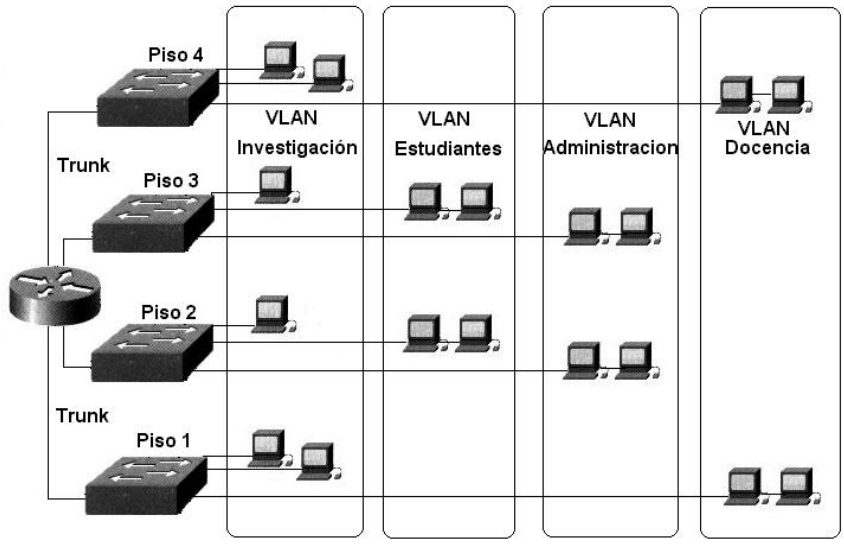


Figura 4.48 Red del Campus

Queda por resolver aún la conexión de las cuatro VLANs con el resto de la red. Una posibilidad sería asignar los puertos 21 a 24 a cada una de las cuatro VLANs y conectarlos a cuatro interfases físicas diferentes del router. Aunque físicamente las cuatro VLANs comparten los switches, sigue habiendo cuatro redes separadas en el cableado, ya que nunca viajan por un mismo cable frames de VLANs diferentes. Cabe también pensar en un nivel adicional de optimización en el que se compartiera un mismo cable para diferentes VLANs. Esto permitiría un ahorro considerable en el número de puertos consumidos especialmente cuando se manejan muchas VLANs.

Por ejemplo, se podría emplear sólo un puerto, por ejemplo el 21, para conectar las cuatro VLANs, liberando así los puertos 22 a 24 para otros usos. Esta situación se denomina configuración de un enlace trunk o troncal. Debiera ser lógico entonces que los enlaces Trunk suelan ser de mayor capacidad que los puertos normales del switch ya que soportan un tráfico más elevado. Por ejemplo, en un switch de puertos a 10 Mbps el enlace trunk típicamente será de 100 Mbps y en uno con puertos de 100 Mbps será de Gigabit Ethernet.

Una propiedad interesante de las VLANs es la posibilidad de configurar interfases virtuales en los hosts. Suponiendo que en el caso analizado con las cuatro VLANs, I, D, E y A, se tiene un servidor que se desea esté accesible de forma directa en las cuatro

VLANs, de forma que cualquier host de cualquiera de las VLANs pueda acceder a él sin necesidad de pasar por un router. Una posible solución sería conectar al servidor mediante cuatro interfases de red y conectar cada una de ellas a un puerto del switch asignado a cada una de las VLANs. Cada interfaz recibiría una dirección de red correspondiente a la VLAN en la que se encuentra. Sin embargo, esta solución se hace inmanejable si aumenta el número de VLANs. Otra posibilidad, más interesante, sería configurar una interfaz de red del servidor como tres interfaces virtuales y conectarla a un puerto trunk del switch. Para esto se necesita disponer de drivers con soporte de IEEE 802.1q para la interfaz de red.

Finalmente para mayor optimización facilitando la administración de las cuatro VLANs, se pueden crear **VLANs por dirección MAC.** Este tipo de VLAN ofrece mayores ventajas ya que las estaciones pueden cambiar su ubicación física sin perder la pertenencia a la VLAN asignada originalmente, evitando así la necesidad de reconfigurar el switch, además, no presenta ningún problema de compatibilidad con los diversos protocolos y soporta incluso la utilización de protocolos dinámicos tipo DHCP.

Esta configuración permite a equipos portátiles conectarse en cualquier nodo de red disponible sin necesidad de hacer cambios en la configuración del switch o del equipo para asegurar su pertenencia a una VLAN.

4.3.2 Aplicación de VLANs a una red empresarial con varios departamentos y sucursales.

Otro ejemplo de aplicación de VLANs en la solución a problemas que se presentan en redes locales, es la problemática de una empresa que tiene varios departamentos y sucursales. Para su control tiene un sistema administrativo interno para la administración de la información que genera la empresa; además de varias aplicaciones comerciales que usan los usuarios para generar reportes de control interno y externo adicionales, pero que necesitan del sistema de red para su distribución entre los diferentes departamentos.

Como e muestra en la Figura 4.49, esta empresa tiene una red compuesta por tres servidores, un switch y dos hubs, el switch divide en dos segmentos la red y en cada segmento se mezclan tráficos de varios departamentos. El primer segmento tiene un servidor el cual esta conectado a una parte del switch y a su vez a un hub. Al hub están conectadas los nodos de los departamentos:

- Almacen que tiene como subdepartamentos los de Aduana, Trafico y Distribución.
- Compras que tiene como subdepartamentos a Exterior y Nacionales.
- Ventas que tiene como subdepartamentos a Licitación, Sucursales y Corporativos.

El segundo segmento esta formado por otro servidor que contiene el sistema de red y el sistema administrativo de la empresa, además de un segundo hub que interconecta los nodos de los departamentos:

- Dirección y Administración.
- Contabilidad con sus subdepartamentos de Fiscal, Recursos Humanos e Insumos.
- Tesorería con los subdepartamentos de Cuentas por Cobrar y Cuentas por Pagar

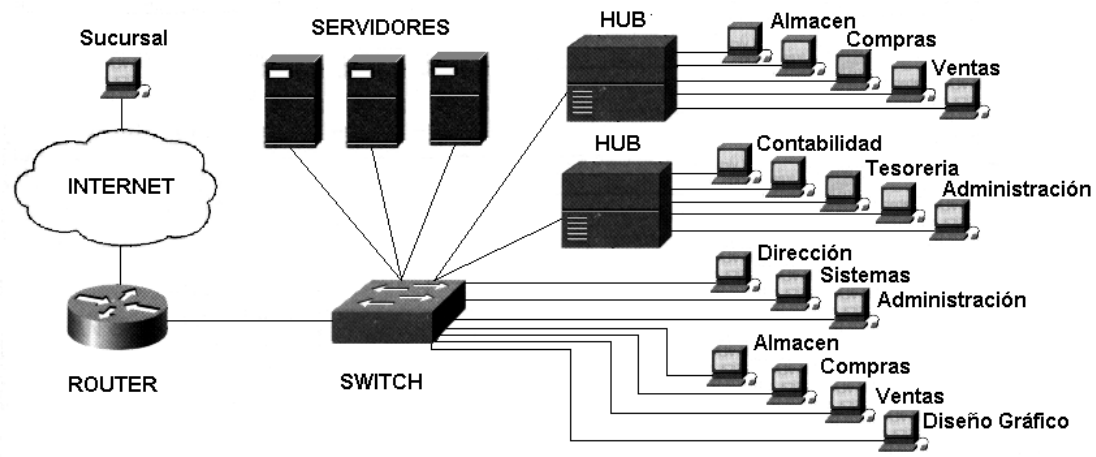


Figura 4.49 Diagrama de red

El tercer servidor lo administra el departamento de sistemas para generar reportes de control para la dirección, también se emplea para realizar los respaldos de los dos servidores anteriores y compartir la información que necesitan los departamentos de los segmentos 1 y 2.

Por necesidades comerciales se contrato el servicio de internet a alta velocidad para usuarios que requerían enviar y recibir correos electrónicos de clientes, proveedores, banco, etc., además de consultar paginas de internet de proveedores, del gobierno, etc. También se tiene un departamento de Diseño Gráfico aunque no hace uso de los servidores si tiene la necesidad de estar conectado a la red para poder tener acceso a internet Este servicio se provee mediante un router conectado directamente al switch. Esto ocasiona un incremento en el tráfico y las colisiones en la red, con la consiguiente disminución de velocidad en la transmisión de información por la red y disminución de seguridad de la red de la empresa.

Estos problemas se soluciona con el uso de VLANs, ya que podemos aislar el tráfico de cada uno de los departamentos de modo que la información solo estará disponible para el departamento que la genera o utiliza, aumentando así la seguridad. El uso de VLANs, mejora también la velocidad de transmisión al controlar el tráfico de broadcast y disminuir el numero de usuarios por segmento.

Para la solución de los problemas de trafico de esta red empresarial se emplean VLAN por dirección MAC, estas VLANs permiten que los operadores de la red puedan mover una estación de trabajo a una ubicación diferente permitiendo que mantenga su posición dentro de la VLAN.

Para la interconexión de la sucursales de esta empresa, veremos que las VLANs pueden ser extendidas a través de una red WAN (teóricamente). Pero, no es muy recomendable, ya que las VLANs definidas sobre una WAN demandarán un excesivo y costoso ancho de banda para permitir tráfico de amplia emisión ó broadcast. Los ruteadores filtran el tráfico de broadcast y resuelven muy bien este problema. Sin embargo, si el ancho de banda de la WAN esta libre para una organización que tenga instaladas fibras ópticas libres, es una

forma muy conveniente de hacerlo. Además, dependiendo de cómo sean construidas estas redes, los grupos de IPs con muticast que operen como VLANs pueden ser muy bien extendidos en una WAN, en la medida en que los ruteadores provean las conexiones WAN, sin desperdiciar ancho de banda. En la Figura 4.50 se muestran como quedaría la red después de la segmentación, conmutación y de la construcción de las VLANs.

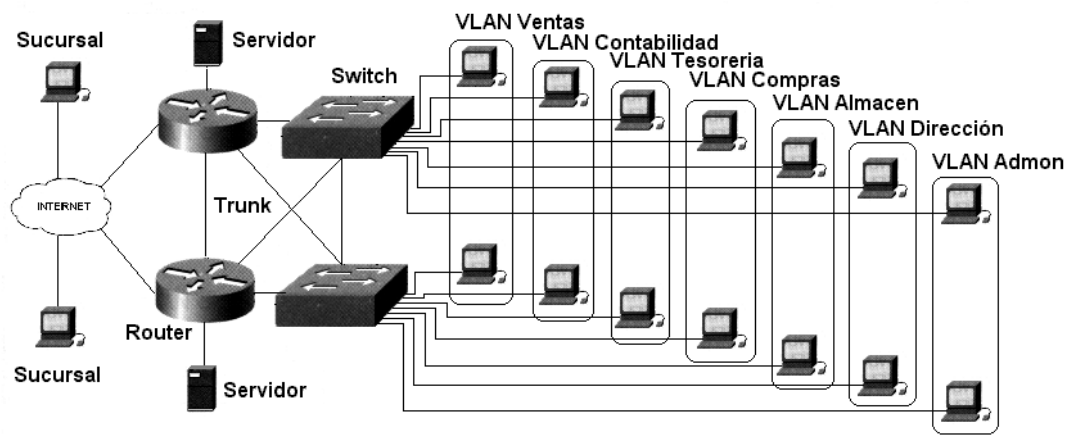


Figura 4.50 Diagrama de redes virtuales

4.4 PALABRAS CLAVES

CISCO
SWITCH ETHERNET CATALYST 1900
DIRECCIONES MAC.
TORMENTAS DE BROADCAST
FRAME
BASE DE DATOS MAC
LOOPS
PROTOCOLO SPANNING-TREE
PUERTOS
BRIDGING.
DIRECCIÓN IP
INTER-SWITCH LINK (ISL)
VTP (VLAN TRUNKING PROTOCOL)

Propuesta del tema de VLANs

Capítulo

5

5. PROPUESTA DE ASIGNATURA OPTATIVA DE VLANs.

5.1 JUSTIFICACIÓN

En este capitulo hacemos una propuesta para incluir en el plan de estudios de la carrera de Ingeniería en Computación la asignatura optativa “Redes Virtuales de Área Local”. Se cubren los métodos y prácticas de actualidad que se utilizan en redes de computadoras para permitir la comunicación. Se cubren también los elementos físicos así como las capas de información para una red de comunicación, junto con las herramientas de diseño, operación y los principios básicos de implementación VLAN.

Para los futuros egresados de la Facultad es importante que estén actualizados con conocimientos que les permitan desempeñar de manera eficiente sus actividades profesionales.

En este sentido, esta tesis aporta información sobre el funcionamiento, ventajas, desventajas y aplicaciones de las redes virtuales de área local, además de las características acerca de los dispositivos de interconexión de las redes.

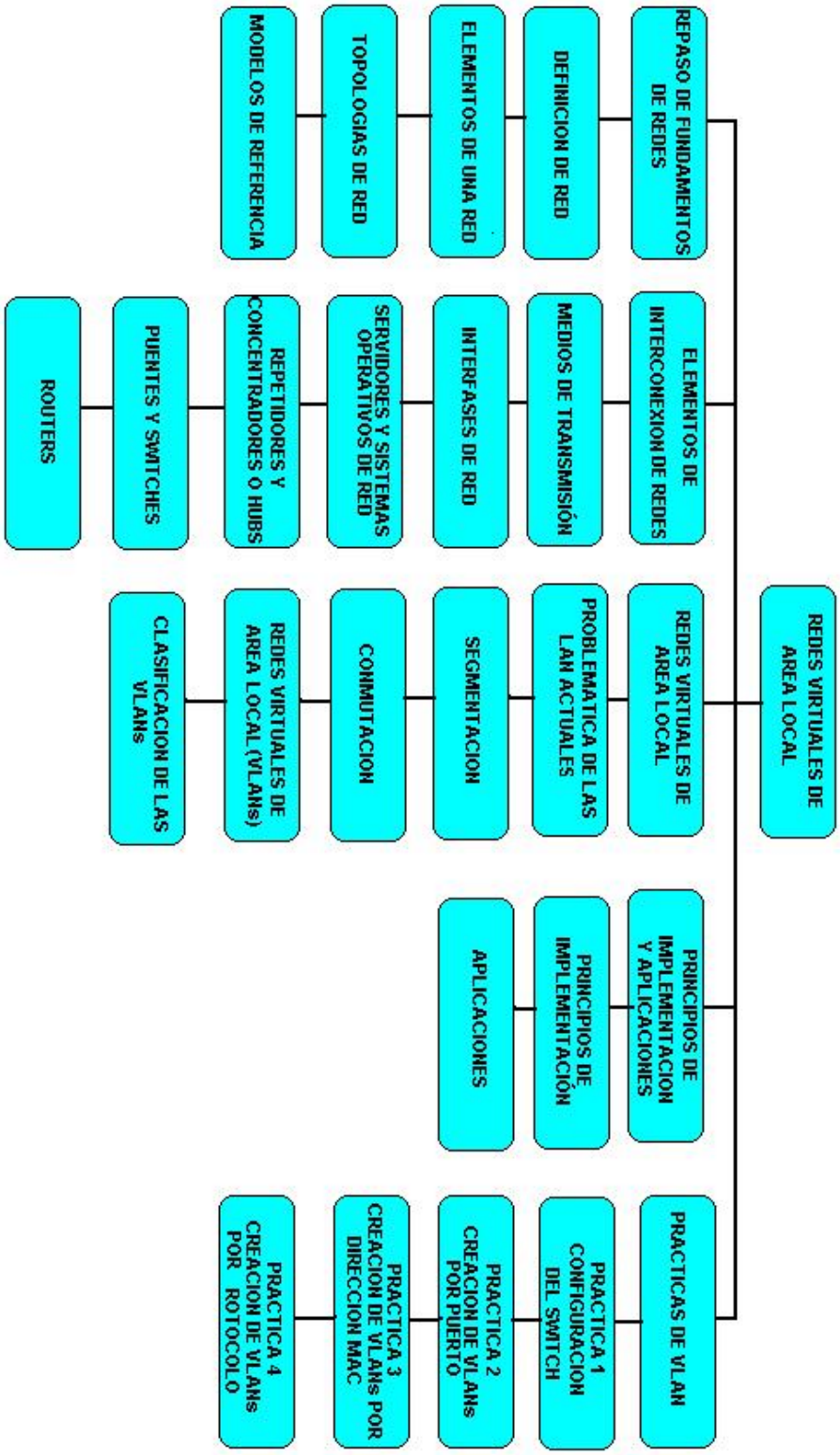
La carrera de Ingeniería en Computación que se imparte en la Facultad de Ingeniería de la UNAM, como parte se su plan de estudios incluye la materia de “Redes de Computadoras”, como continuación de ésta se propone introducir la asignatura optativa de VLANs.

Además, esta tesis sirve como texto básico para ésta asignatura optativa de Redes Virtuales de Área Local (VLANs), que junto con la bibliografía complementaria y las direcciones de páginas web proporcionadas, serán de gran utilidad para el estudio de este tema.

Entre los beneficios que el alumno puede obtener están los siguientes:

- Conocer las características y funcionamiento de las redes VLANs.
- Mostrar como influye la tecnología VLAN en la mejora del desempeño de una Red de Área Local típica.
- El alumno obtendrá un compendio con una explicación de los elementos necesarios para diseñar e implementar redes virtuales de área local (VLANs).
- Proporcionar los conocimientos necesarios que les permitan cubrir exitosamente las expectativas del mercado laboral, en el cual sea necesaria la administración de las VLANs, ampliar su campo de acción tanto en México como en otros países.

5.2 PROGRAMA DE LA ASIGNATURA



REDES VIRTUALES DE AREA LOCAL
Clave: (por asignar)
Número de créditos: 8
Carrera: Ingeniería en Computación
Duración del curso:
Semanas: 16
Horas: 64

Semestre: 10

Horas a la semana:
Teoría: 3.5 Obligatoria:
Practicas: 0.5 Optativa: SI

Temario General

Objetivo:	El alumno conocerá la tecnología y aplicaciones de las Redes Virtuales de Área Local (VLANs), así como las herramientas que existen actualmente para la implementación de ésta clase de redes, con el apoyo de prácticas de laboratorio, las cuales le proporcionarán el conocimiento práctico para reforzar la teoría expuesta en clase.	
UNIDAD	CONTENIDO	HORAS PROPUESTAS
1	REPASO DE FUNDAMENTOS DE REDES	2
2	ELEMENTOS DE INTERCONEXION DE REDES	14
3	REDES VIRTUALES DE AREA LOCAL (VLANs)	20
4	PRINCIPIOS DE IMPLEMENTACION Y APLICACIONES	20
5	PRACTICAS DE VLAN	08
	Total =	64

5.2.1 Objetivos y contenidos de los temas

A continuación se muestra el análisis de tiempos para la asignatura optativa Redes Virtuales de Área Local.

UNIDAD 1 "REPASO DE FUNDAMENTOS DE REDES"

Objetivo: El alumno repasará los conceptos básicos de redes de computadoras

Contenido	Horas propuestas
1.1 Definición de red	0.5
1.2 Elementos de una red	1
1.3 Topologías de Red	0.5
1.4 Modelos de referencia	1

UNIDAD 2 "ELEMENTOS DE INTERCONEXION DE REDES"

Objetivo: El alumno conocerá el equipo necesario para la interconexión de una red haciendo énfasis en los elementos necesarios para construir una Red Virtual de Área Local

Contenido	Horas propuestas
2.1 Medios de transmisión	1
2.2 Interfases de red	2
2.3 Servidores y sistemas operativos de red	1
2.4 Repetidores y Concentradores o Hubs	2
2.6 Puentes y Switches	4
2.8 Routers	4

UNIDAD 3 "REDES VIRTUALES DE AREA LOCAL (VLANs)"

Objetivo: El alumno conocerá la problemática de las redes de área local actuales así como algunas técnicas de segmentación y conmutación para mejorar su rendimiento, y la aplicación de las VLANs como solución a estos problemas.

Contenido	Horas propuestas
3.1 Problemática de la LAN actuales	2
3.2 Segmentación	4
3.3 Conmutación	4
3.4 Redes Virtuales de Área Local (VLANs)	6
3.5 Clasificación de las VLANs	4

UNIDAD 4 "PRINCIPIOS DE IMPLEMENTACION Y APLICACIONES"

Objetivo: El alumno identificará donde se utilizan las redes virtuales de área local, y aprenderá la configuración del switch Catalyst 1900 para la implementación de una VLAN.

Contenido	Horas propuestas
4.1 Principios de implementación	12
4.2 Aplicaciones	8

UNIDAD 5 "PRACTICAS DE VLANs"

Objetivo: El alumno aplicará los conocimientos obtenidos en las unidades 3 y 4 a través de la realización de prácticas de laboratorio.

Contenido	Horas propuestas
5.1 Configuración del switch	2
5.2 Creación de VLANs por puerto	2
5.2 Creación de VLANs por dirección MAC	2
5.2 Creación de VLANs por protocolo	2

5.3 TEMARIO

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE INGENIERÍA

Programa de Asignatura

INGENIERIA ELECTRICA — DIVISION
ING. EN COMPUTACIÓN — DEPARTAMENTO

Programa de la asignatura REDES VIRTUALES DE AREA LOCAL

Clave
No. de créditos: 8 .
Carrera: ING. EN COMPUTACIÓN
Duración del curso Semanas: 16 .
ING. EN TELECOMUNICACIONES
Horas: 64 .
Semestre: 10 .
Horas a la semana Teoría: 3.5 .
Obligatoria:
Practica: 0.5 .
Optativa: X .

Objetivo del curso:

El alumno conocerá la tecnología y aplicaciones de las Redes Virtuales de Área Local (VLANs), así como las herramientas que existen actualmente para la implementación de ésta clase de redes, con el apoyo de prácticas de laboratorio, las cuales le proporcionarán el conocimiento práctico para reforzar la teoría expuesta en clase.

Temas:

Número	Nombre	Horas
1	REPASO DE FUNDAMENTOS DE REDES	2
2	ELEMENTOS DE INTERCONEXION DE REDES	14
3	REDES VIRTUALES DE AREA LOCAL (VLAN)	20
4	PRINCIPIOS DE IMPLEMENTACION Y APLICACIONES	20
5	PRACTICAS DE VLANs	8
		64

UNIDAD 1 "REPASO DE FUNDAMENTOS DE REDES"

Objetivo: El alumno repasará los conceptos básicos de redes de computadoras

Contenido:

1.1 Definición de red
1.2 Elementos de una red
1.3 Topologías de Red
1.4 Modelos de referencia

UNIDAD 2 "ELEMENTOS DE INTERCONEXION DE REDES"

Objetivo: El alumno conocerá el equipo necesario para la interconexión de una red haciendo énfasis en los elementos necesarios para construir una Red Virtual de Área Local

Contenido:

2.1 Medios de transmisión
2.2 Interfases de red
2.3 Servidores y sistemas operativos de red
2.4 Repetidores y Concentradores o Hubs
2.6 Puentes y Switches
2.8 Routers

UNIDAD 3 "REDES VIRTUALES DE AREA LOCAL (VLANs)"

Objetivo: El alumno conocerá la problemática de las redes de área local actuales así como algunas técnicas de segmentación y conmutación para mejorar su rendimiento, y la aplicación de las VLANs como solución a estos problemas.

Contenido:

3.1 Problemática de la LAN actuales
3.2 Segmentación
3.3 Conmutación
3.4 Redes Virtuales de Área Local (VLANs)
3.5 Clasificación de las VLANs

UNIDAD 4 "PRINCIPIOS DE IMPLEMENTACION Y APLICACIONES"

Objetivo: El alumno identificará donde se utilizan las redes virtuales de área local, y aprenderá la configuración del switch Catalyst 1900 para la implementación de una VLAN.

Contenido:

4.1 Principios de implementación
4.3 Práctica de implementación de VLANs
4.2 Aplicaciones

UNIDAD 5 "PRACTICAS DE VLAN"

Objetivo: El alumno aplicará los conocimientos obtenidos en las unidades 3 y 4 a través de la realización de prácticas de laboratorio.

Contenido

5.1 Configuración del switch
5.2 Creación de VLANs por puerto
5.2 Creación de VLANs por dirección MAC
5.2 Creación de VLANs por protocolo

TECNICAS DE ENSEÑANZA:		ELEMENTOS DE EVALUACION:	
Exposición oral	(X)	Exámenes parciales	(X)
Exposición audiovisual	(X)	Exámenes finales	(X)
Ejercicios dentro de clase	(X)	Trabajos y tareas fuera del aula	(X)
Ejercicios fuera del aula	(X)	Participación en clase	(X)
Seminarios	( )	Asistencia a prácticas	(X)
Lecturas obligatorias	(X)		
Trabajo de investigación	(X)		
Prácticas de taller o lab.	(X) *		
Prácticas de campo	( )		

* Nota: El laboratorio se incluye en la materia

ANTECEDENTES:

ASIGNATURA	CLAVE
Redes de Computadoras	0760
Comunicaciones Digitales	0109
Sistemas Operativos	0840

BIBLIOGRAFIA:

Texto	Temas de la materia para los que se recomienda:
TEXTOS BASICOS CARLOS F., Tania L., CAMARGO M., Juan y LORENZO L., Damián “Redes Virtuales (VLANs), su tecnología y sus aplicaciones”	Todos
Tesis De Licenciatura	
TANENBAUM Andrew S. "Computer networks" Prentice Hall, E.E.U.U.,	I, II, III
BERTSEKAS Dimitri y GALLAGER Robert "Data networks" Prentice Hll, 2a. ed., 1992.	I, II
BECKER, Philip L. "Introduction to pc communications" QUE, E.E.U.U., 1992.	I, II
BLACK, Uyless "Computer Networks Protocols, Standars and Interfaces" Prentice Hall. E.E.U.U., 1987.	I, II
GONZALEZ Sainz Nestor "Comunicaciones y redes de procesamiento de datos" Mc Graw-Hill, Colombia, 1987.	I, II
CISCO SYSTEM “Guía del segundo año” Cisco Press, Madrid, 2002.	III, IV
CISCO SYSTEM “Practicas de laboratorio, Volumen II” Cisco Press, Madrid, 2002.	V

5.4 PRACTICAS DE VLANs

En este apartado solo se desarrolla la practica 1 y 2, dejando para trabajo posterior el desarrollo de las demás prácticas con los puntos propuestos o los que el profesor considere conveniente comprobar en el laboratorio. Cabe mencionar que existe un software llamado “Bosom Router Simulator” que permite simular de manera muy sencilla el funcionamiento de redes locales utilizando algunos dispositivos de Cisco como el switch Catalyst de la serie 1912, el cual puede servir como apoyo en el desarrollo de las prácticas.

Práctica 1 Comandos básicos en el Switch Catalyst serie 1900 (Duración estimada 120 min)

Objetivo:
El alumno conocerá el funcionamiento básico del simulador “Bosom Router Simulator”, así como algunos comandos empleados en la construcción de VLANs.

Nota preliminar

Actualmente existen en el mercado algunos switches de varios proveedores que permiten el empleo de comandos para configurar su funcionamiento, y sobre todo, el uso de comandos para configurar VLANs, como es el caso de los switch Catalyst serie 1900 de Cisco.

Específicamente este switch cuenta con tres métodos diferentes de configuración; el método basado en Web usando el VSM (Visual Switch Manager), el método a base de menús desde el puerto de consola y el método de IOS CLI, aunque cada método lleva a cabo las mismas tareas, para usar el VSM requiere que el switch tenga una dirección IP y una conexión de red para comunicarse con alguna PC mediante un navegador como Internet Explorer o Netscape. Los Switches Catalyst serie 1900 traen configurada por default la dirección IP: 0.0.0.0

El simulador Boson Routrer Simulator, es un software para simulación de redes que permite trabajar con un switch Catalyst 1912, el cual tiene 12 puertos 10 base T (nombrados como e0/1 hasta e0/12), un puerto AUI (e0/25) y dos puertos Fast Ethernet 100 base T (fa0/26 port A) y (fa0/27 port B). La diferencia con el switch visto en el capítulo 4 es que, el switch Catalyst 1924 tiene 24 puertos 10 base T (e0/1 hasta e0/24) pero todos los demás componentes son iguales. En este simulador se puede hacer uso de los comandos de MS-DOS para probarla conectividad entre dos PC’s, así como algunas otras funciones.

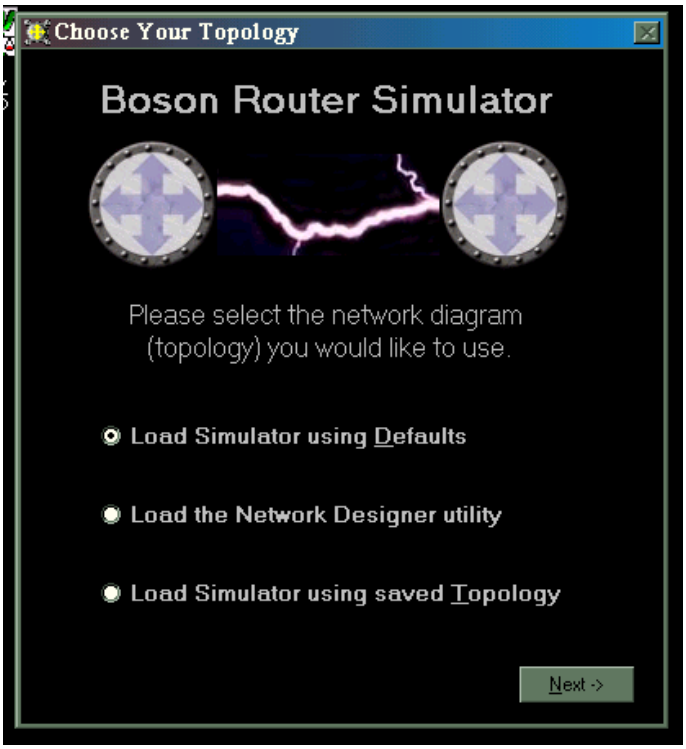
Material y equipo:

En el laboratorio se puede trabajar ya sea con un switch Catalyst 1900 o con el simulador antes mencionado.

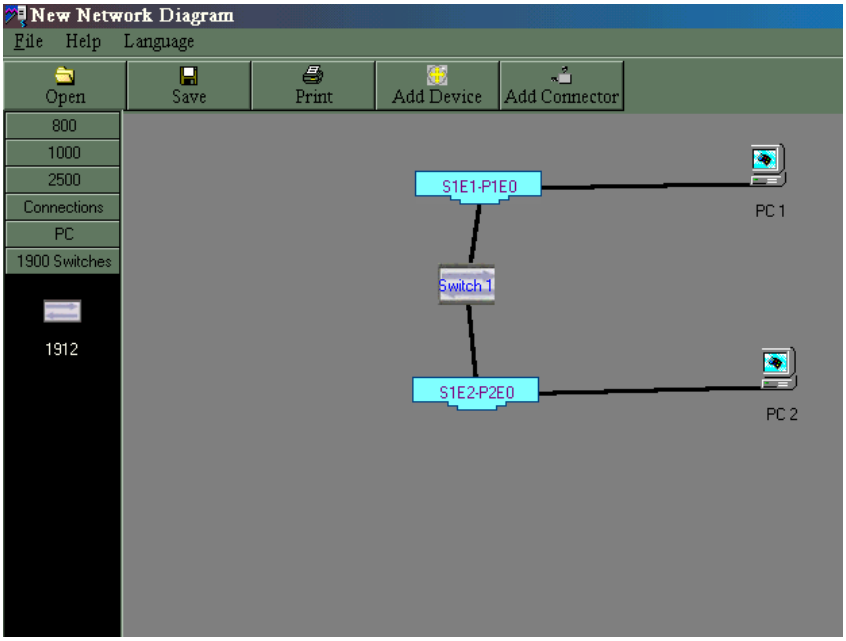
1. PC con win98 o superior.
2. Simulador “Bososm Router Simulator” instalado.

Desarrollo.

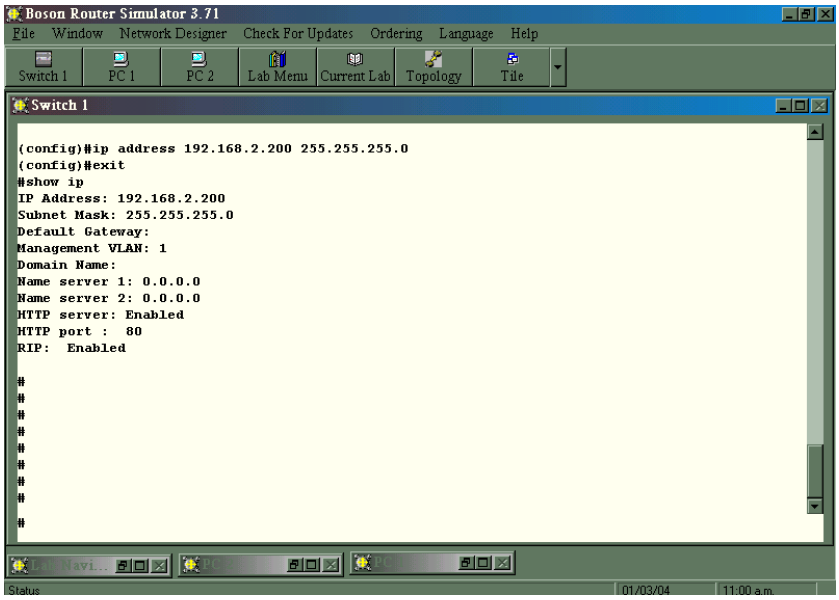
1.- Ejecutar el simulador Bosom Router Simulator



2.- Construya una topología en la cual existan 2 PC's, un switch Catalyst 1912 y 2 enlaces Ethernet.



3.- Ingrese a la consola de configuración de switch.



4.- Una vez en la consola del switch, el comando inicial que usaremos es el comando "?" para obtener información de los comandos que podemos utilizar, escriba los resultados que aparecen en la pantalla.

>?

5.- Configuración de IP: En este caso utilizaremos el comando **"enable"**, después de esto el prompt cambiara al símbolo #.

>enable
#

Podemos usar nuevamente el comando **"?"** para ver los comandos dentro de este menú y tendremos lo siguiente.

#?

Usamos el comando **"show ip"** desde el modo "**EXEC"** para mostrar los valores por default de IP, mascara de subred y gateway, escriba el comando y registre los resultados obtenidos

#show ip

Usamos el comando **"conf term"** para entrar al modo de configuración global, una vez ejecutado este comando, el prompt cambiara nuevamente a (config)#.

(config)#

Aquí utilizaremos el comando **"ip address"** para asignar una IP y mascara de subred, la sintaxis es la siguiente: **(config)#ip address 100.1.120.1 255.255.255.0** donde los primeros cuatro dígitos corresponden a la dirección IP y los siguientes cuatro a la máscara de subred (note que hay un espacio entre las dos direcciones). Investiga con tu profesor si le asignarás una IP de la UNAM o solo una de prueba, al igual que la máscara de subred. La que se muestra es solo como ejemplo.
Para borrar la dirección IP se usa el comando **"no ip address"**, y se le dan los valores 0.0.0.0 0.0.0.0, con esto regresa a los valores por default.

Usamos el comando **"ip default-gateway"** para asignar una puerta de enlace

(config)#ip default-gateway 100.1.121.1

Usamos el comando **"no ip default-gateway"** para regresar a los valores de la puerta de enlace por default (0.0.0.0).

Por último regresamos al modo **"EXEC"** tecleando el comando **"exit"** y desde aquí podemos usar el comando **"show ip"** para ver los valores que hemos configurado.

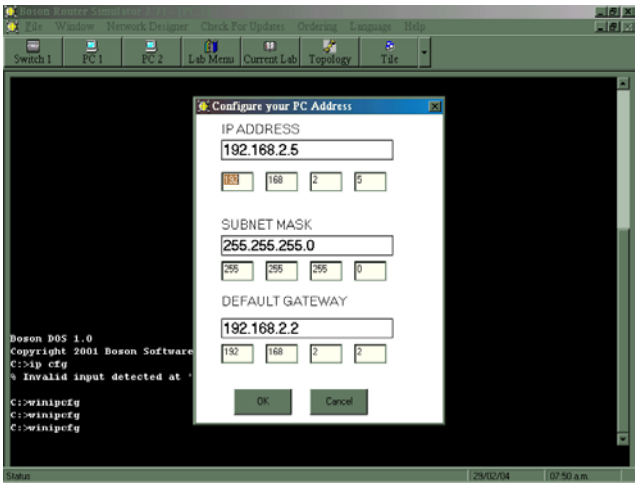
#show ip

IP ardes: 100.1.120.1
Subset mask: 255.255.255.0
Default gateway: 100.1.121.1
Managment VLAN: 1
Domain name:
Name server 1: 0.0.0.0
Name server 2: 0.0.0.0
HTTP server: Enabled
HTTP pport: 80
RIP: Enable

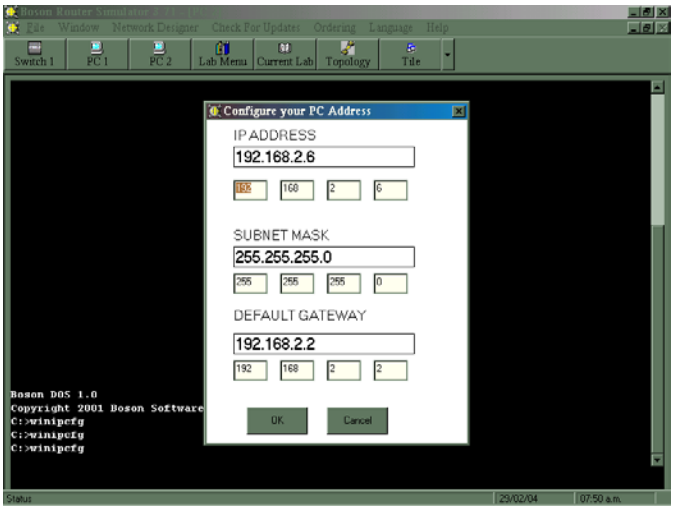
6.- Configurando IP a los host, para esto, deberá acceder a cada una de las ventanas tituladas como PC1 y PC2 para configurar la IP de cada una del terminales, por ejemplo una vez en la ventana de la PC1 tecleamos el comando

>**winipcfg**

una vez ejecutado este comando, aparecerá una pantalla como que se muestra a continuación, donde tendrá que escribir la dirección IP, la mascara de red, y el default getway.



Deberá repetir la misma operación para cada una de las PC's. Cabe mencionar que la IP tiene que ser una perteneciente al grupo de IP's del Switch.



Después de esto deberá usar un comando como el ping, el cual nos permite verificar la comunicación desde la PC al switch y entre ambas PC's.

Conclusiones y resultados.

Práctica 2 "Creación de una VLAN Por puerto" (Duración estimada: 120 minutos)

Objetivos:

- Usar la consola de administración para comprobar las opciones de menú relacionadas con las VLANs.
- Crear dos VLANs, asignarles un nombre y asignar puertos para cada VLAN.
- Comprobar la funcionalidad de las VLANs trasladando una estación de trabajo de una VLAN a otra.

Conocimientos previos:

En esta práctica se trabaja con las Redes Virtuales de Área Local (VLANs) Ethernet. Las VLANs se pueden usar para separar grupos de usuarios en base a su función en vez de su ubicación física. Inicialmente, todos los puertos de un switch están en la misma VLAN predeterminada. Un administrador de red puede crear VLANs adicionales y trasladar algunos puertos a esas VLANs para crear grupos de usuarios aislados, independientemente de dónde se encuentren ubicados. Con esto se crean dominios de difusión más pequeños, lo que ayuda a reducir y localizar el tráfico de red. Si un switch con 24 puertos se divide en dos VLANs de 12 puertos cada una, los usuarios de una VLAN no podrán acceder a los recursos (como servidores o impresoras) de la otra VLAN. Las VLANs también se pueden crear utilizando puertos de múltiples switches que estén "enlazados troncalmente" en un backbone. Para que dos VLANs se comuniquen, deberán estar conectadas por un router.

Para la realización de esta práctica se deberá acceder a la consola del switch y utilizar los comandos para ver las opciones disponibles para administrar las VLANs y comprobar la configuración VLAN activa. Trasladar la conexión de una VLAN a otra a fin de determinar los efectos del dominio de administración. Cuando se administra un switch, el dominio de administración es siempre VLAN 1. La estación de trabajo del administrador de red debe tener acceso al puerto del dominio de administración de VLAN 1. Por defecto, todos los puertos están asignados a VLAN 1.

Antes de empezar esta práctica, se debe tener el simulador "Bosom Router Simulator" instalado, los alumnos deberán trabajar en equipos grandes para adquirir experiencia práctica.

Material y equipo:

En el laboratorio se puede trabajar ya sea con un switch Catalyst 1900 o con el simulador antes mencionado.

3. PC con win98 o superior.
4. Simulador "Bososm Router Simulator" instalado.

Recursos Web:

Fundamentos de la conmutación LAN.
http://www.cisco.com/univercd/cc/td/ doc/cisintwk/ito_doc/lanswtch.htm

Información general sobre todos los productos de Cisco
http://www.cisco.com/univercd/cc/td/doc/pcat/#2

Switches Ethernet de la serie 1900/2820.
http://www.cisco.com/warp/public/cc/cisco/mkt/switch/cat/c1928/prodlit/s1928_ov.htm

Switches Fast Ethernet de la serie 2900.
http://www.cisco.com/warp/public/cc/cisco/mkt/switch/cat/2900xl/prodlit/290xl_ov.htm

Switches Gigabit Ethernet de la serie 3500.
http://www.cisco.com/warp/public/cc/cisco/mkt/switch/cat/3500xl/prodlit/3500x_ov.htm

LAN virtuales para los switches 1900/2820.
http://www.cisco.com/univercd/cc/td/doc/product/lan/28201900/1928v8x/eescg8x/02vlans.htm

Desarrollo:

Paso 1. Acceda a la consola del switch LAN. Responda a las siguientes preguntas.

¿Qué opción de menú del switch se usa para crear o modificar VLAN?

Paso 2. Compruebe la dirección IP y la máscara de subred, del switch y de las estaciones de trabajo para verificar que son compatibles y que están en la misma red, use los comandos vistos en la práctica 1. Escriba su configuración:

IP de switch:_____ Máscara de subred: _____

IP de estación de trabajo 1: _____ Máscara de subred: _____
Gateway predeterminado:_____

IP de estación de trabajo 2: _____ Máscara de subred: _____
Gateway predeterminado: _____

Paso 3. Acceda al modo de configuración VLAN ingresando el comando **"enable"** para entrar a la configuración privilegiada y **"conf term"** para entrar a la configuración global.

>show vlan

```
VLAN  Name                             Status    Ports
----  -------------------------------- --------- -------------------------------
1     default                          Enabled   1-11, AUI, A, B
1002  fddi-default                     Suspended
1003  token-ring-defau                 Suspended
1004  fddinet-default                  Suspended
1005  trnet-default                    Suspended
---------------------------------------------------------------------------------
VLAN  Type  SAID       MTU   Parent RingNo BridgeNo Stp      Trans1 Trans2
```

```
-------------------------------------------------------------------------------------------------------------
1     Ethernet        100001 1500  0     0     0     Unkn  1002  1003
1002  FDDI            101002 1500  0     0     0     Unkn  1     1003

1003  Token-Ring      101003 1500  1005  1     0     Unkn  1     1002
1004  FDDI-Net        101004 1500  0     0     1     IEEE  0     0
1005  Token-Ring-Net  101005 1500  0     0     1     IEEE  0     0
-------------------------------------------------------------------------------------------------------------
```

```
>enable
#?
Clear                Reset functions
Configure            Enter configuration mode
Copy                 Copy configuration or firmware
Delete               Reset configuration
Disable              Turn off privileged commands
Enable               Turn on privileged commands
Exit                 Exit from the EXEC
Help                 Description of the interactive help system
Ping                 Send echo messages
Reload               Halt and perform warm start
Show                 Show running system information

#conf term
(config)#vlan ?
<1-1001>         ISL VLAN index
```

Paso 4. Utilizando las opciones de menú de la VLAN, configure las VLANs.

Compruebe la configuración de la VLAN predeterminada seleccionando la opción. ¿Cuáles son los puertos integrantes de VLAN 1?

Con el comando (**config)#vlan *numero*** cree una nueva VLAN Ethernet y asígnele un nombre.

```
(config)#vlan 2 ?
<cr>
ethernet         ethernet
fddi             fddi
mtu              VLAN MTU
name             Set VLAN name
sde              IEEE 802.10 Said
state            VLAN state
(config)#exit
#show vlan 2

VLAN             Name             Status           Ports
---------------------------------------------------------------------
2                VLAN0002         Enabled
---------------------------------------------------------------------
```

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	Trans1	Trans2
2	Ethernet	100002	1500	0	1	1	Unkn	0	0

Use el comando **#name vlan-name** para asignar un nombre al la VLAN.
¿Qué nombre le ha dado?

¿Cuál es el número de VLAN de la nueva VLAN?

Enumere los pasos necesarios para crear y asignar un nombre a la nueva VLAN:

Para asignar un Puerto a una VLAN deberás utilizar el comando**"(config)#interface"**

```
(config)#interface ?
Ethernet          IEEE 802.3
FastEthernet      FastEthernet IEEE 802.3

(config)#interface ethernet ?
<0-0>/<1-25>      IEEE 802.3
```

En este ejemplo vamos a asignar el Puerto 6 a la VLAN 2

```
(config)#interface ethernet 0/7
(config-if)#?
Cdp                   Cdp interface subcommands
description           Interface specific description
duplex                Configure duplex operation
exit                  Exit from interface configuration mode
port                  Perform switch port configuration
shutdown              Shutdown the selected interface
spantree              Spanning tree subsystem
vlan-membership       VLAN membership configuration

(config-if)#vlan-membership ?
dynamic           Set VLAN membership type as dynamic
static            Set VLAN membership type as static
```

Asignamos el tipo de VLAN estática

```
(config-if)#vlan-membership static ?
<1-105>           ISL VLAN index
```

Agregamos el número de VLAN al que asignaremos este puerto

```
(config-if)#vlan-membership static 2
(config-if)#exit
(config)#exit
#show vlan

VLAN      Name                Status          Ports
```

```
---------------------------------------------------------------------------------------------
1          default              Enabled       1-5, 7-12, AUI, A, B
2          VLAN0002             Enabled       6
1002       fddi-default         Suspended
1003       token-ring-default   Suspended
1004       fddinet-default                Suspended
1005       trnet-default        Suspended
---------------------------------------------------------------------------------------------
```

Asigne los puertos 7 a 12 a la nueva VLAN. Enumere los pasos necesarios para hacerlo:

Compruebe nuevamente la VLAN 1. ¿Qué cambios observa?

Salga al menú principal y diríjase a la consola de administración.

Paso 5. Pruebe la funcionalidad de las dos VLANs.

Para ver la VLAN en acción, configure dos estaciones de trabajo y verifique que las direcciones IP están en la misma subred (véase el Paso 2). Conecte la estación de trabajo 1 a uno de los puertos del 1 al 6 del switch. Conecte la estación de trabajo 2, a uno de los puertos del 1 al 6 del switch.

Haga un ping a cada estación de trabajo. ¿Ha tenido éxito el ping?

Ahora conecte la estación de trabajo 2 a uno de los puertos de la VLAN 2 (puertos 7 a 12). Haga un nuevo ping a cada estación de trabajo. ¿Ha tenido éxito el ping?

Resultados y Conclusiones.

CONCLUSIONES

Con la realización de este trabajo nos hemos percatado que debido al constante aumento en la capacidad de procesamiento de los equipos de computo, aunado al desarrollo de aplicaciones cada día más exigentes en cuanto recursos se refiere, las redes LAN tradicionales sufren constantemente de congestión y otros problemas relacionados con el ancho de banda.

Para aliviar la congestión de red, es necesario que haya mas ancho de banda disponible y sobre todo, que se use de forma eficaz, por lo que proponemos el uso de Redes Virtuales de Área Local como la solución optima para el mejor aprovechamiento del ancho de banda, ya que mediante su empleo, podemos tener los beneficios de la segmentación y la conmutación juntos.

Uno de estos beneficios tienen que ver con que en una LAN segmentada, se reduce la cantidad de trafico ya que solo los equipos ubicados en un segmento, verán el trafico correspondiente a dicho segmento, sin perjudicar otras partes de la red; otro beneficio es que una LAN conmutada utiliza el ancho de banda muy eficientemente pues utilizan conmutadores o switches, los cuales puede iniciar el reenvío de un paquete antes de haberlo recibido por completo, lo que redunda en una mejora de prestaciones.

Además de estos beneficios, las VLAN permiten la movilidad de los usuarios a través de la red sin tener que hacer grandes cambios en ella.

Cabe mencionar que se presentaron algunos contratiempos, como es el hecho de que, aunque el tema de las Redes Virtuales de Área Local existe desde hace mucho tiempo, la información que se encuentra acerca de este tema es muy escasa y la que existe, no se adentra tanto en detalles importantes si se quiere implementar una VLAN.

Debido a que proponemos la asignatura optativa de “Redes Virtuales de Área Local”, algo que pudimos darnos cuenta es que la materia de “Redes de Computadoras” se encuentra en el 10º semestre, por lo que aconsejamos que esta materia pueda darse en un semestre menor para que puedan crearse módulos de especialización en la carrera de Ingeniería en Computación, y recomendamos esta tesis como texto básico para dicha asignatura optativa.

Las prácticas que proponemos, inicialmente consideramos desarrollarlas físicamente, pero el problema con que nos topamos fue que, en la Facultad de Ingeniería no existen switches con los que se puedan trabajar en el laboratorio, pues los que existen, se están usando para la red de la Facultad. Por esto, nos dimos a la tarea de buscar un software que nos permitiera simular el funcionamiento de una red LAN y sobre todo, de redes VLAN.

El simulador que utilizamos es “Bosom Router Simulator”, del cual conseguimos una versión de evaluación que no es muy completa, por lo cual recomendamos que de ser posible se compre dicho software, para que estén disponibles todos sus componentes.

GLOSARIO

A

ACL (Lista de control de acceso, Access Control List). Una lista que mantiene un router Cisco para controlar el acceso a un router de una serie de servicios (por ejemplo, impedir que ciertos paquetes provistos de una determinada dirección IP abandonen una determinada interfaz del router).

Acuse de recibo. Una notificación enviada desde un dispositivo de red hasta otro para confirmar que se ha producido un determinado evento (por ejemplo, la recepción de un mensaje). A veces, se abrevia como ACK.

Algoritmo de árbol de extensión. Un algoritmo que utiliza el algoritmo de árbol de extensión para crear un árbol de extensión. A veces se abrevia como STA.

Ancho de banda. La diferencia entre las frecuencias superior e inferior disponible para las señales de red. Además, la capacidad de rendimiento de un determinado medio o protocolo de red.

Anillo. Una conexión de dos o más estaciones de una topología circular lógica. La información se pasa secuencialmente entre estaciones activas. Token Ring, FDDI y CDDI están basadas en esta topología.

Aplicación cliente/servidor. Una aplicación que está almacenada en un servidor y a la que acceden las estaciones de trabajo, haciendo que su mantenimiento y protección sea más fácil.

AppleTalk. Un conjunto de protocolos de comunicaciones diseñada por Apple Computer que consta de dos fases. La Fase 1, que es la primera versión, soporta una sola red física que sólo puede tener un número de red y estar en una zona. La Fase 2 soporta múltiples redes lógicas en una sola red física y permite que las redes están en más de una zona. Véase también zona.

Árbol de extensión. Un subconjunto sin bucles de una topología de red sin bucles de Capa 2 (conmutada).

ARP (Protocolo de resolución de direcciones, Address Resolution Protocol). Un protocolo de Internet que se usa para asignar una dirección IP a una dirección MAC. Definido en la RFC 826. Compárese con RARP.

ASIC (Circuitos Integrados de Aplicación Especifica). Un **ASIC** es un circuito integrado para aplicaciones específicas.

Atenuación. Pérdida de la potencia de la señal de comunicación.

ATM (Modo de transferencia asíncrona, Asynchronous Transfer Mode). Un estándar internacional para la distribución de celdas en el que múltiples tipos de servicio (como la

voz, el vídeo o los datos) son transportados en celdas de longitud fija (de 53 bytes). Las celdas de longitud fija permiten que tenga lugar el procesamiento de celda en el hardware, reduciendo así los retrasos de tránsito. ATM está diseñado para aprovecharse de las ventajas de los medios de transmisión de alta velocidad, como E3, SONET y T3.

B

BPDU (Unidad de datos del protocolo de puente, Bridge Protocol Data Unit). Un paquete hello del Protocolo de árbol de extensión que se envía a intervalos configurables con el fin de intercambiar información entre los puentes de la red.

Búfer de memoria. El área de memoria donde el switch almacena el destino y la transmisión de datos.

C

CAM (Memoria de contenido direccionable, Content-Addressable Memory). Memoria que mantiene una base de datos de reenvío exacta y funcional.

Colisión. En Ethernet, el resultado de dos nodos transmitiendo a la vez. Las tramas de cada dispositivo colisionan y quedan dañadas cuando confluyen en el medio físico.

Conexión punto a punto. Uno de los dos tipos de conexión principales. En ATM, una conexión punto a punto puede ser una conexión unidireccional o bidireccional entre dos sistemas finales ATM. Compárese con conexión punto a multipunto.

Congestión. El exceso de tráfico que supera la capacidad de la red.

Conmutación. El proceso de tomar una trama de entrada desde una interfaz y de enviarla a través de otra interfaz.

CSMA/CD (Acceso múltiple con detección de carrier y detección de colisiones, Carrier Sense Multiple Access Collision Detect). Un mecanismo de acceso al medio en el que los dispositivos listos para transmitir datos comprueban el canal para ver si hay una portadora. Si no se detecta ningún carrier durante un periodo de tiempo específico un dispositivo podrá transmitir. Si dos dispositivos transmiten a la vez, se producirá una colisión, que será detectada por todos los dispositivos del dominio de colisión colindantes Esta colisión retrasa la retransmisión desde estos dispositivos durante un periodo de tiempo aleatorio. Ethernet e IEEE 802.3 utilizan el acceso CSMA/CD.

D

DHCP (Protocolo de configuración dinámica del host, Dynamic Host Configuration Protocol). Un protocolo que proporciona un mecanismo para asignar direcciones IP dinámicamente, de forma que éstas puedan ser reutilizadas automáticamente cuando los hosts ya no las necesiten.

Difusión. Un paquete de datos que se envía a todos los nodos de una red. Las difusiones vienen identificadas por una dirección de difusión.

Dirección de difusión. Una dirección especial reservada para el envío de un mensaje a todas las estaciones. Generalmente, una dirección de difusión es una dirección de destino MAC con todo unos.

Dirección de multidifusión. Una dirección única que hace referencia a múltiples dispositivos de red. Es sinónimo de dirección de grupo.

Dirección de unidifusión. Una dirección que especifica un solo dispositivo de red.

Dirección IP. Una dirección de 32 bits que se asigna a los hosts por medio de TCP/IP. Una dirección IP pertenece a una de cinco clases (A, B, C, D o E) y está escrita como cuatro octetos separados por puntos (es decir, en formato decimal con puntos). Cada dirección consta de un número de red, un numero de subred opcional y un número de host. Los números de red y subred se usan para el enrutamiento, y el número de host se utiliza para dirigirse a un host individual de la red o subred. Una máscara de subred se usa para extraer información de red y subred de la dirección IP. También se llama dirección de Internet.

Dirección MAC. Una dirección de capa de enlace de datos necesaria en todo puerto o dispositivo que se conecte con una LAN. Otros dispositivos de la red utilizan estas direcciones para localizar puertos específicos de la red y para crear y actualizar tablas de enrutamiento y estructuras de datos. Una dirección MAC tiene 6 bytes. Las direcciones MAC están controladas por el IEEE y también se conocen como direcciones de hardware, direcciones de capa MAC o direcciones físicas. Compárese con dirección de red.

DNS (Sistema de denominación de dominio, Domain Name System). Un sistema que se emplea en Internet para traducir los nombres de los nodos de red en direcciones.

Dominio de colisión. En Ethernet, el área de red en la que se propagan las tramas que hayan colisionado. Los repetidores y hubs propagan colisiones, mientras que los switches, puentes y routers LAN no lo hacen.

Dominio de difusión. El conjunto de dispositivos que recibirán las tramas de difusión que se originan desde cualquiera de los dispositivos del conjunto. Estos dominios suelen estar limitados por routers, ya que estos últimos no reenvían tramas de difusión.

Dúplex. La capacidad de transmisión de datos simultánea entre una estación emisora y otra receptora.

E

Enlace punto a punto. Un enlace que proporciona una ruta de comunicaciones WAN única y preestablecida desde las dependencias del cliente a través de la red carrier, como una compañía telefónica, hasta una red remota. También se llama línea dedicada.

Enrutamiento. El proceso de localizar una ruta a un host de destino. El enrutamiento es muy complejo en redes muy grandes, debido a los numerosos destinos intermedios potenciales que podría atravesar un paquete antes de llegar a su host de destino.

Ethernet de dúplex. Una opción para la transmisión simultánea de datos entre una estación remitente y otra receptora.

Ethernet de semidúplex. Una opción para la transmisión de datos en una sola dirección a la vez entre una estación remitente y otra receptora.

Ethernet. Una especificación LAN de banda base inventada por Xerox Corporation y desarrollada conjuntamente por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet utilizan CSMA/CD y se ejecutan sobre una serie de tipos de cable a 10 Mbps. Ethernet es parecida a la serie de estándares IEEE 802.3.

F

Fast Ethernet. Cualquiera de las especificaciones Ethernet de 100 Mbps. Fast Ethernet ofrece un incremento de velocidad diez veces superior al de la especificación 10BaseT Ethernet, conservando cualidades como el formato de trama, los mecanismos MAC y la MTU. Tales similitudes permiten el uso de las aplicaciones 10BaseT existentes y las herramientas de gestión de red en redes Fast Ethernet. Se basa en una extensión de la especificación IEEE 802.3.

FDDI (Interfaz de datos distribuidos por fibra, Fiber Distributed Data Interface). Un estándar LAN, definido por la X3T9.5 del ANSI, que especifica una red de transmisión de testigos de 100 Mbps que utiliza cable de fibra óptica, con distancias de transmisión de hasta 2 km. FDDI utiliza una arquitectura de anillo doble con el fin de proporcionar redundancia.

Filtro. Por regla general, un proceso o dispositivo que detecta el tráfico de red en lo que respecta a algunas de sus características, como la dirección de origen, la dirección de destino o protocolo, y que determina si va a reenviar o descartar el tráfico en base a los criterios establecidos.

Firewall. Un router de un servidor de acceso, o varios routers de servidores de acceso, que está designado como búfer entre cualquier red pública conectada y una red privada. Un router firewall utiliza listas de control de acceso y otros métodos para garantizar la seguridad de la red privada.

Fragmentación. El proceso de división de un paquete en unidades más pequeñas cuando se transmite sobre un medio de red que no puede soportar el tamaño original del paquete.

FTP (Protocolo de transferencia de archivos, File Transfer Protocol). Un protocolo de aplicación, parte de la pila del protocolo TCP/IP, que se usa para transferir archivos entre nodos de red. FTP está definido en la RFC 959.

G

Gateway. En la comunidad IP, un término que se refiere a un dispositivo de enrutamiento. Actualmente, el término router se usa para describir los nodos que llevan a cabo esta función, mientras que gateway hace referencia a un dispositivo de propósito especial que

realiza una conversión de la información de la capa de aplicación de una pila del protocolo a la otra.

H

Host. Un sistema computacional de una red. Parecido al nodo, exceptuando que host suele aludir a un sistema computacional, mientras que nodo suele aplicarse a cualquier sistema de red, incluyendo el acceso a los servidores y los routers.

HTTP (Protocolo de transferencia de hipertexto, Hypertext Transfer Protocol). El protocolo que utilizan los navegadores web y los servidores web para transferir archivos, como archivos de texto y archivos gráficos.

Hub. 1) Por regla general, un dispositivo que sirve como centro de una red de topología en estrella. También llamado repetidor multipuerto. 2) Un dispositivo de hardware o software que contiene múltiples módulos independientes (pero conectados) de equipos de red e internetwork. Los hubs pueden ser activos (donde repiten las señales que se envían a través de ellos) o pasivos (no repiten$_1$ sólo dividen, las señales que se envían a través de ellos).

I

ICMP (Protocolo de mensajes de control en Internet, Internet Control Message Protocol). Un protocolo de Internet de la capa de red que indica errores y proporciona información relevante para el procesamiento de paquetes IP. Documentado en la RFC 792.

Interfaz de red. El límite entre una red de proveedor de servicios y una instalación privada.

Internet. La red global más grande, que conecta decenas de miles de redes a nivel mundial y que se centra en la investigación y en la normalización en base al uso en la vida real. Muchas de las tecnologías de redes más avanzadas proceden de la comunidad Internet. Internet se desarrolló a partir de ARPANET. Se le llamó DARPA Internet, término que no hay que confundir con el término general internet.
Intranet. Una red interna a la que acceden los usuarios que tengan acceso a la LAN interna de una organización.

Inundación. Una técnica de paso de tráfico que utilizan los *switches y* los puentes en los que el tráfico que se recibe en una interfaz es enviado a todas las interfaces de ese dispositivo, a excepción de la interfaz en la que se recibió originariamente la información.

IP (Protocolo de Internet, Internet Protocol). Un protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork sin conexión. IP proporciona funciones para el direccionamiento, la especificación de tipo de servicio, la fragmentación y el reensamblado *y* la seguridad. Se define en la RFC 791. IPv4 (Protocolo Internet versión 4) es un protocolo de conmutación de paquetes sin conexión y de máximo esfuerzo de entrega

IPv6 (IP versión 6). Un sustituto de la versión actual de IP (versión 4). IPv6 incluye

soporte para el 1') de flujo en la cabecera de paquete, que se puede usar para identificar los flujos. Anteriormente llamado IPng (IP de próxima generación).

L

LAN (Red de área local, Local-Area Network). Una red de datos de alta velocidad y de bajo índice de errores que cubre un área geográfica relativamente pequeña (hasta unos miles de metros). Las LAN conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un solo edificio u otra área limitada geográficamente. Los estándares LAN especifican el cableado y la señalización de las capas de enlace de datos y física del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN ampliamente utilizadas.

Latencia. El retraso entre el tiempo que tarda un dispositivo en solicitar acceso a una red *y* el momento en que se le permite transmitir.

M

MAC (Control de acceso al medio, *Medía Access Control).* La parte de la capa de enlace de datos que incluye la dirección de 6 bytes (48 bits) del origen *y* del destino, así como el modo de obtener permiso para transmitir. Véase también capa de enlace de datos *y* LLC.

MAN (Red de área metropolitana, *Metropolitan Area Network).* Una red que abarca un área metropolitana. Por regla general, una MAN abarca un área geográficamente más pequeña que la de una WAN. Compárese con LAN *y* WAN.

Máscara de subred. Una máscara que se usa para extraer información de redes *y* sobre las subredes de la dirección IP.

Microsegmentación. La división de una red en fragmentos más pequeños, generalmente con la intención de aumentar el ancho de banda añadido para los dispositivos de red.

MTU (Unidad máxima de transmisión, *Maximum Transmissíon Unít).* Tamaño máximo de un paquete, en bytes, que puede manejar una determinada interfaz.

Multidifusión. Paquetes únicos copiados por una red *y* enviados a una serie de direcciones de red. Estas direcciones están especificadas en el campo de dirección de destino. Compárese con difusión *y* unidifusión.

N

NetBEUI (Interfaz de usuario NetBIOS extendida, *NetBIOS Extended User InteTface).* Una versión mejorada del protocolo NetBIOS que utilizan los sistemas operativos de red, como LAN Manager, LAN Server, Windows para grupos de trabajo *y* Windows NT. NetBEUI formaliza la trama de transporte *y* e incorpora funciones adicionales. NetBEUI implementa el protocolo OSI LLC2.

NetBIOS (Sistema básico de entrada/salida de red, *Netu>ork Basic InputlOutput System).* Una interfaz de programación de aplicaciones que utilizan las aplicaciones de una LAN IBM para solicitar servicios de los procesos de red de nivel inferior. Entre estos servicios se pueden incluir el establecimiento *y* el cierre de la sesión, *y* la transferencia de información.

NetWare. Un NOS desarrollado por Novell. Proporciona el acceso transparente a archivos remotos *y* numerosos servicios de redes distribuidas.

NOS (Sistema operativo de red, *Network Operating System).* El sistema operativo que se usa para ejecutar una red como Novell NetWare *y* Windows NT.

P

Paquete hello. Un paquete multidifusión que utilizan los *routers* que emplean ciertos protocolos de descubrimiento *y* recuperación de vecinos. Los paquetes hello también notifican que un cliente sigue funcionando *y* que la red está lista.

Paquete. Un agrupamiento lógico de información que incluye una cabecera que contiene información de control *y* (generalmente) datos de usuario. Los paquetes suelen utilizarse para hacer referencia a unidades de datos de la capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir agrupamientos lógicos de información de las distintas capas del modelo de referencia OSI *y* de varios círculos tecnológicos.

Protocolo de árbol de extensión. Un protocolo puente que utiliza el algoritmo de árbol de extensión, permitiendo que un puente trabaje dinámicamente con los bucles de tina topología de red creando un árbol de extensión. Los puentes intercambian mensajes BPDU con otros puentes para detectar bucles, *y* luego los eliminan cerrando las interfaces de puente seleccionadas. Hace referencia al estándar STA del IEEE 802.1 *y* al primer STA de Digital Equipment Corporation, en el que se basa. La versión IEEE soporta dominios de puente *y* permite que éste construya una topología sin bucles por una LAN extendida. La versión del IEEE suele ser más utilizada que la versión de Digital.

Protocolo de enrutamiento. Un protocolo que lleva a cabo el enrutamiento a través de la implementación de un protocolo de enrutamiento espedfico. Ejemplos de protocolos de enrutamiento son IGRP, OSPF *y* RW Compárese con protocolo enrutado.

Protocolo enrutado. Un protocolo que puede ser enrutado por un *router.* Un *router* debe ser capaz de interpretar la *internetwork* lógica, tal *y* como especifique ese protocolo enrutado. Ejemplos de protocolos enrutados son AppleTalk, DECnet e IP. Compárese con protocolo de enrutamiento.

Protocolo. Una descripción formal de una serie de reglas *y* convenciones que rigen cómo los dispositivos de una red intercambian información.

Puente. Un dispositivo que conecta *y* pasa paquetes entre dos segmentos de red que usan el mismo protocolo de comunicaciones. Los puentes operan en la capa de enlace de datos (la Capa 2) del modelo de referencia OSI. Por regla general, un puente filtra,

reenvía o inunda una trama de entrada en base a la dirección MAC de esa trama.

R

RARP (Protocolo de resolución inversa de direcciones, *Reverse Address Resolution Protocol).* Un protocolo de la pila TCP/IP que proporciona un método de localización de direcciones IP basándose en las direcciones MAC. Compárese con ARP.

Red plana. Una red en la que no hay *routers* colocados entre los *switches,* en las que las difusiones *y* las transmisiones de Capa 2 son enviadas a cada puerto conmutado, *y* donde hay un dominio de difusión para toda la red.

Red. Una colección de computadoras, impresoras, *routers, switches y* otros dispositivos que son capaces de comunicarse entre sí a través de un medio de transmisión.

Redundancia. 1). En *internetworking,* la duplicación de dispositivos, servicios o conexiones, de forma que, en caso de fallo, los dispositivos, servicios o conexiones redundantes pueden llevar a cabo el trabajo de los que fallaron.

Repetidor. Un dispositivo que regenera *y* propaga señales eléctricas entre dos segmentos de red.

Router. Un dispositivo de capa de red que utiliza una o más métricas para determinar la ruta óptima por la que hay que reenviar el tráfico de red. Los *routers* reenvían paquetes desde una red a otra en base a la información de la capa de red. A veces se le llama *gateway* (aunque esta definición se está quedando obsoleta).

S

Segmentación. El proceso de dividir un solo dominio de colisión en dos o más dominios de colisión con el fin de reducir las colisiones *y* la congestión de la red.

Semidúplex. La capacidad de transmisión de datos en un solo sentido a la vez entre una estación emisora *y* otra receptora. Compárese con dúplex *y* unidirecdonal.

Servidor. Un nodo o programa de software que proporciona servicios a los clientes. Véase también cliente.

SNMP (Protocolo simple de administración de redes, Simple Network Management Protocol). Un protocolo de administración de redes que se usa casi exclusivamente en redes TCP/IP. SNMP proporciona una forma de controlar los dispositivos para redes *y* administrar las configuraciones, estadísticas, recopilación, rendimiento *y* seguridad.
Sobrecarga. Una parte de una celda, trama o paquete que contiene información de capa superior (datos).

STP (Par trenzado apantallado, Shielded Twisted-Pair). Un medio de cableado de dos pares que se emplea en una serie de implementaciones de red. El cableado STP tiene una capa de aislamiento para reducir las EMI. Compárese con UTP.

Switch LAN. Un *switch* de alta velocidad que reenvía paquetes entre segmentos de enlace de datos. La mayoría de los *switches* LAN reenvían el tráfico en base a las direcciones MAC. Los *switches* LAN suelen estar categorizados en función del método que usan para reenviar el tráfico: conmutación de paquetes por método de corte o conmutación de paquetes de almacenamiento *y* reenvío. Un ejemplo de *switch* LAN es el Cisco Catalyst 5000.

Tabla de enrutamiento. Una tabla almacenada en un *router* o cualquier otro dispositivo de *internetworking* que controla las rutas a destinos de red concretos *y,* en algunos casos, la métrica asociada a estas rutas.

TCP (Protocolo para el control de la transmisión, *Transmission Control Protocol).* Un protocolo de capa de transporte orientado a la conexión que proporciona la transmisión de datos dúplex fiable. TCP forma parte de la pila del protocolo TCP/IP.

TCP/IP (Protocolo para el control de la transmisión/Protocolo Internet, *Transmission Control ProtocoUInternet Protocol).* Un nombre común para el conjunto de protocolos desarrollado por el DoD de los EE.UU. en los años setenta para soportar la construcción de *internetworks* a nivel mundial. TCP e IP son los dos protocolos más conocidos del conjunto.

Telnet. Un protocolo de emulación de terminal estándar de la pila del protocolo TCP/IP. Telnet se usa para la conexión de terminales remotos, permitiendo a los usuarios conectarse a sistemas remotos *y* utilizar los recursos como si estuvieran conectados a un sistema local. Telnet está definido en la RFC 854.

Token Ring. Una LAN de paso de testigo desarrollada *y* mantenida por IBM. Token Ring se ejecuta a 4 ó 16Mbps sobre una topología en anillo. Parecido a IEEE 802.5.

Topología. Una organización física de nodos de red *y* medios en una estructura de *networking* empresarial.

Tormenta de difusión. Un evento de red no deseable en el que se envían muchas ditusiones simultáneamente por todos los segmentos de red. Una tormenta de difusión emplea un ancho de banda de red sustancial *y,* generalmente, origina limites de tiempo en la red. Véase también difusión.

Trama. Un agrupamiento lógico de información que se envía como unidad de capa de enlace de datos por un medio de transmisión. Suele hacer referencia a la cabecera *y* a la información final *y* se usa en la sincronización *y* el control de errores de los datos de usuario que contiene la unidad. Los términos datagrama, mensaje, paquete y segmento también se emplean para describir agrupamientos lógicos de información de las distintas capas del modelo de referencia OSI *y* de distintos circulos tecnológicos.

Unidifusión. Un mensaje que se envía a un solo destino de la red.

UTP (Par trenzado sin apantallar, *Unshielded Tu'isted-Pair).* Un medio de cableado de cuatro pares que se usa en varios tipos de redes. El UTP no requiere el espacio fijo entre conexiones que es necesario en las conexiones de tipo coaxial. Existen cinco tipos de

cableado UTP: el cableado de Categoría 1, el cableado de Categoría 2, el cableado de Categoría 3, el cableado de Categoría 4 *y* el cableado de Categoría 5. Compárese con STP.

BIBLIOGRAFIA

TANENBAUM Andrew S.
"Computer networks"
Prentice Hall, E.E.U.U.,

BERTSEKAS Dimitri y GALLAGER Robert
"Data networks"
Prentice Hll, 2a. ed., 1992.

BECKER, Philip L.
"Introduction to pc communications"
QUE, E.E.U.U., 1992.

BLACK, Uyless
"Computer Networks Protocols, Standars and Interfaces"
Prentice Hall. E.E.U.U., 1987.

GONZALEZ Sainz Nestor
"Comunicaciones y redes de procesamiento de datos"
Mc Graw-Hill, Colombia, 1987.

CISCO SYSTEM
"Guía del segundo año"
Cisco Press, Madrid, 2002.

CISCO SYSTEM
"Practicas de laboratorio, Volumen II"
Cisco Press, Madrid, 2002

HELD, Gilbert y WILEY, Edit.
"Virtual LANs Construction, Implementation and Management"

CLAK, Kennedy y HALLMILTON, Kevin.
"Cisco LAN Switching"
Edit Ciscopress

S. LONG, Carmac
"Cisco Internetworking & Troubleshooting"
Edit McGranw Hill

Innokenty Rudenk and Tsunami Computing
"Cisco Routers for IP Networking"
Edit Coriolis

ODOM, Sean y NOTTINGHAM, Hanson
“Cisco Switching”
Edit Coriolis

TERE, Parnell
“Guía de redes de alta velocidad”
Serie LAN Time
Edit Osborne McGraw Hill

BLACK, Uyless
“Redes de Computadoras Protocolos, Normas e Interfaces”
Edit Alfa Omega