

11126
16



**UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO**

**FACULTAD DE ESTUDIOS SUPERIORES
CUAUTITLAN**

COMUNICACIONES
"CONFIGURACIONES DEL SWITCH CISCO CATALYST 1900"

TRABAJO DE SEMINARIO
QUE PARA OBTENER EL TITULO DE:
INGENIERO MECANICO ELECTRICISTA
P R E S E N T A :
JOSE IGNACIO CHAVEZ SALADINO

ASESOR: ING. MARICELA SERRANO FRAGOSO.

CUAUTITLAN IZCALLI, EDO. DE MEX.

2003

A



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

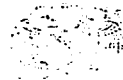
El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.



INSTITUTO NACIONAL
DE ESTUDIOS
SUPERIORES

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN
UNIDAD DE LA ADMINISTRACION ESCOLAR
DEPARTAMENTO DE EXAMENES PROFESIONALES

U. N. A. M.
FACULTAD DE ESTUDIOS
SUPERIORES-CUAUTITLAN



DEPARTAMENTO DE
EXAMENES PROFESIONALES

DR. JUAN ANTONIO MONTARAZ CRESPO
DIRECTOR DE LA FES CUAUTITLAN
P R E S E N T E

ATN. Q. Ma. del Carmen García Mijares
Jefe del Departamento de Exámenes
Profesionales de la FES Cuautitlán

Con base en el art. 51 del Reglamento de Exámenes Profesionales de la FES-Cuautitlán, nos permitimos comunicar a usted que revisamos el Trabajo de Seminario

Comunicaciones:

Configuración del Switch Cisco Catalyst 1900

que presenta el pasante. José Ignacio Chávez Saladino

con número de cuenta: 079071530 para obtener el título de
Ingeniero Mecánico Electricista

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXAMEN PROFESIONAL correspondiente, otorgamos nuestro VISTO BUENO

ATENTAMENTE
"POR MI RAZA HABLARA EL ESPIRITU"

Cuautitlán Izcalli, Méx. a 06 de Diciembre de 2002

MODULO

PROFESOR

FIRMA

I

Ing. Rodolfo López Gonzáloz

II

Ing. Jorge Ramírez Rodríguez

III

Ing. Maricela Serrano Fragosó

B

INTRODUCCION

Una red de campus se define como una porción o segmento de una red corporativa que utiliza una corporación o institución en su conjunto. Los campus de red normalmente se limitan a un edificio o grupo de edificios, y utilizan fundamentalmente tecnologías LAN, como Ethernet o Token Ring.

El crecimiento de una red de campus supone ampliar el número de estaciones de trabajo y servidores conectados y, a medida que la red va creciendo, el número de estaciones de trabajo y servidores que se agregan aumenta la carga que tiene que soportar la red en términos de ancho de banda disponible. En este caso, suele aplicarse la segmentación como estrategia para dividir la red global en segmentos más pequeños que operen como unidades separadas cuando se comuniquen localmente dentro del segmento. De esta forma, el ancho de banda queda preservado. En aquellos casos en que la red se amplía más allá del entorno geográfico en que se halla ubicada, la ampliación requerirá posiblemente el uso de la tecnología WAN.

Con lo anterior se desprende que a medida que crece la red es necesario resolver cuestiones relacionadas con la ampliación de la red, como conservar el ancho de banda y conectar la red con otras redes.

En este trabajo se realiza un análisis y estudio de las tecnologías que existen para construir y mantener una red del tamaño de un campus. Se analiza el funcionamiento de los distintos dispositivos, como son Repetidores, Switches y Routers; también se describen las tecnologías para la conexión de redes MAN Y WAN y, como ejercicio práctico, se explica la instalación y configuración del Switch Cisco Catalyst 1900, dispositivo que responde a la necesidad de conservar el ancho de banda en una red.

INDICE

| | |
|---|-----|
| Capítulo I. Conceptos generales sobre redes | |
| Definición de redes..... | 1 |
| Componentes básicos de una red..... | 3 |
| Hubs, Repetidores y MAU..... | 4 |
| Cableado de la red..... | 5 |
| Cobertura de las redes..... | 7 |
| Arquitecturas de red..... | 9 |
| Capítulo II. Protocolos de comunicaciones | |
| El proceso de comunicación..... | 14 |
| El modelo de referencia OSI..... | 16 |
| El modelo Internet..... | 27 |
| Ethernet..... | 29 |
| La LAN IEEE..... | 32 |
| Redes IEEE 802.3..... | 37 |
| Redes IEEE 802.5 (Token Ring)..... | 39 |
| Capítulo III. Interconexión de redes | |
| Multiplexión..... | 44 |
| Conmutación de datos..... | 45 |
| Bridges, Routers y switches..... | 48 |
| Servicio digitales..... | 52 |
| Líneas digitales conmutadas..... | 54 |
| X25..... | 55 |
| Frame Relay..... | 57 |
| ATM..... | 59 |
| Capítulo IV. Tecnología de Conmutación (switching) | |
| Dominios de colisión y difusión..... | 65 |
| Tecnología de conmutación..... | 69 |
| Aprendizaje de direcciones..... | 70 |
| Decisiones de retransmisión y filtrado..... | 73 |
| Evitar los bucles..... | 74 |
| Tormentas de difusión..... | 75 |
| Bucles múltiples en una red conmutada..... | 78 |
| Cómo funciona el árbol de extensión..... | 79 |
| Capítulo V. Configuración del Switch Cisco Catalyst 1900 | |
| Interfaces del Switch..... | 90 |
| Inicio de una sesión del Switch tras el arranque..... | 97 |
| Ayuda de teclado en la interfaz de línea de comandos..... | 99 |
| Mensajes de error de consola..... | 100 |
| Comandos para obtener información básica..... | 102 |
| Configuración desde la línea de comandos..... | 107 |
| Ejemplos de configuración de switch..... | 108 |
| Configuración de la dirección IP, Máscara de subred y gateway predeterminado..... | 111 |
| Configuración del modo duplex..... | 113 |
| Direcciones MAC e interfaces..... | 115 |
| Resumen de los comandos de configuración..... | 123 |
| Glosario..... | 124 |
| Conclusiones..... | 137 |
| Referencias..... | 138 |

Capítulo I Conceptos generales sobre redes

En 1981 IBM presentó la computadora personal (PC) y estaba dirigido a las personas que deseaban disponer de su propia computadora, sobre la que se ejecutaban sus propias aplicaciones, y en la que administraban archivos personales en lugar de utilizar las minicomputadoras y grandes sistemas que estaban bajo el estricto control de los departamentos de informática. Los usuarios de las computadoras personales comenzaron pronto a conectar entre sí sus sistemas formando redes, de forma que podían compartir archivos y recursos como las impresoras. Ocurrió entonces que, alrededor de 1985, las redes se hicieron tan grandes y complejas que el control volvió a los departamentos de informática. En la actualidad, las redes no son elementos simples y fáciles de manejar, necesitan un control de seguridad, monitorización y administración. Las redes a menudo se llegan a extender fuera de la oficina local, abarcando el entorno de una ciudad o uno mayor y necesitan entonces expertos que puedan desarrollar las técnicas para tratar los problemas derivados del crecimiento de la red y de las comunicaciones.

Definición de las redes

La más simple de las redes conecta dos computadoras, permitiéndoles compartir archivos e impresoras. Una red mucho más compleja conectaría todas las computadoras de una compañía en el mundo. Para compartir impresoras basta con un switch (conmutador manual o automático), pero si se desean compartir eficientemente archivos y ejecutar aplicaciones de red, hacen falta tarjetas de interfaz de red (NIC, Network Interface Cards) y cables para conectar los sistemas. Aunque se pueden utilizar diversos sistemas de interconexión vía los puertos serie y paralelo, estos sistemas baratos no ofrecen la velocidad e integridad que necesita un sistema operativo de red seguro y con altas prestaciones, que permita manejar muchos usuarios y recursos. Una vez realizadas las conexiones, se ha de instalar el sistema operativo de red (NOS, Network Operating System). Hay dos tipos básicos de sistema operativo de red que nos permiten configurar dos tipos de redes: **punto a punto** y **con servidor dedicado**.

- **Punto a punto.** Este es un tipo de sistema operativo que le permite a los usuarios el compartir los recursos de sus computadoras y acceder a los recursos compartidos de las otras computadoras. Microsoft Windows en sus diferentes versiones y Novell Lite son sistemas operativos punto a punto. Según este esquema, se puede compartir un directorio o una impresora de la computadora propia, de forma que otros usuarios pueden acceder a

ellos, pudiendo hacer éstos lo mismo con sus computadoras. El modo punto a punto implica que todas las computadoras poseen el mismo estatus en la red. Ningún sistema es «esclavo» de otro.

- **Con servidor dedicado.** En un sistema operativo con servidor dedicado, como son Windows NT Server y Novell Server, una o más computadoras se reservan como servidores de archivos, no pudiendo utilizarse para nada más. Los usuarios acceden a los directorios y recursos de los servidores de archivos dedicados, pero no a los de los otros sistemas. De esta forma, se aumenta la seguridad y se evita el reducir el rendimiento de las computadoras personales.

Para entender la importancia de los sistemas operativos de red, es útil el compararlos con los sistemas de procesamiento centralizados, como las minicomputadoras y grandes sistemas (mainframes). En una red, cada computadora accede a los programas y archivos que se encuentran en un servidor central, pero ejecutan estos programas en su propia memoria y con su propio procesador. Una mini o gran computadora tiene centralizado también el procesamiento; gestiona las tareas de procesamiento de los terminales que se encuentran conectados a ella. A menudo, a estos terminales, se les denomina terminales tontos ya que no poseen ni memoria ni procesador propios. Las redes son sistemas de procesamiento distribuido, ya que cada computadora lleva a cabo su propio procesamiento. El servidor de archivos no se encuentra sobrecargado por las tareas de procesamiento de las estaciones de trabajo individuales, y puede optimizar los servicios de archivo y red como el almacenamiento y recuperación de archivos, tareas de gestión, monitorización del acceso de los usuarios, compartición de las impresoras y seguridad.

Nota: A los sistemas de procesamiento distribuido se les llama a veces sistemas cliente-servidor, ya que utilizan la capacidad de computación de un cliente que ve el usuario (front-end) y un servidor por detrás (back-end). El servidor se encuentra en el servidor de archivos y ofrece comúnmente funciones de gestión, de los datos y de multiusuario.

Sin embargo, las mini y grandes computadoras no se han quedado obsoletas con la aparición de las redes. En vez de ello, han pasado a tener un papel distinto dentro de las constantes necesidades informáticas de las empresas. Como se ve en la Figura 1-1, estos grandes sistemas se pueden conectar a una red, pudiendo acceder a ella cualquier usuario que necesite de sus funciones más específicas como si fuera otro periférico. De este modo se puede aumentar la eficiencia en el uso de los recursos de la empresa. La red de la Figura 1-1 es una red de empresa, ya que permite conectar todos los recursos informáticos de la empresa, incluyendo los sistemas Apple Macintosh, los basados de IBM, en UNIX y otras estaciones de trabajo conectados a la misma red. La red es una plataforma de interconexión que admite diversos sistemas.

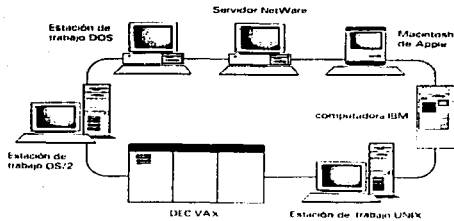


Figura 1-1. Las redes de computadoras se pueden utilizar como plataformas modulares para la interconexión de diversos tipos de sistemas.

Componentes básicos de una red

Una red de computadoras está compuesta tanto por hardware como por software. El hardware incluye tanto las tarjetas de interfaz de red como los cables que las unen, y el software incluye los controladores (programas que se utilizan para gestionar los dispositivos periféricos) y el sistema operativo de red que gestiona la red. A continuación se listan y describen los componentes, tal y como se muestran en la Figura 1-2.

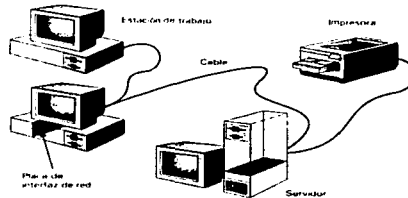


Figura 1-2. Componentes de una red.

- Servidor.
- Estaciones de trabajo.
- Tarjetas de interfaz de red (NIC).
- Sistema de cableado.

- Recursos periféricos y compartidos.

Servidor. El servidor ejecuta el sistema operativo de red y ofrece los servicios de red a las estaciones de trabajo. Entre estos servicios se incluyen el almacenamiento de archivos, la gestión de usuarios, la seguridad, las órdenes y opciones para usuarios de red, las órdenes del responsable de la red y otros.

Estaciones de trabajo. Cuando una computadora se conecta a una red. La primera se convierte en un nodo de la última, y se puede tratar como una estación de trabajo o cliente. Las estaciones de trabajo pueden ser computadoras personales Windows, sistemas Macintosh de Apple o sistemas basados en UNIX.

Tarjetas de interfaz de red (NIC). Toda computadora que se conecte a una red necesita de una tarjeta de interfaz de red que soporte un esquema de red específico, como Ethernet o Token Ring. El cable de la red se conectará a la parte trasera de la tarjeta. También están disponibles redes sin cables por radio o infrarrojos.

Sistema de cableado. El sistema de cableado de la red está constituido por el cable utilizado para conectar entre sí el servidor y las estaciones de trabajo. En el caso de las redes sin cable que utilizan la radio o los infrarrojos no es necesario.

Recursos y periféricos compartidos. Entre los recursos compartidos se incluyen los dispositivos de almacenamiento ligados al servidor, las unidades de disco óptico, las impresoras, los trazadores (plotters) y el resto de equipos que puedan ser utilizados por cualquiera en la red.

Hubs, Repetidores y MAU

En función del tipo de cable empleado y de la topología de la red, se utilizan dispositivos para conectar los nodos o ampliar su número en la red. El tipo de dispositivo de conexión que se utiliza depende, también, del tipo de arquitectura de red que se implementa (Ethernet o Token Ring), conceptos que trataremos posteriormente.

Los *hubs* (concentradores) se utilizan en las instalaciones de par trenzado y sirven como punto central de conexión para la red. Un hub básico no contiene circuitos electrónicos activos, por lo que no puede utilizarse para ampliar la red. Básicamente, se encarga de organizar el cableado de la red y de transmitir las señales a todos los dispositivos de conexión. (Figura 1-3)

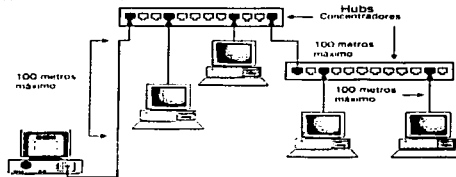


Figura 1-3 Conexión de estaciones de trabajo por medio de hubs

En aquellos casos en que la red tenga que ampliarse más allá de la longitud máxima que permita el tipo de cable utilizado, se utilizan los dispositivos llamados repetidores. Los repetidores toman la señal recibida y la amplifican generándola de nuevo.

Nota: La tecnología de los hubs no deja de evolucionar. Existen ya los llamados hubs activos no sólo sirven como conexión física entre los distintos nodos que componen la red, sino que también hacen la veces de repetidores, permitiendo así ampliar la red según se requiera.

En las redes Token Ring, el dispositivo utilizado como punto central de conexión es una unidad de acceso multiestación, conocida como MAU (Multistation Access Unit). Estas unidades contienen circuitos electrónicos activos por lo que, al tiempo que conectan físicamente los distintos dispositivos que conforman la red, proporcionan el anillo lógico necesario para que se genere el tráfico de la red.

Se explicarán con más detalle el funcionamiento de estos dispositivos de conexión de redes en los próximos apartados.

Cableado de la red

El cable de cobre es el medio de conexión en red más utilizado para las redes de área local. Pero cada vez se recurre con mayor frecuencia al cable de fibra óptica, dado su mayor ancho de banda y recorrido. De hecho, el cable de fibra óptica suele utilizarse en las implementaciones de red de alta velocidad, como FDDI y SONET (Synchronous Optical Network o Red Óptica Sincrónica), capaz de transmitir datos, voz e imágenes por una red de fibra óptica de alta velocidad).

El cable de par trenzado de categoría 5 es el más utilizado hoy en día y permite realizar implementaciones de 10Mbps, 100Mbps (Fast Ethernet) y de 1Gbps (Ethernet de gigabits). Los cables de par trenzado sin blindaje también pueden utilizarse en las redes Token Ring IBM. IBM cuenta con su propio sistema de definición para cables de par Trenzados (tanto blindados como sin blindaje); el Tipo 1 es el cable de par trenzado más utilizado en las instalaciones de redes Token Ring. El cable de par trenzado se utiliza con un conector RJ-45 para conectar tarjetas de red, hubs y otros dispositivos de conexión.

Las instalaciones con cableado coaxial (RG-58) eran el medio de conexión por el que se conectaban todas las empresas hace algunos años, dada su facilidad de instalación y bajo costo. Las redes LAN conectadas con este tipo de cable utilizan una topología de bus donde la tarjeta de red de cada computadora va conectada a un conector en forma de T. Las computadoras están a su vez conectadas entre sí por medio de cables con la longitud adecuada. Estas instalaciones requieren que cada nodo final de la red esté terminado sin posibilidad de conexión, por lo que se colocan terminadores en la salida del conector T de aquellas computadoras que residen en cualquiera de los nodos finales de la red.

Aunque el cable de cobre es un medio de conexión para red barato y de instalación sencilla, presenta una serie de limitaciones inherentes al mismo. En primer lugar, está expuesto a interferencias electromagnéticas. La atenuación (el hecho de que la señal se debilite debido a la extensión misma del cable) también limita la longitud del cable de cobre que puede utilizarse. El cable de cobre puede además derivarse, lo cual puede afectar a la seguridad de la información que viaja a través de la red.

El cable de fibra óptica es una alternativa con mayor velocidad de transmisión al cable de cobre, y a menudo se emplea como cable principal en las grandes redes corporativas. El cable de fibra óptica utiliza filamentos de vidrio y plástico para conducir los datos, y ofrece mayor ancho de banda y recorrido, además de no permitir la derivación. Con la creciente necesidad de mayores velocidades de transmisión, las instalaciones de fibra óptica se están multiplicando a pasos agigantados.

Nota: Al seleccionar el cable de la red, deben tenerse en cuenta una serie de factores importantes, como el costo del mismo, su ancho de banda (es decir, la cantidad de información que puede transmitirse por la red), su grado de exposición a interferencias electromagnéticas, la atenuación, que condiciona la longitud máxima de cable que puede utilizarse en la red, así como la complejidad de su instalación.

La Tabla 1.1 ofrece un breve resumen de los distintos tipos de cables disponibles. Por su parte, la Figura 1-4 presenta una imagen de cada uno de los tipos de cables incluidos en la tabla.

| Tipo de cable | Ancho de banda | Longitud máxima |
|--------------------------------------|------------------------|-----------------|
| Par trenzado de categoría 5 | entre 10Mbps y 100Mbps | 100 metros |
| Coaxial Ethernet RG-58 delgado | 10Mbps | 185 metros |
| Coaxial Ethernet RG-58 grueso grueso | 10Mbps | 500 metros |
| Fibra óptica | entre 100Mbps y 2Gbps | 2 kilómetros |

Tabla 1-1 Comparación de cables de red



Figura 1-4 Tipos de cables

Cobertura de las redes

Existen redes de todos los tamaños. La red puede comenzar como algo pequeño y crecer con la organización. En la Figura 1-5 se muestra el ámbito de cobertura de las redes.

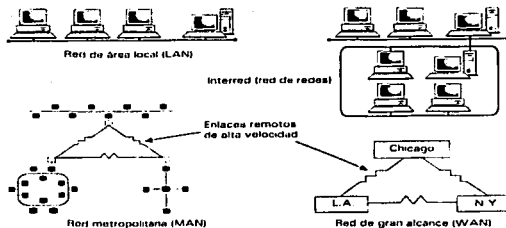


Figura 1-5. Cobertura de las redes

RED DE ÁREA LOCAL (LAN). Red pequeña (de 3 a 50 nodos), localizada normalmente en un solo edificio o grupo de edificios pertenecientes a una organización.

REDES INTERCONECTADAS (Interredes). Una red de redes (redes interconectadas), se encuentra formada por dos o más segmentos de red local conectados entre sí para formar un sistema que puede llegar a cubrir una empresa. Esto es normal en las empresas u organizaciones departamentalizadas, disponiendo cada departamento de su propia red local, estando estas redes interconectadas entre sí. A menudo, como veremos posteriormente, las redes más grandes se encuentran divididas en varios segmentos más pequeños para optimizar el rendimiento y su gestión, utilizando dispositivos como *switches* (conmutadores). Para enlazar dos o más redes iguales o distintas se utilizan los *routers* (ruteadores).

RED A NIVEL DE EMPRESA. Una red a nivel de empresa es similar a una interred, excepto en que la red a nivel de empresa interconecta todos los sistemas informáticos de la organización, independientemente de los sistemas operativos que utilicen. En una red a nivel empresarial se pueden encontrar conectados mini o grandes computadoras, estaciones de trabajo UNIX, computadoras Apple, estaciones basadas en IBM, servidores basados en NT de Microsoft, servidores basados en Novell NetWare y cualquier otro elemento informático, en un único sistema interconectado.

METROPOLITANA (MAN) Y RED DE GRAN ALCANCE (WAN). Estas ofrecen la conexión de redes y recursos distantes. Las redes metropolitanas son normalmente redes de fibra óptica de gran velocidad que conectan segmentos de red local de un área específica, como un complejo industrial o una ciudad. Estas redes utilizan unas líneas básicas de alta velocidad (normalmente de fibra) que conectan directamente los servidores. Otra alternativa es la conexión con microondas

dentro de la ciudad. Las parábolas para microondas se montan en lo alto de los edificios apuntando de uno a otro para establecer la conexión entre las redes. La red metropolitana consta normalmente de un cableado y unos sistemas de comunicaciones que son instalados y propiedad del dueño de la red.

Las redes de gran alcance permiten la interconexión nacional o mundial mediante líneas telefónicas y satélites. Las grandes empresas que poseen oficinas en grandes territorios por todo el mundo pueden interconectar sus redes de área local dentro de una red de gran alcance. Los operadores de larga distancia (compañías telefónicas) alquilan líneas dedicadas para poder establecer la interconexión en forma dedicada y completa entre diversos sistemas.

Arquitecturas de red

La arquitectura de una red viene definida por su *topología*, el *método de acceso* a la red y los *protocolos de comunicación*. Antes de que cualquier estación de trabajo pueda utilizar el sistema de cableado, debe definir una sesión de comunicación con cualquier otro nodo de la red. Los métodos de acceso a la red describen como puede acceder al cable la estación de trabajo sin hacerlo cuando otra estación de trabajo lo está utilizando. Los protocolos son las reglas que controlan la forma en que se transfieren paquetes de información de una estación de trabajo a otra.

Topología

Se puede representar la topología de la red como un mapa del cableado. La topología define cómo se llevará el cable a cada estación de trabajo concreta, y tiene un papel muy importante en las decisiones a tomar sobre el cableado. Como se puede ver en la Figura 1-4, una red puede tener una topología lineal, en anillo o en estrella. Al pensar la topología de una red se ha de pensar cuál es el mejor método para realizar el cableado en el edificio.

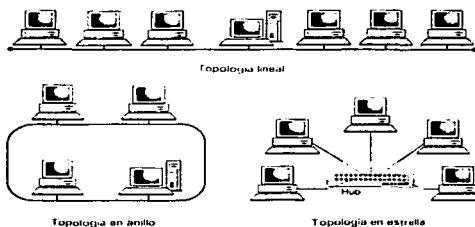


Figura 1.4 Topologías de red

Topología de bus lineal

Una red lineal o de bus se caracteriza por un segmento principal o línea central al que están conectadas las distintas computadoras a intervalos determinados. Las redes de bus conforman lo que se conoce como una topología pasiva. Las computadoras conectadas en bus actúan de forma "expectante", es decir, que antes de transmitir datos, comprueban que ninguna de las restantes computadoras del bus está transmitiendo información, pasando a enviar los paquetes cuando la conexión queda libre. Por lo general, las redes pasivas basadas en la contención (así denominadas porque cada computadora tiene que competir por el tiempo de transmisión) utilizan la arquitectura de red Ethernet.

Las redes lineales utilizan normalmente cables coaxiales que se conectan a cada una de las computadoras por medio de conectores en forma de T. En cada nodo final de la red se coloca un terminador específico para el tipo de cable utilizado (si se utiliza un cable de 50 Ohm, deben emplearse terminadores de 50 Ohm). Puesto que la red de bus no es más que un conjunto de cables, conectores y terminadores, la señal no se amplifica al viajar por el cableado.

Las redes de bus son fáciles de instalar y ampliar. Tan sólo requieren una pequeña cantidad de cable, comparadas con otras topologías de red. Pero estas redes pueden sufrir roturas de cables, y deficiencias en la longitud necesaria del cableado, a menudo de difícil resolución. De hecho, cualquier problema físico en la red, como un conector suelto, puede inutilizar el funcionamiento de toda la red.

Topología de estrella

En una topología en forma de estrella, las computadoras de la red están conectadas a un dispositivo central denominado hub. Cada computadora está conectada con su propio cable (normalmente, un cable de par trenzado) a un puerto del hub. Aunque la topología de estrella utiliza un hub (existen hubs especiales, como los repetidores multipuerto, capaces de mejorar las señales de los paquetes antes de transmitirlos por la red), este tipo de red también se sirve de un método pasivo de contención para transmitir la información por la red. Las computadoras comprueban antes que nada si el medio compartido está siendo utilizado y se disputan el tiempo de transmisión disponible.

Puesto que en la topología de estrella cada computadora de la red utiliza una conexión distinta de cables, este tipo de topología es ampliable, característica únicamente limitada por el número de puertos disponibles en el hub (es posible unir varios hubs para aumentar el número de puertos). La ampliación de una red de topología de estrella no presenta ninguna dificultad, puesto que añadir otra computadora a la red no supone más que colocar un cable entre la computadora y el hub.

La principal desventaja de la topología de estrella tiene que ver con el hub central. Si el hub falla, la red deja de funcionar.

Topología de anillo

En una topología de anillo, las computadoras se conectan al cable una detrás de otra formando un círculo físico. La topología de anillo (por ejemplo, Token Ring o la Fiber Distributed Data Interface, FDDI (Intertaz de Datos Distribuidos por Fibra Óptica) transfiere la información por el cable en una sola dirección y se considera una topología activa. De hecho, las computadoras conectadas a la red retransmiten los paquetes recibidos y los envían a la siguiente computadora incluida en el anillo.

El acceso al canal de comunicación de la red se otorga por medio de una señal especial o token. El token viaja por el anillo y, cuando una computadora desea enviar datos, tiene que esperar a que llegue el token para hacerse con él. La computadora pasa entonces a enviar los datos por el cable. Cuando la computadora que envió los datos recibe la comprobación de que el paquete llegó a la computadora de destino, la computadora remitente crea un nuevo token y lo transfiere a la siguiente computadora del anillo, volviendo a iniciarse así la pasada de token o señales.

El hecho de que una computadora deba estar en posesión del token para enviar datos por la red significa que todas las computadoras cuentan con el mismo nivel de acceso al canal de comunicación. La pasada del token entre computadoras ofrece una transmisión más sincronizada de los datos (debido al campo de nivel de ejecución que proporciona la estrategia de pasada del token) comparada con las redes basadas en la contención, como son las topologías de bus o estrella. Cuando el tráfico se satura en la red, la degradación de las redes en anillo (en términos de rendimiento) es menor a las topologías pasivas, que pueden interrumpirse rápidamente en situaciones de sobrecarga del sistema debido a su mayor exposición a las colisiones de datos.

Las auténticas topologías de anillo son de resolución compleja, y el fallo de una computadora del anillo puede interrumpir el flujo de datos, ya que los datos viajan por el anillo en una sola dirección. Igualmente, añadir o quitar computadoras en este tipo de topología puede ocasionar una interrupción en el funcionamiento de la red.

Topología en malla

Existe otra topología en malla que utiliza conexiones redundantes entre las computadoras de la red aplicando una estrategia de tolerancia a los fallos. Cada dispositivo incluido en la red está conectado al resto de dispositivos, lo que explica que este tipo de topología requiera de un gran cableado. Este tipo de topología puede hacer frente al fallo de uno o dos segmentos de la red sin interrumpir el tráfico, ya que dispone de líneas redundantes.

Las redes en malla, obviamente, resultan más costosas y difíciles de instalar que otro tipo de topologías de red. Debido al gran número de conexiones que requieren. En la mayoría de los casos, las redes que utilizan esta estrategia de conexión redundante están incluidas dentro de redes híbridas más amplias. En una red híbrida tan sólo los servidores y computadoras más importantes y cruciales están configurados con conexiones redundantes. De esta forma, los segmentos fundamentales de la red corporativa quedan protegidos sin necesidad de utilizar múltiples líneas para cada una de las computadoras conectadas a la red.

Método de acceso al cable

El método de acceso al cable describe cómo accede un nodo al sistema de cableado. Una vez que la tarjeta de red consigue el acceso al cableado comienza a enviar paquetes de información, llamados bloques (frames) o células (cells), al tratar los métodos de comunicación telefónica, a otros nodos. Todas las estaciones de trabajo de una red de área local (LAN) deben de utilizar el mismo método de acceso a la red.

Los sistemas de cableado lineales, como Ethernet, utilizan un método de detección de portadora, con el cual la estación comprueba el cable para ver si esta siendo utilizado antes de transmitir. En este caso, la transmisión es como la difusión de la radio por el cable: todos los nodos la reciben, siendo éstos los que determinan si la información va dirigida a ellos o no. Si no lo fuera el nodo devuelve la información recibida. Si dos nodos emiten al mismo tiempo se produce una colisión, debiendo volver a reenviarla ambos después de esperar un tiempo fijado de forma aleatoria para cada uno. En este tipo de redes, el rendimiento se reduce cuando el tráfico es pesado, debido a estas colisiones y las retransmisiones necesarias.

Las redes en anillo, como Token Ring, normalmente utilizan un método de paso de testigo (token). Con este sistema, una estación de trabajo sólo transmite cuando pasa el testigo. Se puede pensar en este testigo como en una especie de resguardo o pase que permite usar la red. Cuando una estación está preparada para transmitir ha de esperar a que esté libre el testigo y apoderarse de él. De esta forma, se evita que dos máquinas puedan utilizar simultáneamente el cable.

Protocolos de comunicaciones

Los protocolos de comunicaciones son las reglas y procedimientos utilizados en una red para establecer la comunicación entre los nodos que disponen de acceso a la red. Los protocolos gestionan dos niveles de comunicación distintos. Las reglas de alto nivel definen cómo se comunican las aplicaciones, mientras que las de bajo nivel definen cómo se transmiten las señales por el cable.

Nota: Las redes, por ejemplo Ethernet, Token Ring y FDDI son una combinación de hardware y software que poseen una topología, método de acceso y criterios de diseño específicos. Generalmente al referirse a ellas puede dar lugar a confusión. Por ejemplo, se podría decir «red Ethernet» o «topología Ethernet», e incluso «estándar Ethernet», pero por simplicidad es normal el decir simplemente «Ethernet».

Capítulo II Protocolos de comunicaciones

Una de las mejores formas para entender el funcionamiento de las redes es, en primer lugar, comprender la forma en que el tráfico circula a través de la red. Sería, también, sumamente difícil hablar de instalación y configuración de dispositivos o de interconexión de redes si no se habla de las reglas de comunicación usadas para conseguir un *dialogo* entre los dispositivos y equipos interconectados. Esto se consigue por medio del modelo de referencia OSI que a continuación se explica.

El proceso de comunicación

La comunicación de datos es sorprendentemente similar a la conversación humana. Tanto las personas como las computadoras utilizan una comunicación formal para realizar intercambios complejos de información y procesos informales para objetivos específicos. Ambos respetan unos protocolos, reglas que posibilitan que los sujetos intercambien información de manera ordenada y libre de errores. Los protocolos se siguen para establecer y finalizar la comunicación de modo que ninguna parte quede bloqueada en un estado no deseable. Del mismo modo que una interrupción ruda puede ofender a una persona, la interrupción de la comunicación de datos sin un procedimiento ordenado puede confundir a una computadora. Por tanto, la primera característica de un proceso de comunicación es que resulta imprescindible utilizar protocolos de comunicaciones para lograr una comunicación sin errores. La imposibilidad de que dos entidades se comuniquen de manera directa complica la comunicación. Considere lo que sucede cuando una persona envía una carta por correo a otra:

1. El remitente escribe la carta en un papel.
2. El remitente introduce la carta en un sobre y escribe en él su remite y la dirección del destinatario.
3. El remitente introduce el sobre en un buzón donde un cartero lo recogerá para situarlo en un saco de transporte.
4. El cartero transporta el saco a una oficina de correos en la que otra persona retira la carta y la sitúa en otro saco que se transportará a la ciudad del destinatario.
5. El servicio de correos transporta el saco que contiene la carta a la ciudad de destino.
6. Tras la llegada del saco a la ciudad del destinatario, una persona clasifica las cartas para entregárselas a los carteros encargados de las distintas zonas de la ciudad.
7. El cartero transporta la carta hasta la dirección del destinatario.
8. Finalmente, el destinatario abre el sobre y recupera el mensaje original del remitente.

9. Este proceso ilustra muchas características importantes de la comunicación. El diagrama de la Figura 2-1 se asemeja profundamente a los modelos de arquitectura que se examinan posteriormente en este capítulo.

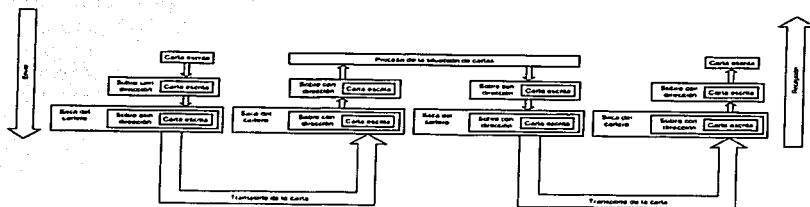


Figura 2-1 Modelo de comunicación por carta.

Una de las características del modelo de la Figura 2-1 consiste en que la comunicación se desarrolla en capas. Cada una de ellas cuenta con su propia área de responsabilidad definida específicamente. Cuando desea que alguien reciba una carta, sólo tiene que preocuparse de introducirla en un sobre con la dirección escrita. No necesita preocuparse por las otras capas del proceso. Le es indiferente si la carta se transporta en tren o en avión, esa responsabilidad es de otra capa.

Este enfoque para diseñar un sistema de comunicaciones se denomina *arquitectura de capas*. Cada capa se responsabiliza de determinadas tareas y utiliza sus propias reglas para llevarlas a cabo sin conocer los procedimientos seguidos por otras capas. La capa se limita a desarrollar sus tareas y a entregar el mensaje a la siguiente capa del proceso. Es posible deducir varias características de las arquitecturas de capas utilizando el ejemplo anterior:

- Las capas dividen el proceso de comunicación en partes fácilmente manejables. El diseño de una pequeña parte de un proceso resulta más sencillo que el diseño de todo el proceso y la ingeniería se ve simplificada. Un usuario del servicio de correos debe realizar los procedimientos locales sin preocuparse del mecanismo completo que permite entregar la carta en su destino remoto.
- El cambio de una capa no afecta a las capas restantes. El proceso de dirigir un sobre a un destinatario no cambia aunque la carta se envíe en tren, avión o paloma mensajera. Es posible introducir nuevas tecnologías en el proceso de entrega sin afectar a las capas restantes. Esta es la razón principal para implementar los protocolos en capas.

- Cuando una capa recibe un mensaje de la capa superior, la capa inferior guarda el mensaje en un paquete distinto. Por ejemplo, las cartas se introducen en sacos de correos durante su transporte. En términos de comunicación de datos, los protocolos de las capas inferiores suelen tratar los mensajes de las capas superiores de manera similar, introduciéndolos en un "sobre de datos". El término técnico de este proceso es *encapsulación*.
- Los protocolos de las distintas capas tienen un aspecto apilado y la totalidad del modelo de una arquitectura de comunicación suele denominarse *pila de protocolos*. Es posible mezclar y ensamblar capas para lograr distintos objetivos. Si añade el sello URGENTE al sobre, la carta se enviará utilizando el servicio de transporte nocturno para acelerar su entrega.
- Cada capa sigue unos procedimientos preestablecidos para comunicarse con las capas adyacentes. Las interfaces entre capas deben definirse con claridad.
- Un mecanismo de dirección es el elemento común que permite dirigir las cartas a través de las distintas capas hasta que alcanzan su destino. En ocasiones, las capas añaden su propia información a la dirección.. Las direcciones postales constan de dos partes: una ciudad y un código postal que permiten entregar el mensaje a la oficina postal correcta, y una calle y un número que posibilita que el cartero deposite la carta en el buzón correcto.
- Básicamente, cada capa del lado del remitente se comunica con la capa correspondiente del lado del destinatario. Por ejemplo, el proceso de introducir la carta en un sobre cuenta con un proceso correspondiente en la ciudad de destino: abrir el sobre y extraer la carta. El remitente y el destinatario son los únicos en examinar el contenido de la carta, éste carece de importancia para el resto de las capas.
- Pueden producirse errores en cualquiera de las capas. En el caso de mensajes críticos, deben establecerse mecanismos que detecten los errores y que los corrijan o informen al remitente.

Cada una de estas características tiene su contrapartida en la comunicación de datos. Ha llegado el momento de examinar algunos modelos de comunicación reales, comenzando por el modelo de referencia OSI, que es lo bastante genérico como para ilustrar las características generales de los modelos de comunicación de datos.

El modelo de referencia OSI

La Organización Internacional de Normalización (ISO) desarrolló el modelo de referencia OSI a modo de guía para definir un conjunto de protocolos abiertos. Este modelo de referencia es la norma más común para describir y comparar conjuntos de protocolos.

La Figura 2-2 muestra el modelo de referencia OSI de siete capas. Cada capa ofrece un tipo específico de servicio de red..

| |
|-----------------|
| Aplicación |
| Presentación |
| Sesión |
| Transporte |
| Red |
| Enlace de datos |
| Física |

TESIS CON
FALLA DE ORIGEN

Figura 2-2 Las capas del modelo de referencia OSI.

La Figura 2-2 explica por qué los protocolos relacionados se suelen denominar *pilas de protocolos*. Las capas facilitan los cambios físicos en una red, por ejemplo de Ethernet a Token Ring, sin necesidad de cambiar otras capas.

Las capas de protocolos se numeran desde la base hasta la cima. Las siguientes secciones describen cada capa siguiendo un orden ascendente.

La capa física

La capa física comunica directamente con el medio de comunicación y tiene dos responsabilidades: enviar bits y recibir bits.. Otras capas se responsabilizan del agrupamiento de los bits de forma que representen datos de un mensaje.

Los bits se representan por cambios en las señales del medio de la red. Algunos cableados representan los unos y los ceros con distintos voltajes, otros utilizan tonos de audio distintos y otros utilizan métodos más sofisticados, por ejemplo transiciones de estado (cambios de alto a bajo voltaje y viceversa).

Se utilizan una gran variedad de medios en la comunicación de datos; entre otros, cables eléctricos, fibras ópticas, ondas de luz o de radio y microondas. El medio empleado puede variar, para sustituirlo, basta con utilizar un conjunto distinto de protocolos de capa física. Las capas superiores son totalmente independientes del proceso utilizado para transmitir los bits a través del medio de la red.

Una distinción importante es que la capa física OSI no describe los medios, estrictamente hablando. Las especificaciones de la capa física describen el modo en que los datos se codifican en señales del medio y las características de la interfaz de conexión con el medio, pero no describen el medio en sí. Sin embargo, en la práctica, la mayoría de las normas de las capas físicas incluyen las características de la capa física OSI y del medio.

La capa de enlace de datos

Los dispositivos que pueden comunicarse a través de una red suelen denominarse nodos (se denominan también estaciones y puestos). La capa de enlace de datos es responsable de proporcionar la comunicación nodo a nodo en una misma red de área local. Para ello, la capa de enlace de datos debe realizar dos funciones. Debe proporcionar, un mecanismo de direcciones que permita entregar los mensajes en los nodos correctos y debe traducir los mensajes de las capas superiores en bits que puedan ser transmitidos por la capa física.

Cuando la capa de enlace de datos recibe un mensaje, le da formato para transformarlo en un marco de datos (Frame en Ingles. En las diferentes traducciones al español se denomina igualmente trama). La Figura 2-3 ilustra el formato clásico de un marco de datos. Otro apartado de este capítulo, **protocolos de las capas de acceso a la red**, presenta los formatos de marco de datos de los protocolos Ethernet y Token Ring. Las secciones de un marco de datos se denominan campos. Los campos del ejemplo son los siguientes:

- **Indicador de inicio.** Un patrón de bits que indica el inicio de un marco de datos.
- **Dirección de origen.** La dirección del nodo que realiza el envío se incluye para poder dirigir las respuestas al mensaje.
- **Dirección de destino.** Cada nodo queda identificado por una dirección. La capa de enlace de datos del remitente añade la dirección de destino al marco. La capa de enlace de datos del destinatario examina la dirección de destino para identificar los mensajes que debe recibir.
- **Control.** En muchos casos es necesario incluir información adicional de control. Cada protocolo determina la información específica.
- **Datos.** Este campo contiene todos los datos enviados a la capa de enlace de datos por las capas superiores del protocolo.
- **Control de errores.** Este campo contiene información que permite que el nodo destinatario determine si se ha producido algún error durante la transmisión. El sistema habitual es la *verificación de redundancia cíclica (CRC)*, que consiste en un valor calculado que resume todos los datos del marco. El nodo destinatario calcula nuevamente el valor y, si coincide con el del marco, entiende que el marco se ha transmitido sin errores.

| | | | | | |
|---------------------|---------------------|----------------------|---------|-------|--------------------|
| Indicador de inicio | Dirección de origen | Dirección de destino | Control | Datos | Control de errores |
|---------------------|---------------------|----------------------|---------|-------|--------------------|

Figura 2-3 Ejemplo de un marco de datos.

La entrega de marcos resulta muy sencilla en una red de área local. Un nodo remitente se limita a transmitir el marco. Cada nodo de la red ve el marco y examina su dirección de destino. Cuando coincide con su dirección, la capa de enlace de datos del nodo recibe el marco y lo envía a la siguiente capa de la pila.

La capa de red

Las redes más pequeñas consisten en una sola red de área local pero, como ya lo mencionamos anteriormente, la mayoría de las redes deben subdividirse (véase la Figura 2-4). Una red que consta de varios segmentos de red suele denominarse interred (no confundir con Internet).

Cuando las redes se subdividen, no es posible dar por sentado que los mensajes se entregan en la red de área local. Es necesario recurrir a un mecanismo que dirija los mensajes de una red a otra.

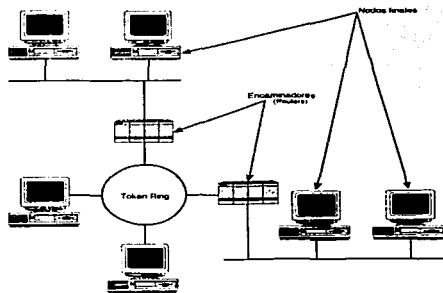


Figura 2-4 Una interred que consta de varias redes.

Para entregar mensajes en una interred, cada red debe estar identificada de manera única por una *dirección de red*. Al recibir un mensaje de las capas superiores, la capa de red añade una cabecera al mensaje que incluye las direcciones de red de origen y destino. Esta combinación de datos sumada a la capa de red se denomina *paquete*. La información de la dirección de red se utiliza para entregar el mensaje a la red correcta. A continuación, la capa de enlace de datos puede utilizar la dirección del nodo para realizar la entrega del mensaje.

El proceso de hacer llegar los paquetes a la red correcta se denomina *encaminamiento* (routing), y los dispositivos que encaminan los paquetes se denominan *routers*.

Según muestra la Figura 2-4, una interred tiene dos tipos de nodos:

- Los nodos finales proporcionan servicios a los usuarios. Utilizan la capa de red para añadir las direcciones de red a los paquetes, pero no llevan a cabo el encaminamiento. En ocasiones, los nodos finales se denominan *sistemas finales* (terminología OSI) o *hosts* (terminología TCP/IP).
- Los routers incorporan mecanismos especiales para realizar el encaminamiento. Dado que se trata de una tarea compleja, los routers suelen ser dispositivos dedicados que no proporcionan servicios a los usuarios finales. En ocasiones los routers se denominan *sistemas intermedios* (terminología OSI) o *gateways* en (terminología TCP/IP).

La capa de red opera con independencia del medio físico, que es competencia de la capa física. Dado que los routers son dispositivos de la capa de red, pueden utilizarse para intercambiar paquetes entre distintas redes físicas. Por ejemplo, un router puede enlazar una red Ethernet a una red Token Ring. Los routers también se utilizan frecuentemente para conectar una red de área local, por ejemplo Ethernet, a un red de área extensa, por ejemplo ATM.

La capa de transporte

Todas las tecnologías de red establecen un tamaño máximo para los marcos que pueden ser enviados a través de la red. Por ejemplo, Ethernet limita el tamaño del campo de datos a 1,500 bytes. Este límite es necesario por varias razones:

- Los marcos de tamaño reducido mejoran el rendimiento de una red compartida por muchos dispositivos. Si el tamaño de los marcos fuera ilimitado, su transmisión podría monopolizar la red durante un tiempo excesivo. Los marcos pequeños permiten que los dispositivos se turnen a intervalos cortos de tiempo y tengan más opciones de acceder a la red.

- Al utilizar marcos pequeños, es necesario volver a transmitir menos datos cuando se produce un error. Si un mensaje de 100 KB contiene un error en un solo byte, es preciso volver a transmitir los 100 KB. Si el mensaje se divide en 100 marcos de 1 KB, basta con retransmitir un solo marco de 1 KB para corregir el error.

Una de las responsabilidades de la capa de transporte consiste en dividir los mensajes en fragmentos que coincidan con el límite del tamaño de la red. En el lado receptor, la capa de transporte reensambla los fragmentos para recuperar el mensaje original.

Cuando un mensaje se divide en varios fragmentos, aumenta la posibilidad de que los segmentos no se reciban en el orden correcto. La Figura 2-5 ilustra el modo en que la red puede encaminar los paquetes en distinto orden a medida que los routers intentan enviar cada paquete siguiendo la ruta disponible más eficiente. Al recibir los paquetes, la capa de transporte debe recomponer el mensaje reensamblando los fragmentos en el orden correcto. Para ello, la capa de transporte incluye un número de secuencia en la cabecera del mensaje.

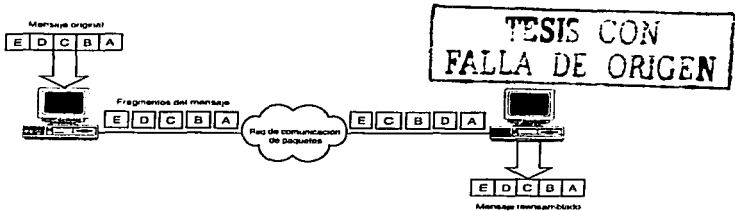


Figura 2-5 Fragmentación y reensamblaje de un mensaje en una red de conmutación de paquetes

Muchas computadoras son multitarea y ejecutan varios programas simultáneamente. Por ejemplo, la estación de trabajo de un usuario puede estar ejecutando al mismo tiempo un proceso para transferir archivos a otra computadora, recuperando el correo electrónico y accediendo a una base de datos de la red. La capa de transporte debe entregar los mensajes del proceso de una computadora al proceso correspondiente de la computadora de destino.

Según el modelo OSI, la capa de transporte asigna una identificación de *punto de acceso a servicio* (SAP) a cada paquete (puerto es el término TCP/IP correspondiente a un punto de acceso a servicio). La ID de un SAP es una dirección que identifica el proceso que ha originado el mensaje. La ID permite que la capa de transporte del nodo receptor encamine el mensaje al proceso adecuado. La identificación de mensajes de distintos procesos para posibilitar su

transmisión a través de un mismo medio de red se denomina *multiplexión*. El procedimiento de recuperación de mensajes y de su encaminamiento a los procesos adecuados se denomina *demultiplexión*. La Figura 2-6 ilustra la multiplexión y demultiplexión de mensajes. Esta práctica es habitual en las redes diseñadas para permitir que varios diálogos compartan un mismo medio de red.

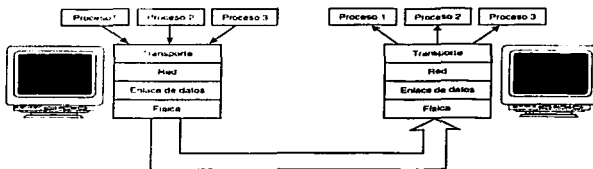


Figura 2-6 Multiplexión y demultiplexión de mensajes.

Nota: Dado que una capa puede admitir distintos protocolos, la multiplexión y demultiplexión puede producirse en distintas capas. La siguiente lista expone algunos ejemplos:

- Transporte de distintos tipos de marcos Ethernet a través del mismo medio (capa de enlace de datos).
- Soporte simultáneo de NWLink y de TCP/IP en computadoras Windows NT (capa de enlace de datos).
- Mensajes de varios protocolos de transporte como TCP y UDP en un sistema TCP/IP (capa de transporte).
- Mensajes de distintos protocolos de aplicación (como Telnet, FTP y SMTP) en un host
- UNIX(capas de sesión y superiores).

Es preciso examinar otra de las competencias de la capa de transporte. Aunque las capas de enlace de datos y de red pueden encargarse de detectar errores en los datos transmitidos, esta responsabilidad suele recaer sobre la capa de transporte. La capa de transporte puede realizar dos tipos de detección de errores:

- **Entrega fiable.** Entrega fiable no significa que los errores no puedan ocurrir, sino que los errores se detectan cuando ocurren. La recuperación puede consistir únicamente en

notificar el error a los procesos de las capas superiores. Sin embargo, la capa de transporte suele solicitar que el paquete erróneo se transmita nuevamente.

- **Entrega no fiable.** No significa que los errores puedan producirse, sino que la capa de transporte no los verifica. Dado que la comprobación requiere cierto tiempo y reduce el rendimiento de la red, es frecuente que se utilice la entrega no fiable cuando se confía en el funcionamiento de la red. Este es el caso de la mayoría de redes de área local. La entrega no fiable es preferible cuando los mensajes constan de un alto número de paquetes. Con frecuencia, se denomina entrega de datagramas y cada paquete transmitido de este modo se denomina *datagrama*.

La idea de que siempre es preferible utilizar la entrega fiable constituye un error común. La entrega no fiable es aconsejable en al menos dos situaciones: cuando la red es altamente fiable y es necesario optimizar su rendimiento o cuando los paquetes contienen mensajes completos y la pérdida de un paquete no plantea un problema crítico.

La capa de sesión

El control de los diálogos entre distintos nodos es competencia de la capa de sesión. Un diálogo es una conversación formal en la que dos nodos acuerdan un intercambio de datos.

La comunicación puede producirse en tres modos de diálogo (véase la Figura 2-7):

- Simple (Simplex). Un nodo transmite de manera exclusiva mientras otro recibe de manera exclusiva.
- Semidúplex (Half-duplex). Un solo nodo puede transmitir en un momento dado, y los nodos se turnan para transmitir.
- Dúplex total (Full-duplex). Los nodos pueden transmitir y recibir simultáneamente. La comunicación dúplex total suele requerir un control de flujo que asegure que ninguno de los dispositivos envía datos a mayor velocidad de la que el otro dispositivo puede recibir.

Las sesiones permiten que los nodos se comuniquen de manera organizada. Cada sesión tiene tres fases:

1. Establecimiento de la conexión. Los nodos establecen contacto. Negocian las reglas de la comunicación incluyendo los protocolos utilizados y los parámetros de comunicación.
2. Transferencia de datos. Los nodos inician un diálogo para intercambiar datos.

3. Liberación de la conexión. Cuando los nodos no necesitan seguir comunicados, inician la liberación ordenada de la sesión.

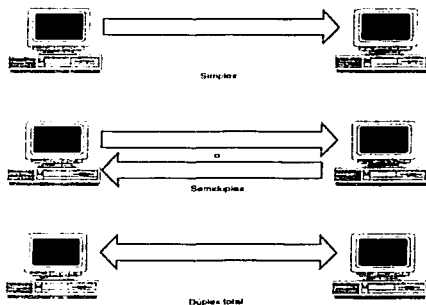


Figura 2-7 Modos de diálogo

Los pasos 1 y 3 representan una carga de trabajo adicional para el proceso de comunicación. Esta carga puede no ser deseable para comunicaciones breves. Por ejemplo, considere la comunicación necesaria para una tarea administrativa de la red. Cuando una red administra varios dispositivos, éstos envían periódicamente un breve informe de estado que suele constar de un solo marco. Si todos estos mensajes se enviaran como parte de una sesión formal, las fases de establecimiento y liberación de la conexión transmitirían más datos que los del propio mensaje.

En estas situaciones, se comunica *sin conexión*. El nodo emisor se limita a transmitir los datos dando por sentado que el receptor está disponible.

Una sesión *con conexión* es aconsejable cuando la comunicación es compleja. Imagine la transmisión de una gran cantidad de datos de un nodo a otro. Si no se utilizaran controles formales, un solo error durante la transferencia obligaría a enviar de nuevo todo el archivo. Una vez establecida la sesión, los nodos implicados pueden pactar un procedimiento de comprobación. Si se produce un error, el nodo emisor sólo debe retransmitir los datos enviados desde la última comprobación. El proceso de gestión de actividades complejas se denomina *administración de actividad*.

La capa de presentación

La capa de presentación se responsabiliza de presentar los datos a la capa de aplicación. En ciertos casos, la capa de presentación traduce los datos directamente de un formato a otro. Las grandes computadoras IBM utilizan una codificación de caracteres denominada EBCDIC, mientras que las computadoras restantes utilizan el conjunto de caracteres ASCII. Por ejemplo, si se transmiten datos de una computadora EBCDIC a otra ASCII, la capa de presentación podría encargarse de traducir de un conjunto de caracteres al otro. Además, la representación de los datos numéricos varía entre distintas arquitecturas de computadoras y debe convertirse cuando se transfieren datos de una máquina a otra.

Otras funciones que pueden corresponder a la capa de presentación son la encriptación/desencriptación y compresión/descompresión de datos.

La capa de presentación es la que se implementa con menor frecuencia de las capas OSI. Se han definido pocos protocolos para esta capa. En la mayoría de los casos, las aplicaciones de red desempeñan las funciones asociadas con la capa de presentación.

La capa de aplicación

La capa de aplicación proporciona los servicios utilizados por las aplicaciones para que los usuarios se comuniquen a través de la red. La siguiente lista enumera varios ejemplos de servicios:

- **Transporte de correo electrónico.** Gran variedad de aplicaciones pueden utilizar un protocolo para gestionar el correo electrónico. Los diseñadores de aplicaciones que recurren al correo electrónico no necesitan desarrollar sus propios programas para gestionar el correo. Además, las aplicaciones que comparten una misma interfaz de correo pueden intercambiar mensajes utilizando el gestor de correo electrónico.
- **Acceso a archivos remotos.** Las aplicaciones locales pueden acceder a los archivos ubicados en los nodos remotos.
- **Ejecución de tareas remotas.** Las aplicaciones locales pueden iniciar y controlar procesos en otros nodos.
- **Directorios.** La red puede ofrecer un directorio de recursos, incluyendo nombres de nodos lógicos. El directorio permite que las aplicaciones accedan a los recursos de la red utilizando nombres lógicos en lugar de identificaciones numéricas abstractas.
- **Administración de la red.** Los protocolos de administración de la red permiten que varias aplicaciones puedan acceder a la información administrativa de la red.

Es frecuente encontrar el término *interfaz de programa de aplicación* (API) asociado a los servicios de la capa de aplicación. Un API es conjunto de reglas que permiten que las aplicaciones escritas por los usuarios puedan acceder a los servicios de un sistema de software. Los diseñadores de programas y protocolos suelen proporcionar varias API para que los programadores puedan adaptar fácilmente sus aplicaciones y utilizar los servicios disponibles en sus productos. Un API habitual de UNIX es Berkeley Sockets; Microsoft lo ha implementado denominándolo Windows Sockets.

Características de los protocolos en forma de capas

El modelo de referencia OSI ilustra varias características de las pilas de protocolos en forma de capas: Cuando un dispositivo transmite datos a la red, las capas del protocolo procesan los datos una a una. La Figura 2-8 muestra los pasos de los dispositivos emisor y receptor.

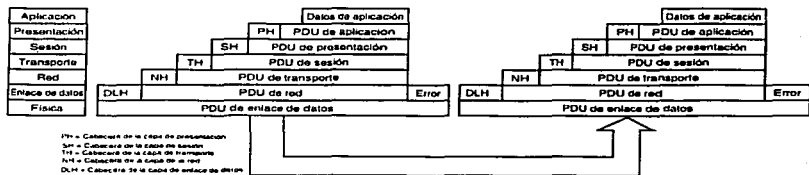


Figura 2-8 Cabeceras y capas del protocolo OSI.

Considere la capa de red del dispositivo emisor. Los datos que se van a transmitir proceden de la capa de transporte. La capa de red se encarga de encaminar los datos y de añadir la información de encaminamiento. La información de la capa de red se añade en forma de cabecera al principio de los datos.

OSI utiliza el término *unidad de datos de protocolo* (PDU) para describir la combinación de la información de control de una capa y de los datos de la capa superior. Según muestra la Figura 2-8, cada capa añade una cabecera a la PDU que recibe de la capa anterior. El campo de datos de cada capa consiste en la PDU de la capa superior. Además, la capa de enlace de datos añade un campo que contiene los datos para el control de errores. La capa física no encapsula de este modo, ya que gestiona los datos bit a bit.

TESIS CON
FALLA DE ORIGEN

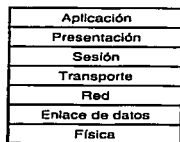
Cuando una capa añade su cabecera a los datos de la capa superior, el proceso equivale a introducir una carta en un sobre. El sobre puede utilizarse para entregar los datos a la dirección correcta para que se abra y se recuperen los datos. Cuando un protocolo utiliza cabeceras para empaquetar los datos de otro protocolo, el proceso se denomina *encapsulación* la capa de red *encapsula* los datos de la capa de transporte.

Cuando los datos recibidos ascienden a través de la pila de protocolos, cada capa elimina la cabecera correspondiente de la unidad de datos. Este proceso se denomina *desencapsulación* y permite que cada capa del dispositivo emisor se comunique con la capa correspondiente del dispositivo receptor. Cada capa del dispositivo emisor se comunica con su capa *hermana* del dispositivo receptor y el proceso se denomina comunicación de *hermano a hermano*.

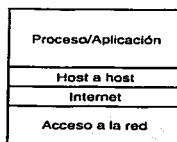
Nota: Como consecuencia del proceso de encapsulación/desencapsulación, dos PDU idénticas existen en las capas correspondientes de las pilas de protocolos emisora y receptora. La PDU de la capa de red del nodo emisor es idéntica a la PDU de la capa de red del nodo receptor.

El modelo Internet

El modelo se remonta a la red ARPAnet (Red de la Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa de los Estados Unidos) y se suele denominar modelo DoD (Department of Defense). La arquitectura del protocolo DoD es anterior a la del modelo de referencia OSI, que data de 1979. Por ello, no es posible establecer una correspondencia sin ambigüedades entre los modelos DoD y OSI. La Figura 2-9 ilustra el modelo Internet de cuatro capas estableciendo las correspondencias posibles con el modelo de referencia OSI.



Modelo de referencia OSI



Modelo Internet

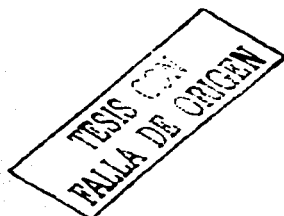


Figura 2-9 Comparación del modelo del protocolo Internet y del modelo de referencia OSI

La capa de acceso a la red se encarga del intercambio de datos entre un host y la red y entre los dispositivos de la misma red. En una red de área local, se utilizan direcciones físicas para realizar la entrega de los datos. El diseño de la arquitectura DoD pretendía utilizar las normas de red existentes, y TCP/IP fue adaptado a muchos tipos de red incluyendo las de conmutación de circuitos (por ejemplo X.21), conmutación de paquetes (como X.25), Ethernet, los protocolos IEEE 802.x, ATM y frame relay.

La capa de interred corresponde a la capa de red de OSI y se encarga de encaminar los mensajes a través de las interredes. Los dispositivos de encaminamiento se denominan gateways en terminología TCP/IP, aunque el uso del término router es el que se utiliza con mas frecuencia. El protocolo TCP/IP de esta capa es el protocolo de interred (IP). Además de las direcciones físicas utilizadas en la capa de acceso a la red, el protocolo IP implementa un sistema de direcciones lógicas de hosts denominadas direcciones IP. La capa de interred y las superiores utilizan direcciones IP para identificar los dispositivos y para realizar el encaminamiento entre las redes. El protocolo de resolución de direcciones (ARP) permite que IP identifique la dirección física correspondiente a una dirección IP.

La capa de host a host es muy similar a la capa de transporte de OSI y se encarga de la integridad de los datos de punto a punto. Esta capa utiliza dos protocolos: protocolo de control de transmisión (TCP) y protocolo de datagramas de usuario (UDP). TCP proporciona fiabilidad en las conexiones de tipo dúplex total y seguridad en el servicio, manteniendo la presencia de los datos cuando se produce un error. Además, TCP permite que los hosts puedan mantener varias conexiones simultáneas. UDP proporciona un servicio no fiable (datagramas) que mejora el rendimiento de la red cuando no se requiere corrección de errores en la capa de host a host.

La capa de proceso/aplicación abarca las funciones de tres capas del modelo de referencia OSI: sesión, presentación y aplicación. No resulta extraño que esta capa del modelo DoD incluya una gran variedad de protocolos. La siguiente lista menciona algunos ejemplos:

- **FTP (File Transfer Protocol -Protocolo de transferencia de archivos).** Realiza transferencias de archivos entre hosts.
- **Telnet.** Permite que los usuarios ejecuten sesiones de terminal con hosts remotos.
- **SMTP (Simple Mail Transfer Protocol -Protocolo simple de transferencia de correo).** Implementa servicios básicos de entrega de mensajes.
- **SNMP (Simple Network Management Protocol - Protocolo simple de administración de red).** Utilizado para recabar información administrativa de los dispositivos de red.

- **NFS (Network File System – Sistemas de archivos de red.** Sistema desarrollado por Sun Microsystem que permite montar unidades en hosts remotos y operar sobre ellas como si fueran locales

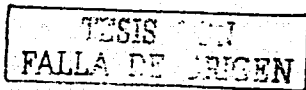
Algunas de estas aplicaciones engloban funciones de varias capas del modelo de referencia OSI. Por ejemplo, NFS permite que los host mantengan una sesión (capa de sesión), define una representación de los datos (capa de presentación) e implementa un sistema de archivos de red (capa de aplicación).

Protocolos de las capas de acceso a la red

Las capas inferiores del modelo de referencia OSI (Física, Enlace de datos y Capa de red) son las responsables de definir cómo han de transferirse los datos a través de un cable físico por medio de la conexión de dispositivos, hasta la estación de trabajo de destino y, finalmente, hasta la aplicación que está del otro lado. Como el objetivo de este trabajo no es otro que analizar las tecnologías para la interconexión de estos dispositivos, a continuación se describen los protocolos de estas capas del modelo OSI.

Los protocolos para redes e interconexión dispositivos y redes que se describen en de este trabajo son:

- IEEE 802.3 (Ethernet IEEE)
- IEEE 802.5 (Token Ring IEEE)
- X.25
- Frame relay
- ATM



Ethernet

Ethernet se basa en el trabajo de científicos del Centro de Investigación de Palo Alto de Xerox (Xerox PARC). Los primeros trabajos condujeron a todas las redes que utilizan el método de control de acceso por detección de portadora. La primera red se denominó Ethernet en honor al éter, la sustancia mítica que permitía el viaje de la luz a través del espacio.

La primera norma Ethernet, DIX 1.0, data de septiembre de 1980. El acrónimo DIX proviene de las tres empresas que colaboraron en su desarrollo: Digital Equipment Corporation, Intel y

Xerox. En noviembre de 1982 se presentó DIX 2.0, una norma revisada denominada comúnmente Ethernet II.

La disponibilidad de Ethernet II coincidió en el tiempo con la expansión de TCP/IP. Ambos están estrechamente asociados y Ethernet es la LAN dominante entre las redes.

Cómo funciona Ethernet

Normalmente, las redes de área local no permiten que más de un nodo transmita al mismo tiempo. Esta limitación plantea un problema, ya que todos los nodos tienen la necesidad de transmitir. Los métodos de control de acceso son sistemas que permiten que muchos nodos puedan acceder a un medio de red compartido mediante la concesión organizada de accesos.

Ethernet utiliza un método eficaz de control de acceso denominado *detección de portadora*. Cuando un nodo necesita transmitir datos, comprueba el medio escuchando si algún otro nodo está transmitiendo. Si el medio está ocupado, el nodo espera unos microsegundos antes de volverlo a intentar. Si el medio está inactivo, el nodo inicia la transmisión. El nombre completo de este método es *acceso múltiple por detección de portadora* (CSMA -Carrier Sensing Multiple Access). Permite que varios nodos accedan a un medio detectando la portadora. El método CSMA se denomina frecuentemente "escuchar antes de hablar".

Debe transcurrir un breve periodo de tiempo antes de que una señal eléctrica alcance el punto del medio al que está siendo enviada. La Figura 2-10 muestra el modo en que dos nodos comprueban una red inactiva e inician la transmisión al mismo tiempo. Dado que las dos señales fluyen a través del medio, es posible que se solapen y causen una colisión. Las colisiones siempre provocan daños en los datos, por tanto, resulta vital disponer de un mecanismo para resolverlas.

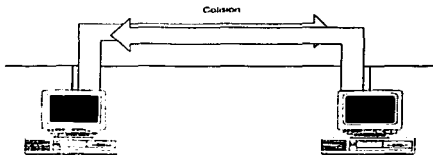


Figura 2-10 Una colisión Ethernet

TESIS CON
FALLA DE ORIGEN

Los nodos Ethernet detectan las colisiones manteniéndose a la escucha mientras transmiten. Si se produce una colisión, los nodos miden que el voltaje de la señal es el doble del esperado. Una vez detectada la colisión, los nodos transmiten una señal de congestión que indica a todos los nodos de la red que ignoren el marco, puesto que se ha producido una colisión. A continuación, el nodo espera un tiempo aleatorio antes de volver a transmitir. Dado que la espera de cada nodo es distinta, la probabilidad de una nueva colisión es escasa. Esta técnica para gestionar colisiones se denomina *detección de colisiones* (CD -Collision Detection). La abreviatura completa del método de control de acceso Ethernet es CSMA/CD.

Los nodos Ethernet solo detectan las colisiones si están transmitiendo. La Figura 2-11 ilustra un problema potencial en la detección de una colisión. Los nodos A y B han enviado marcos que todavía no han colisionado. Cuando se produzca el choque, ningún nodo estará transmitiendo y, por tanto, la colisión no se detectará. Esta situación se debe a que, los marcos no son lo bastante largos como para alcanzar a otro nodo emisor durante su transmisión. El diámetro máximo de una red Ethernet es de 2,500 metros. Dada la velocidad de propagación de las señales a través del medio, se requiere el tiempo de 576 bits para que los primeros bits de una transmisión se propaguen completamente a través de la red. Según se mostrará, el tamaño mínimo de un marco en la especificación Ethernet es de 576 bits. Esta medida garantiza que los nodos que transmiten vean todas las transmisiones que puedan provocar colisiones,

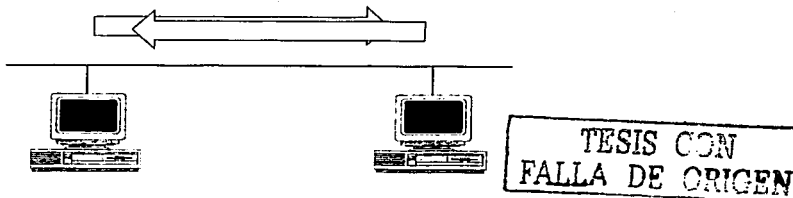


Figura 2-11 Una colisión no detectada.

Las colisiones forman parte del funcionamiento normal de una red Ethernet. Dado que el método de acceso CSMA/CD es excepcionalmente eficiente, una tasa normal de colisiones no reduce significativamente el rendimiento de la red. Sin embargo, en ciertos casos, una red con alto nivel de tráfico puede sufrir un número importante de colisiones que disminuyan su rendimiento y, eventualmente, provoquen un colapso. Esta situación desastrosa ocurre rara vez en una red Ethernet correctamente diseñada con un número razonable de nodos y utilizando las técnicas de segmentación que veremos más adelante.

La mayor virtud del método de acceso CSMA/CD radica en su sencillez. Otras redes, como las Token Ring, emplean mecanismos muy elaborados para controlar el acceso. Ethernet requiere pocos mecanismos y dedica gran parte del ancho de banda de la red a la transmisión de datos útiles. Ethernet ofrece un buen servicio a la mayoría de las redes. La sencillez de CSMA/CD ha permitido la fabricación de hardware Ethernet de muy bajo coste y, en muchos casos, Ethernet es la opción más económica al elegir un medio para la red. Los ingenieros han ampliado el alcance de CSMA/CD para llegar a medios más modernos, como el par trenzado sin blindaje (UTP).

LAS LAN IEEE

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) es la organización profesional que define de normas internacionales en el campo de las redes de área local. El comité 802 (llamado así porque se reunió por primera vez en febrero de 1980), ha definido las normas IEEE para las LAN.

El comité 802 ha definido una amplia gama de normas de redes aunque este trabajo sólo describe unas pocas. Esta sección examina la arquitectura general de las normas 802 junto con las normas de capas físicas más frecuentemente implementados. La ISO (Organización Internacional de Normalización) ha establecido las normas internacionales para las LAN adoptando las normas IEEE 802 bajo el nombre ISO 8802.

Arquitectura de las normas IEEE 802

En su conjunto, las normas IEEE 802 corresponden a las capas OSI de enlace de datos y física. Sin embargo, la arquitectura de las normas IEEE no coincide con la organización de las capas OSI. La Figura 2-12 muestra que la arquitectura IEEE define dos subcapas que corresponden a la capa OSI de enlace de datos.

- **Control de enlaces lógicos (LLC -Logical Link Control).** La subcapa LLC proporciona una interfaz de red para los protocolos de las capas superiores. Se encarga de la transmisión de datos entre dos estaciones de un mismo segmento de la red.
- **Control de acceso al medio (MAC -Medium Access Control).** La subcapa MAC proporciona el método para que los dispositivos accedan al medio de transmisión compartido de la red.

La Figura 2-12 ilustra la relación entre la familia de normas 802 y el modelo de referencia OSI.

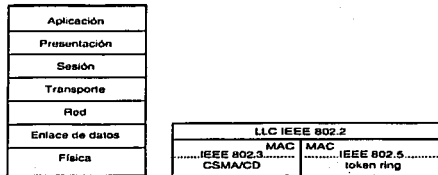


Figura 2-12 Relación entre las normas 802 y el modelo de referencia OSI.

El comité 802 consta de varios subcomités denominados 802.X. Algunos definen normas, otros son consultivos. En este apartado examina las siguientes normas 802.X:

- 802.2. Define el protocolo de la subcapa LLC.
- 802.3. Define las capas MAC y física de las redes CSMA/CD (Ethernet 802.3).
- 802.5. Define las capas MAC y física de las redes token ring basadas en la tecnología Token-Ring de IBM.

La relación existente entre estas normas puede verse en la Figura 2-12. ilustra una importante característica del diseño de las normas 802, esto es: todas las normas de LAN 802 que definen capas físicas de red utilizan el protocolo LLC 802.2. Este enfoque de protocolos por capas simplifica el diseño de sistemas que se adapten a las distintas redes físicas. Es posible convertir fácilmente un sistema Ethernet 802.3 en un sistema Token Ring 802.5 sin modificar las capas de protocolos superiores.

Otra característica consiste en que las normas de red 802.3 y 802.5 amplían la funcionalidad de la capa OSI física, así como la subcapa MAC de la capa de enlace de datos.

Direcciones físicas de las LAN 802

Las normas 802 han sido diseñadas para conseguir la máxima uniformidad posible entre las distintas normas de LAN. Ya se ha mencionado el uso de una capa LLC común para todos los protocolos LAN. Otro aspecto importante consiste en que todos los protocolos de LAN utilizan el mismo esquema de direcciones.

**TESIS CON
FALLA DE ORIGEN**

Bajo el modelo 802, las direcciones físicas de dispositivos quedan definidas al subnivel del protocolo MAC. Por consiguiente, las direcciones físicas suelen denominarse direcciones MAC. Las direcciones MAC pueden tener dos formatos: 16 y 48 bits. Todos los dispositivos de la red deben configurarse para utilizar el mismo formato de dirección. Dado que el formato de 48 bits se utiliza con mayor frecuencia, es el único que se examina en detalle. El formato de una dirección MAC de 48 bits proviene de Ethernet y es válido para IEEE 802, ISO 8802 y otras normas de LAN.

La Figura 2-13 muestra el formato de direcciones de 48 bits.

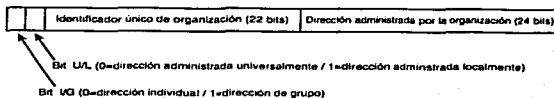


Figura 2-13 Formato de las direcciones MAC IEEE 802.

El primer bit de la dirección (bit 47, el de mayor orden) es el bit I/G. Si su valor es 0, la dirección es individual, si es 1, la dirección es de grupo (multidifusión). Una dirección compuesta por valores 1 en su totalidad en un mensaje de difusión.

El bit 46 se denomina U/L e indica si la dirección se administra universal o localmente. Si su valor es 0, la dirección se refiere a un formato universal compuesto por un identificador único de organización de 22 bits y de una dirección de 24 bits asignada por la organización. Si el valor del bit U/L es 1, la dirección de 46 bits se administra localmente, normalmente por el software del dispositivo de red.

Las organizaciones adheridas al IEEE disponen de un identificador único de 22 bits. Cuando la organización combina su identificador con una dirección de 24 bits asignada a un dispositivo, se obtiene una dirección única para cada dispositivo de red fabricado según las normas LAN IEEE 802.

Control de enlaces lógicos de IEEE 802.2

LLC desempeña varias funciones. Algunas de ellas son opcionales y pueden ser implementadas por los protocolos de las capas superiores.

TESIS CON
FALLA DE ENTRENAMIENTO

Multiplexión y demultiplexión

La función más importante del LLC es la multiplexión y demultiplexión de los datos para distintos protocolos de las capas superiores

Un *punto de acceso al servicio de enlaces* (LSAP -Link Service Access Point) es una interfaz entre la subcapa LLC y los protocolos de las capas superiores. Un LSAP es una dirección lógica que identifica el protocolo de la capa superior del que proceden o al que se envían los datos.

Servicios de entrega LLC

LLC fue diseñado para proporcionar varios servicios de entrega que determinan el nivel de integridad de la comunicación establecida entre los dispositivos. Existen tres tipos de servicios de entrega LLC con distintas características.

Los dispositivos disponen de un número limitado de memorias intermedias de recepción que se utilizan para guardar los marcos recibidos pendientes de procesar. Si el dispositivo emisor continúa la transmisión y las memorias intermedias de recepción están llenas los marcos no recibidos se pierden. El *control de flujo* asegura que los marcos no se envíen a mayor velocidad de la admitida por el dispositivo receptor. Es posible utilizar diversos mecanismos para implementar el control de flujo.

El método de *parada y espera* requiere que el receptor acuse el recibo de los marcos indicando su disposición para recibir nuevos datos. Este sencillo mecanismo es adecuado para un servicio de datagramas sin conexión.

Si el emisor debe esperar el acuse de recibo de cada marco, las transmisiones de múltiples marcos resultan poco eficientes. La técnica de *ventanas deslizantes* es más sofisticada y permite que el emisor transmita múltiples marcos sin esperar cada acuse de recibo. El receptor puede acusar el recibo de varios marcos de una sola vez. Una ventana determina el número de marcos que pueden enviarse en un momento dado sin saturar la memoria intermedia del receptor. La complejidad de este control de flujo requiere el uso de un servicio LLC orientado a la conexiones.

La capa MAC realiza la detección de errores pero su recuperación, cuando se lleva a cabo en la capa de enlace de datos, es una función del LLC. Es posible que el LLC utilice una *solicitud de repetición automática* (ARQ -Automatic Repeat Request) para que cada marco recibido correctamente genere un acuse de recibo. La ARQ de *parada y espera* requiere un acuse de recibo para cada marco y funciona con un servicio sin conexión; los marcos cuyo recibo no se

acusa vuelven a transmitirse. La ARQ *de retroceso* permite que el receptor solicite la retransmisión de marcos específicos y requiere un servicio en modo de conexión.

LLC admite los tres tipos siguientes de servicios de entrega:

- **Servicio de datagramas sin acuse de recibo (servicio de tipo 1).** Este servicio sin conexión admite transmisiones de punto a punto, multipunto y de difusión. No lleva a cabo detección o recuperación de errores ni control de flujo.
- **Servicio de circuito virtual (servicio de tipo 2).** Este modo de conexión proporciona secuencia de marcos, control de flujo, así como detección y recuperación de errores.
- **Servicio de datagramas con acuse de recibo (servicio de tipo 3).** Esta modalidad implementa un servicio de datagramas de punto a punto con acuse de recibo. Es un término medio entre los servicios de tipo 1 y 2.

LLC suele implementarse con el servicio de tipo 1 para mejorar la eficiencia de los protocolos de las capas inferiores. En caso de necesidad, el control de flujo y la recuperación de errores pueden implementarse utilizando un protocolo de transporte adecuado como TCP.

Formato de datos LLC

Al igual que otras capas, LLC construye una unidad de datos de protocolo (PDU) añadiendo los campos específicos de LLC a los datos recibidos de las capas superiores. La Figura 2-14 ilustra el formato de la PDU LLC.

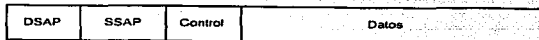
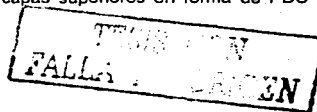


Figura 2-14 Formato de la unidad de datos de protocolo LLC.

La PDU LLC contiene los siguientes campos:

- **Punto de acceso al servicio de destino (DSAP -Destination Service Access Point).** La dirección LSAP que identifica la pila de protocolos en la computadora de destino.
- **Punto de acceso al servicio de origen (SSAP -Source Service Access Point).** La dirección LSAP asociada a la pila de protocolos de la computadora de origen.
- **Control.** Información de control que varía en función de la PDU.
- **Datos.** Datos recibidos de los protocolos de las capas superiores en forma de PDU de capa de red.



Redes IEEE 802.3

Digital, Intel y Xerox entregaron su tecnología Ethernet al IEEE para lograr su normalización. Como resultado, nació la norma 802.3 para LAN de tipo CSMA/CD. El cambio más significativo para la adaptación de Ethernet DIX a la arquitectura 802 fue consecuencia de la decisión de implementar la capa LLC 802.2 como protocolo común a todas las LAN 802.X.

Las redes IEEE 802.3 utilizan el mismo mecanismo de control de acceso CSMA/CD desarrollado para Ethernet II. Se emplean las mismas técnicas de señalización del medio y es posible intercambiar el hardware de red 802.3 y Ethernet II

Medios IEEE

El comité 802.3 adoptó los sistemas de cableado utilizados por Ethernet II. Estaban basados en cable coaxial y en una velocidad de datos de 10 megabits por segundo. Desde entonces, el comité ha desarrollado varias configuraciones de medios más modernos.

Cada una de las normas de cableado 802.3 cuenta con un nombre compuesto por tres partes (por ejemplo 10BASE5). El primer número indica la velocidad de datos, donde 10 significa 10 megabits por segundo. BASE especifica el funcionamiento en banda base y BROAD en banda ancha. La última parte indica el tipo de cable. Por ejemplo, 5 indica una configuración que admite cables de hasta 500 metros de longitud.

- **10BASE5.** Es la configuración original de las redes Ethernet y utiliza un cable coaxial grueso de 50 ohms. Los cables pueden alcanzar 500 metros sin necesidad de repetidores y cada sección de cable admite hasta 100 estaciones conectadas. El cable de la norma 10BASE5 es costoso y difícilmente manejable, por lo que se utiliza con menor frecuencia que otras opciones.
- **10BASE2.** El diseño de este sistema perseguía ofrecer una alternativa económica al sistema 10BASE5. Utiliza un cable coaxial más delgado que admite segmentos de hasta 185 metros (el número 2 indica una longitud aproximada de 200 metros). 10BASE2 es económico y más fácil de instalar que 10BASE5, pero no se adapta bien a los sistemas de cableado estructurado que se configuran tirando un cable desde cada dispositivo hasta un concentrador (hub) central. Actualmente, el cableado estructurado se utiliza en la mayoría de instalaciones de tamaño medio y alto.
- **10BASE-T.** La tendencia general consiste en reducir el uso de cables coaxiales y otros tipos de cable blindado. Los diseñadores confían crecientemente en el cable de tipo par trenzado no blindado (UTP -Unshielded twisted pair) cuyo coste es ligeramente inferior al

del cable coaxial. La letra T indica el uso del cable de tipo par trenzado. 10BASE-T utiliza un sistema de cableado basado en un concentrador y se adapta perfectamente al concepto de cableado estructurado.

- **10BROAD36.** Un sistema de cable de banda ancha que permite mantener varios canales de 10 Mbps en un mismo cable coaxial.
- **100BASE-TX.** Distintos comités IEEE 802 están evaluando varias normas de 100 Mbps. Todas utilizan cables UTP, pero difieren en la clase del cable y en el número de pares necesarios. 100BASE-TX utiliza un cable UTP de dos pares de clase alta (categoría 5). 100BASE-T4, una de las normas de 100 Mbps, utiliza un cable UTP de cuatro pares de datos estándar (categoría 3). 100BASE-FX emplea cables de fibra óptica.

Marcos IEEE 802.3

La Figura 2-15 ilustra el formato de un marco IEEE 802.3.

| | | | | | | |
|--------------------------|--|-------------------------------------|------------------------------------|-------------------------|--------------------------------|--------------------|
| Preámbulo (7 octetos) | Delimitador de inicio de marco (1 octeto) | Dirección de destino (6 octetos) | Dirección de origen (6 octetos) | Longitud (2 octetos) | Datos LLC (46-1500 octetos) | FCS (3 octetos) |
|--------------------------|--|-------------------------------------|------------------------------------|-------------------------|--------------------------------|--------------------|

Figura 2-15 Formato de un marco IEEE 802.3.

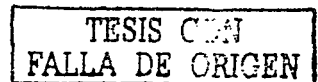
El preámbulo 802.3 consta de siete bytes que siguen el patrón 10101010. Va seguido de un byte delimitador de inicio del marco (SFD -Start Frame Delimiter) con el patrón de bits 10101011.

La *dirección de destino* y la *dirección de origen* admite direcciones de 48 bits. El formato de las direcciones físicas 802 se ha descrito en la sección *Direcciones físicas de las LAN 802*.

El campo *longitud* consta de dos bytes que indican el número de bytes del campo de datos LLC. El valor debe estar comprendido entre 46 y 1,500.

El campo de *datos LLC* contiene la unidad de datos de protocolo recibida de la subcapa LLC y consta de la cabecera LLC y de los datos. El tamaño de este campo está comprendido entre 46 y 1,500 bytes. Si el campo de datos no alcanza los 46 bytes mínimos se añaden bytes con valor 00000000 para rellenar el campo.

El campo *secuencia de verificación del marco* (FCS -Frame Check Sequence) es una suma de verificación que permite detectar errores en la transmisión.



Redes IEEE 802.5 (Token Ring)

IBM desarrolló la red Token Ring y la cedió al IEEE para su normalización. El subcomité 802.5 se encargó de esta tarea. Token Ring IEEE 802.5 es la segunda capa física de LAN más utilizada, aunque a gran distancia de Ethernet. La escasa popularidad de las redes Token Ring se debe a las siguientes razones:

- Fue desarrollada como tecnología IBM. Aunque muchos fabricantes ofrecen actualmente esta tecnología, gran parte de los usuarios perciben la sensación de que es propiedad de IBM.
- Ethernet es sencilla, fiable y efectiva para la amplia mayoría de las redes. Además, su costo es muy inferior al de una red Token Ring.
- TCP/IP ha estado ligado desde siempre a Ethernet. La demanda creciente de TCP/IP ha impulsado un nuevo auge de Ethernet. Sin embargo, Token Ring es una tecnología de capa física muy efectiva y, en ciertos casos, sus características la hacen preferible.

Como funciona una red Token Ring

IBM desarrolló la tecnología Token Ring (anillo de señales) para superar una deficiencia del método de acceso CSMA/CD. Existe la posibilidad de que la red esté ocupada cada vez que un dispositivo necesita transmitir. Incluso cuando el dispositivo inicia una transmisión, existe la probabilidad de que otro transmita y provoque una colisión obligando a ambos dispositivos a intentar una nueva transmisión. Estas probabilidades aumentan con el nivel de actividad de la red y, en casos extremos, un dispositivo puede ser incapaz de encontrar la ocasión para transmitir. Dado que el acceso a una red CSMA/CD no está garantizado, se dice que el método de acceso CSMA/CD está basado en la probabilidad.

La simple probabilidad de acceso no es aceptable en ciertas situaciones críticas como el control industrial. Imaginemos la situación en la que un sensor de sobrecalentamiento deba enviar una advertencia urgente a los operadores de una fábrica. Los diseñadores de la fábrica no aceptarían la más mínima posibilidad de que el sensor no pudiera emitir.

El acceso por señales garantiza que cada dispositivo de la red reciba periódicamente la oportunidad de transmitir. El método de acceso por señales elegido por IBM fue desarrollado en un anillo según muestra la Figura 2-16

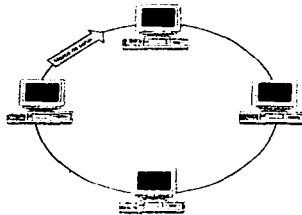


Figura 2-16 El método de acceso de señales en una red de anillo

La señal es un marco especial que circula de un dispositivo a otro a lo largo del anillo. El dispositivo propietario de la señal es el único que puede transmitir. Después de la transmisión, el dispositivo reinicia la señal permitiendo que otros puedan transmitir.

La implementación inicial Token Ring de IBM (4 Mbps) permitía la circulación de una sola señal por la red. Antes de liberar una señal para permitir que los dispositivos restantes transmitieran, el dispositivo emisor del marco debía esperar su retorno después de haber circulado por el anillo. Una nueva característica denominada liberación anticipada de señal, presentada con la tecnología Token Ring de 16 Mbps, permite que un dispositivo emisor libere una señal inmediatamente después de finalizar la transmisión de un marco. De este modo, una señal puede circular al mismo tiempo que un marco de datos.

Token Ring ofrece importantes beneficios. El caudal de datos de una red Token Ring nunca puede alcanzar el nivel cero, situación teóricamente posible en una red Ethernet con exceso de colisiones. Aunque el rendimiento de la red disminuye a medida que aumenta la demanda, todo dispositivo dispone de una oportunidad periódica para transmitir.

Token Ring permite establecer las prioridades de acceso de la red, lo cual es imposible con Ethernet. Los dispositivos prioritarios pueden obtener un acceso preferente a la red. Esta posibilidad permite que los dispositivos críticos consigan mayores cuotas de acceso a la red.

Token Ring fue diseñado para permitir un mayor nivel de diagnósticos y de administración que el de Ethernet. Los mecanismos de recuperación de errores permiten al mismo tiempo diagnosticar otros problemas de la red. Por ejemplo, es posible detectar los dispositivos que causan errores y desconectarlos de la red. Además, el sistema de cableado diseñado por IBM

utiliza dos anillos de cables para dar servicio a la red. Si uno de ellos falla, es posible utilizar el otro para reconfigurar la red y mantenerla operativa.

Sin embargo, Ethernet sigue siendo la capa física de red que goza de mayor popularidad. Ethernet funciona adecuadamente en la mayoría de las redes y su costo es considerablemente inferior al de Token Ring. El costo de los dispositivos para redes Token Ring, duplica o triplica al de los componentes Ethernet.

Medios Token Ring

IEEE 802.5 no describe un sistema de cableado para Token Ring. Se limita a proporcionar especificaciones para la velocidad de los datos, la señalización y la interfaz de red. Con frecuencia, los fabricantes diseñan sus equipos para el sistema de cableado IBM (IBM Cabling System) desarrollado a principios de los ochenta. El cable más popular es el de tipo 1, un cable grueso de par trenzado y apantallado con excelentes características eléctricas pero demasiado voluminoso y costoso. El tipo 3 es un cable UTP de datos. IBM admite una velocidad de 4 Mbsp en los cables de tipo 1 y 3. Actualmente IBM y otros fabricantes suministran cable UTP para 16 Mbps. IBM ha anunciado un nuevo sistema de cableado que permitirá operar a 100 Mbps.

Aunque las redes Token Ring operan como anillos a nivel lógico, el sistema físico de cables tiene forma de estrella en la que todos los dispositivos se conectan a un concentrador central MAU utilizando su propio cable. La Figura 2-17 muestra la configuración de cables en estrella para una red Token Ring.

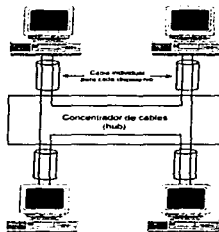


Figura2-17 Configuración de cables en estrella para una Token Ring

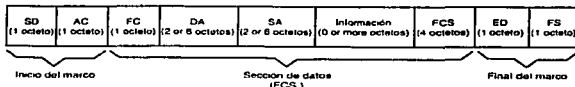
TESIS CON
FALLA DE ORIGEN

Token Ring puede admitir un máximo de 260 dispositivos pero normalmente se conecta un número menor. La planificación de estas redes resulta complicada debido a que el número de dispositivos permitidos varía en función del tamaño del anillo y de la velocidad de los datos.

Marcos IEEE 802.5

La Figura 2-18 muestra el formato del marco Token Ring. Consta de tres secciones principales:

- **Secuencia de inicio del marco (SFS -Start-of-Frame Sequence).** Esta sección indica el inicio de un marco a los dispositivos de la red.
- **Sección de datos.** Contiene información de control, los datos de la capa superior y la secuencia de verificación del marco utilizada para la detección de errores
- **Secuencia de final del marco (EFS -End-of-Frame Sequence).** Esta sección indica el final de un marco y consta de varios bits de control.



SD = Delimitador de inicio SA = Dirección de origen
 AC = Control de acceso FCS = Secuencia de verificación de datos
 FC = Control de marco ED = Delimitador de final
 DA = Dirección de destino FS = Estado de marco

Figura 2-18 Formato de un marco token ring.

El campo *delimitador de inicio (SD)* es un byte que consta de señales eléctricas que no puedan aparecer en ningún otro lugar del marco. El SD viola las reglas de codificación de datos del marco y contiene señales que no son de datos.

El campo *control de acceso (AC)* incluye bits de prioridad y de reserva utilizados para establecer las prioridades de la red. Incluye igualmente un bit de control utilizado para la administración de la red. Un bit de señal indica si el marco es de señal o de datos.

El campo *control de marco (FC)* indica si el marco contiene datos LLC o si se trata de un marco de control MAC. Es posible utilizar varios tipos de marcos de control MAC para controlar las funciones de la red.

TESIS
 FALLA DE ORIGEN

La *dirección de destino (DA)* especifica la o las estaciones a las que va dirigido el marco. Además de las transmisiones a un dispositivo, se aceptan difusiones y multidifusiones. Se admiten direcciones de 16 y 48 bits.

La *dirección de origen (SA)* especifica el dispositivo que ha originado el marco. Debe emplearse el mismo formato para la DA y la SA.

La *secuencia de verificación de marco (FCS)* es una verificación de redundancia cíclica de 32 bits que se aplica a los campos FC, DA, SA y de información.

El *delimitador de final (DE)*, al igual que el delimitador de inicio, viola el formato de datos de red e indica el final de un marco. Este campo incluye dos bits de control. El bit intermedio indica si se trata de un marco intermedio o del marco final de una transmisión. El bit de error queda marcado por cualquier dispositivo que detecte un error en la FCS.

El *campo estado de marco (FS)* contiene otros bits de control que indican si una estación ha reconocido su dirección y si el dispositivo receptor ha copiado el marco.

Capítulo III Interconexión de redes

En este capítulo se describen las tecnologías para extender una red utilizando los repetidores, puentes (bridges), conmutadores (switches) y encaminadores (routers). También se describen las tecnologías para la conexión de redes MAN Y WAN

Transferencia de datos a través de interredes

Cuando se describan los protocolos que tratan sobre el modo en que los datos se comportan a través de las interredes encontraremos varios conceptos de redes que se explican en esta sección y que son:

- Métodos para transportar varias corrientes de datos en un medio común, una técnica denominada multiplexión.
- Métodos para intercambiar datos a través de las rutas de la red.
- Métodos para determinar qué ruta se debe utilizar.

Multiplexión

Las LAN funcionan normalmente en modo de *banda base*, lo que significa que un cable transporta una única señal en un momento dado. Los dispositivos de la LAN deben turnarse para utilizar el medio. Este método es aceptable para las LAN debido a que los medios empleados ofrecen un alto rendimiento a bajo costo.

La instalación y el mantenimiento de los medios para comunicaciones de datos de larga distancia resultan costosos y resultarían deficientes si cada ruta sólo pudiera admitir una corriente de datos. Imaginemos el costo que supondría equipar cada teléfono con su propio satélite de comunicaciones o cable submarino para establecer una conexión con Europa. Las WAN tienden a utilizar medios de *banda ancha*, que son capaces de admitir dos o más corrientes de datos. A medida que se exige que las LAN transporten mayor cantidad y variedad de datos, los medios de banda ancha se aplican igualmente a este tipo de redes.

La técnica denominada multiplexión permite que varias corrientes de datos compartan un mismo medio de alto ancho de banda. La Figura 3-1 ilustra un método de multiplexión de señales digitales. La capacidad portadora de señales del medio se divide en intervalos de tiempo asignando un intervalo a cada señal. Esta técnica se denomina multiplexión por división de tiempos

(TDM). Dado que los dispositivos emisor y receptor están sincronizados para reconocer los mismos intervalos de tiempo, el receptor puede identificar cada corriente de datos y crear la señal original.



Figura 3-1 Multiplexión por división de tiempos.

El dispositivo emisor sitúa los datos en los intervalos de tiempo, y se denomina multiplexor o mux. El dispositivo receptor se denomina demultiplexor o demux.

La TDM puede resultar ineficiente. Si termina una corriente de datos, sus intervalos de tiempo quedan inutilizados y el ancho de banda no se aprovecha plenamente. La Figura 3-2 ilustra una técnica más avanzada: la *multiplexión por división estadística de tiempos* (stat-TDM). También utiliza intervalos de tiempo, pero algunas corrientes reservan más intervalos a ciertas corrientes que a otras. Un canal sin actividad no dispone de ningún intervalo. El dispositivo que lleva a cabo la TDM estadística se denomina stat-MUX.

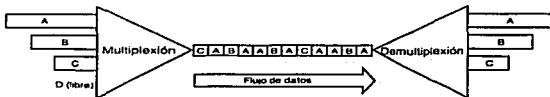
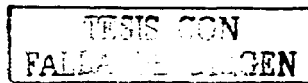


Figura 3-2 Multiplexión por división estadística de tiempos.

Conmutación de datos.

En toda interred, las unidades de datos deben conmutarse a través de varios dispositivos intermedios hasta que se entregan en sus destinos. Se utilizan comúnmente dos métodos muy distintos para conmutar los datos: *La conmutación de circuitos* y *la conmutación de paquetes*.



Conmutación de circuitos

La Figura 3-3 ilustra la conmutación de circuitos. Cuando dos dispositivos negocian el principio de un diálogo, establecen una ruta (denominada circuito) a través de la red, así como un ancho de banda dedicado en el circuito. A continuación, todos los datos del diálogo fluyen a través del circuito. Este enfoque es similar a una conexión telefónica en la que se establece un circuito de voz para que dos terminales puedan comunicarse. La desventaja principal de este método consiste en que, cuando se establece la comunicación a menor capacidad de la asignada al circuito, se desperdicia el ancho de banda. Además, los dispositivos no pueden beneficiarse de otras rutas con menor tráfico a no ser que se reconfigure el circuito.

La conmutación de circuitos no implica necesariamente la existencia continua de una ruta física para uso exclusivo del circuito. La corriente del mensaje puede multiplexarse con otras en un circuito de banda ancha. De hecho, las comunicaciones modernas tienden a compartir un mismo medio. A efectos de los dispositivos terminales, la red configura un circuito dedicado a su uso exclusivo.

Los dispositivos terminales pueden beneficiarse de la conmutación de circuitos. Desde el momento en que la ruta queda preestablecida, el tránsito de los datos que viajan por la red requiere muy poco proceso. Dado que los mensajes fragmentados se transmiten secuencialmente a través de la misma ruta, los segmentos se reciben ordenadamente y el esfuerzo dedicado a su reconstrucción es mínimo.

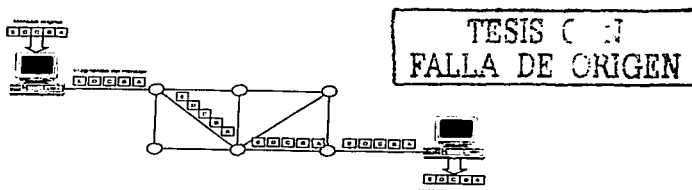


Figura 3-3 Conmutación de circuitos.

Conmutación de paquetes

La conmutación de paquetes utiliza un enfoque distinto, y generalmente más eficiente, para conmutar datos a través de una red. A finales de los sesenta, la conmutación de paquetes era un

nuevo concepto investigado por el DoD durante la fase inicial de la red ARPAnet. Según muestra la Figura 3-4, los mensajes se parten en secciones, denominadas *paquetes*, que se encaminan por separado a través de la red. El dispositivo receptor reensambla los paquetes para construir el mensaje completo. La división en paquetes impide que un mensaje largo monopolice la red. Los paquetes de distintos mensajes pueden multiplexarse a través de un mismo canal de comunicación, por lo que la conmutación de paquetes permite compartir eficazmente todo el ancho de banda de la red.

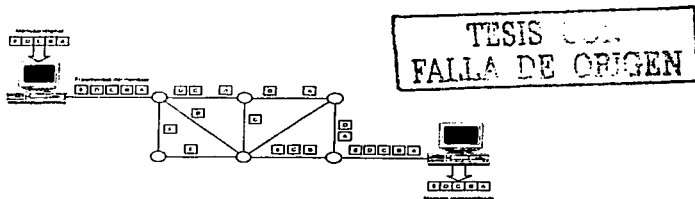


Figura 3-4 Conmutación de paquetes

Pueden utilizarse dos variantes de la conmutación de paquetes:

- Los servicios de *datagrama* tratan cada paquete como un mensaje independiente. Los paquetes, denominados igualmente datagramas, se encaminan a través de la red utilizando la ruta más eficiente disponible en cada momento. De este modo, los conmutadores pueden omitir los segmentos con mayor actividad y utilizar los de menor tráfico. Las LAN suelen utilizar datagramas y los protocolos de la capa de red se encargan de su encaminamiento. El servicio de datagramas se denomina *no fiable* debido a que no garantiza la entrega de los datos. Los protocolos de las capas superiores se encargan de recuperar los posibles errores. Además, si es preciso reconstruir un mensaje a partir de varios fragmentos, las capas superiores se encargan de reensamblar ordenadamente los datagramas. Los protocolos que proporcionan un servicio de datagramas se denominan *protocolos sin conexión*.
- Los *circuitos virtuales* establecen una conexión formal entre dos dispositivos simulando un circuito dedicado. Al establecer la *conexión*, se seleccionan de mutuo acuerdo los parámetros de comunicación, el tamaño de los mensajes, la capacidad de las memorias intermedias y las rutas de la red. Un circuito virtual define una conexión, una ruta de comunicación a través de la red, y permanece activo mientras se mantenga la comunicación entre los dispositivos. Al finalizar la comunicación, un procedimiento formal

libera el circuito virtual. Un circuito virtual garantiza la entrega de los datos y, por tanto, proporciona un servicio fiable. Los protocolos de las capas superiores no necesitan encargarse de la detección y recuperación de los errores. Los protocolos asociados a los circuitos virtuales se denominan *orientados a conexiones*.

En TCP/IP, el protocolo de datagramas de usuario (UDP) proporciona el servicio de datagramas. La amplia mayoría de los sistemas se basan en el protocolo de control de transmisión (TCP) para proporcionar entregas fiables.

Bridges, routers y switches

Es posible encaminar datos a través de una interred utilizando los tres tipos siguientes de información:

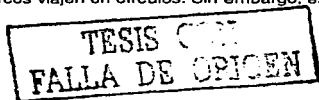
- La dirección física del dispositivo de destino en la capa de enlace de datos. Los dispositivos que hacen progresar los mensajes en base a direcciones físicas se denominan puentes (bridges).
- La dirección de la red de destino en la capa de red. Los dispositivos que utilizan direcciones de red para hacer progresar los mensajes se denominan encaminadores (routers), aunque su nombre original es gateway (término utilizado con frecuencia en TCP/IP).
- El circuito establecido para una conexión. Los dispositivos que encaminan mensajes en base a los circuitos asignados se denominan conmutadores (Switches).

Las secciones siguientes describen cada uno de estos dispositivos.

Bridge (Puente)

Los bridges crean y mantienen una base de datos con las direcciones conocidas de los dispositivos y con la información que permite llegar a ellos. Al recibir una trama, el bridge consulta su base de datos para determinar la conexión que debe utilizarse para enviar el marco. La Figura 3-5 ilustra el proceso a partir del modelo de referencia OSI. Un bridge sólo debe implementar las capas física y de enlace de datos de la pila de protocolos.

Los bridges son dispositivos muy sencillos. Reciben marcos de una conexión y los envían a sus destinos a través de rutas conocidas. Cuando existe más de una ruta posible, generalmente los puentes no pueden determinar cuál de ellas es más eficiente. De hecho, si se produce esta circunstancia, el uso de bridges puede provocar que los marcos viajen en círculos. Sin embargo, es



recomendable que la red cuente con varias rutas disponibles para impedir que el fallo de una de ellas paralice la red. Las redes Ethernet utilizan una técnica denominada algoritmo de árbol de extensión (spanning tree algorithm) que permite que una red con bridges y switches contengan rutas redundantes.

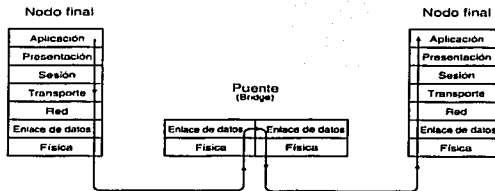


Figura 3-5 El modelo de pila de protocolos al utilizar puentes.

Las redes Token Ring utilizan un enfoque distinto para gestionar los bridges. Cuando un dispositivo necesita enviar datos a otro, inicia un proceso de exploración para determinar una ruta hasta su destino. La información de la ruta se almacena en cada trama transmitida, y los bridges la utilizan para hacer llegar las tramas a las redes adecuadas. Aunque se trata de una función de la capa de enlace de datos, esta técnica se denomina encaminamiento en origen. Observe que en la Figura 3-5 el bridge debe implementar dos pilas de protocolos: una para cada conexión. En teoría, estas pilas podrían pertenecer a protocolos distintos, permitiendo la conexión de distintos tipos de red. Sin embargo, como se explicó anteriormente, Ethernet y Token Ring hacen uso de sus propios protocolos en la capa de enlace de datos. La conversión de los datos de la capa de enlace de datos de una red Ethernet a la de una red Token Ring es difícil. Por tanto, los bridges que operan en la capa de enlace de datos suelen vincular redes del mismo tipo.

Dado que los bridges ignoran las direcciones de red, no pueden utilizarse para crear interredes extensas compuestas por varias redes. Con frecuencia, el tamaño de las redes depende de las limitaciones tecnológicas.

Router (Encaminar)

Otro método para determinar las rutas consiste en utilizar los datos de la capa de red que identifican las redes mediante identificadores lógicos. Esta información permite trazar un esquema

de la red que se utiliza para elegir las rutas con mayor eficiencia. Los dispositivos que se basan en las direcciones de red para enviar datos se denominan Routers.

La Figura 3-6 ilustra un modelo de pila de protocolos que utiliza enrutamiento.

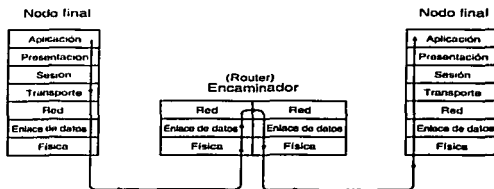


Figura 3-6 Un modelo de pila de protocolos que utiliza enrutamiento.

En TCP/IP, el enrutamiento es una función de la capa de red. A continuación se describe brevemente esta técnica.

La Figura 3-7 ilustra una red. La cuenta de saltos indica el número de redes que se deben atravesar entre dos nodos terminales. Es posible identificar una gran cantidad de caminos entre A y E:

- A-B-C-E (5 saltos)
- A-E (3 saltos)
- A-D-E (4 saltos)

TESIS CON
FALLA DE ORIGEN

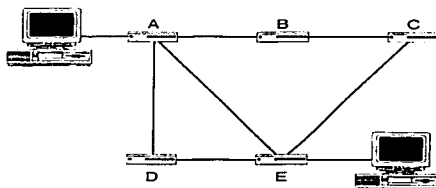


Figura 3-7 Enrutamiento por cuenta de saltos.

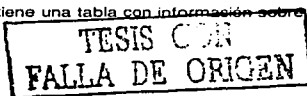
Según este método, la ruta más eficiente es A-E si se parte de la base de que todos los tramos que unen los routers ofrecen el mismo nivel de servicio. No sería adecuado utilizar un algoritmo de cuenta de saltos si las líneas A-D y D-E fueran de 1,5 Mbps mientras que la línea A-E fuera de 56 Kbps. Exceptuando estos casos extremos, el enrutamiento por cuenta de saltos supone una mejora clara.

El enrutamiento trabaja sobre la capa de red. Cuando los datos llegan a la capa, han desaparecido todas las pistas de la red física. Por tanto, las dos pilas de protocolos del router de la Figura 3-6 pueden compartir el mismo protocolo de la capa de red. La capa de red es ajena al hecho de que la red sea Ethernet o Token Ring. Por consiguiente, los routers, a diferencia de la mayoría de los bridges, tienen la capacidad de dirigir el tráfico entre distintos tipos de redes. Gracias a esta capacidad, los routers suelen utilizarse para conectar redes LAN a redes WAN.

Switch (Conmutador)

Básicamente un switch LAN es un puente dotado de una gran cantidad de puertos. Además, utiliza técnicas que permiten aumentar la velocidad de envío de las tramas. Por ejemplo, no suelen perder tiempo guardando la totalidad de un paquete en la memoria intermedia antes de enviarlo; una vez identificada la dirección física de destino, el switch puede iniciar el envío del paquete sin esperar a recibir el final del marco. Por consiguiente, un switch LAN no puede utilizar el campo de control de errores para determinar si la trama se ha recibido correctamente. En entornos de red fiables, la ausencia de una verificación de integridad es aceptable a favor de una mayor velocidad. Dado que se basan en las direcciones de la capa de enlace de datos, los switch LAN (y los bridges) no pueden utilizarse para construir interredes,

Las redes basadas en circuitos operan con gran eficacia, ya que la ruta sólo se establece una vez al abrir el circuito. Cada switch de la Figura 3-8 mantiene una tabla con información sobre



el modo en que deben conmutarse los circuitos. La conmutación suele ser tarea de los protocolos de bajo nivel para mejorar la eficiencia y está estrechamente relacionada con la capa de enlace de datos.

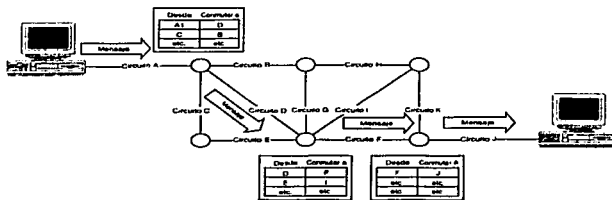


Figura 3-8 Conmutación.

En la realidad, no es frecuente que los circuitos se asemejen a los de la Figura 3-8, un cable dedicado a cada circuito de comunicación. Habitualmente, se multiplican varios circuitos en un solo canal y la multiplexión queda oculta para los nodos terminales. Este tipo de circuitos se denominan circuitos virtuales, ya que para los nodos terminales se trata de circuitos físicos aunque comparten el ancho de banda de la red con otros circuitos virtuales.

Servicios de digitales

Cuando la extensión de las redes supera unos pocos kilómetros entran en escena nuevos tipos de tecnologías. Antes de considerar las normas de las redes de área extensa (WAN) es conveniente examinar las algunas opciones disponibles para construir una WAN privada.

Líneas dedicadas

Los proveedores de comunicaciones ofrecen líneas dedicadas de varias capacidades. Una línea dedicada es un canal de comunicación entre dos puntos alquilado por una organización para su uso exclusivo. La línea dedicada no consiste en un par de cables tendidos entre dos puntos terminales. La señal de un cliente puede atravesar cualquier combinación de cables de cobre y de fibra óptica, así como microondas terrestres y vía satélite. Sin embargo, de cara al cliente la apariencia es la de un canal cableado directamente.

Las líneas dedicadas pueden ser analógicas o digitales. Antiguamente, las líneas dedicadas analógicas de 56 Kbps se utilizaban con frecuencia para interconectar grandes computadoras. En la actualidad crece el número de líneas dedicadas digitales, y las líneas de servicio digital de datos (DDS - Digital Data Service) de 64 Kbs son una opción viable.

La portadora T1 es un ejemplo de tecnología de línea digital dedicada. Las líneas T1 fueron las primeras portadoras digitales empleadas en los Estados Unidos. Admite comunicaciones dúplex total entre dos puntos. Inicialmente diseñada para comunicaciones digitales de voz, T1 se adapta correctamente a la comunicación de datos y admite velocidades de hasta 1,544 Mbps. Los circuitos T1 pueden utilizar combinaciones de cables y enlaces de microondas.

Una línea T1 admite 24 canales digitales de 64 Kbps con multiplexión, los datos de control utilizan parte del ancho de banda. En algunas zonas es posible alquilar parte de una línea T1 en incrementos de 64 Kbps pagando únicamente el ancho de banda utilizado. Otras normas como T2, T3 y T4 admiten velocidades de datos de 6,312, 44,736 y 274,176 Mbps..

La portadora ampliamente utilizada en México es la Llamada E1 y está basada en el estándar de la Conferencia Europea de Correos y Telecomunicaciones (CEPT). La línea E1 multiplexa 32 canales de 64 Kbs estableciendo una velocidad de 2,048 Mbps.

Una organización que desee conectar computadoras remotas puede optar por utilizar una línea dedicada con una configuración similar a la de la Figura 3-9 La interfaz a la línea alquilada consta de los siguientes componentes:

- Un bridge o un router para transmitir los marcos al circuito alquilado.
- Una unidad de servicio de canal/unidad de servicio digital (CSU/DSU) para traducir los formatos de señales LAN a DDS y viceversa.
- Una interfaz de red proporcionada por el proveedor de comunicaciones.

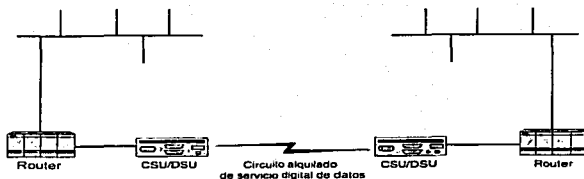


Figura 3-9 Conexión de computadoras remotas utilizando un circuito digital alquilado.

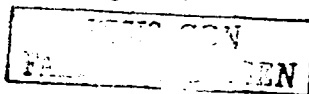
Las líneas alquiladas permiten construir redes muy extensas. Internet es una red a nivel mundial que consiste en miles de servidores, muchos de ellos conectados a través de líneas alquiladas. Los participantes en Internet comparten el costo de la red soportando el gasto de una o más líneas alquiladas para conectarse a otros hosts.

El punto negativo de las líneas alquiladas consiste en que una organización asume el costo de toda la capacidad alquilada. Es necesario prever los momentos de mayor tráfico en la red, pero parte de la capacidad que se paga puede quedar infrutilizada gran parte del tiempo. Las líneas dedicadas garantizan una gran capacidad de comunicación, pero su costo es elevado.

Líneas digitales conmutadas

Las líneas conmutadas son una alternativa a las dedicadas. Cuando un host remoto necesita comunicarse con otro, le llama para establecer una conexión temporal. Las conexiones conmutadas pueden configurarse utilizando módems convencionales y líneas de voz. Permiten que las organizaciones que no requieran un elevado ancho de banda ahorren el gasto de un servicio digital. También existen servicios digitales conmutados y CSU/DSU de 56 Kbps conmutados.

Una tecnología que permite reducir el costo de las comunicaciones digitales conmutadas es la Red Digital de Servicios Integrados (RDSI o ISDN). Existen varios servicios RDSI que proporcionan distintos anchos de banda. El servicio básico más común consta de dos canales digitales de 64 Kbps. Aunque el ancho de banda potencial es de 128 Kbps, los canales de 64 Kbps funcionan independientemente. El equipo del cliente debe ser capaz de agregar los dos canales de 64 Kbps para obtener un canal lógico de 128 Kbps. RDSI ofrece la posibilidad de extender las comunicaciones digitales conmutadas con un bajo costo. Sin embargo, los proveedores de



servicios han tardado en comercializar esta tecnología. En los últimos tiempos, RDSI está disponible principalmente en las áreas metropolitanas.

X.25

Los circuitos dedicados tienen una serie de inconvenientes. Su uso resulta gravoso y el costo de su configuración es muy elevado cada vez que se produce un cambio. Además son inflexibles, ya que el cambio de ubicación de un host puede resultar muy complicado. A menudo, es más razonable adquirir servicios de datos en un proveedor de red, al igual que se adquieren los servicios de telefonía.

Un proveedor de red construye una red de datos que da servicio a un área geográfica con capacidad para soportar los grandes niveles de tráfico de sus clientes. Los clientes que necesitan conectar distintos hosts dentro del área cubierta; se conectan a la red y pagan una parte de su ancho de banda.

X.25 es una de las tecnologías WAN más antiguas y disponibles. Es una recomendación de la Unión Internacional de Telecomunicaciones (ITU), antiguamente denominada Comité Internacional Consultivo de Telégrafos y Teléfonos (CCITT). La ITU es la agencia de Naciones Unidas que establece la normativa internacional de comunicaciones.

X.25 es una red de conmutación de paquetes. Los dispositivos se comunican a través de ella estableciendo circuitos virtuales. Al igual que sucede al marcar un número de teléfono, los dispositivos pueden configurar circuitos virtuales para satisfacer una necesidad de comunicación de duración limitada. Es posible establecer circuitos virtuales permanentes que funcionan de modo similar a los circuitos dedicados.

La norma X.25 utiliza tres protocolos que corresponden a las capas de red, de enlace de datos y física del modelo OSI (véase la Figura 3-10). X.21 proporciona la funcionalidad de la capa física para los circuitos digitales y X.21 bis para los analógicos. A nivel de la capa de enlace de datos, el protocolo Link Access Procedures Balance (LAPB) proporciona comunicaciones síncronas de tipo dúplex total. Por último, el protocolo X.25 proporciona servicio fiable y control de flujo en la capa de red.

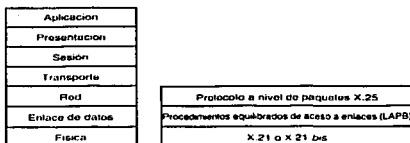


Figura 3-10 La pila de protocolos X.25.

X.25 proviene de una época en la que las líneas de comunicación eran lentas y poco fiables. Su velocidad máxima, 64 Kbps, es adecuada para las conexiones terminal-host basadas en caracteres, pero resulta muy limitada para las aplicaciones actuales en tiempo real que requieren velocidades de LAN.

Dado que fue diseñado para proporcionar comunicaciones fiables basadas en líneas poco fiables, el protocolo X.25 se encarga de la detección de errores y de su corrección mediante la solicitud de retransmisión de los paquetes dañados. Las comunicaciones digitales modernas son altamente fiables y las características de corrección de errores de X.25 sólo suponen una carga de trabajo que disminuye el rendimiento del proceso. En X.25, cada conmutador de la ruta verifica los errores. Actualmente, se opta por comprobar la integridad de los datos en el nodo final para evitar verificaciones redundantes.

La Figura 3-11 ilustra una red X.25. La propia red consta de varios conmutadores X.25 que encaminan los marcos a través de la red. El usuario es ajeno a la mecánica de la conmutación. Por esta razón, las WAN como X.25 suelen dibujarse como nubes que representan la naturaleza oculta del proceso de conmutación. Los paquetes entran en la red en un determinado punto y emergen en otro, pero el proceso intermedio no concierne al usuario.

TESIS CON
FALLA DE ORIGEN

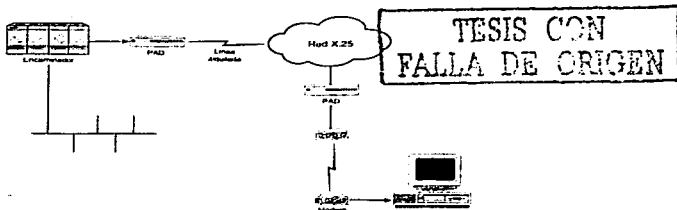


Figura 3-11 Ejemplo de una red X.25.

La interfaz entre los dispositivos y la red X.25 es un ensamblador-desensamblador de paquetes (PAD). El PAD puede estar ubicado junto con la computadora del cliente, comunicando con la red X.25 a través de una línea, o en el punto de recepción de llamadas al que los clientes pueden acceder utilizando un módem.

Las redes públicas X.25 están disponibles en muchos puntos y permiten construir una WAN económica para un nivel de tráfico moderado.

X.25 es una tecnología anticuada con muchos inconvenientes. Dado que X.25 no puede adaptarse para admitir las mejoras en velocidad y fiabilidad de los medios de las WAN modernas, ha sido necesario desarrollar una nueva norma de conmutación de paquetes que supere las limitaciones de X.25: Frame Relay.

Frame relay

Frame relay es una norma para redes de área extensa de conmutación de paquetes y banda ancha. Es una actualización de la norma X.25, y la ITU (CCITT) es el organismo encargado de su normalización. Según muestra la Figura 3-12, los servicios proporcionados por Frame relay corresponden a las capas de enlace de datos y física del modelo OSI. Su diseño partió de la base de que los canales de comunicación serían fiables. Por tanto, Frame relay no se encarga de la corrección de errores ni del control de flujo. Se limita a detectar errores, a descartar los marcos dañados y a notificar los errores a los protocolos de las capas superiores. Estos se encargan de corregir los errores solicitando la retransmisión de los marcos dañados. Al delegar la recuperación de errores en los protocolos de las capas superiores de los nodos terminales, los conmutadores

operan con mayor agilidad. Las redes X.25 realizan la detección y la recuperación de errores en cada conmutador.

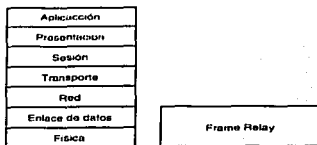


Figura 3-12 Relación de frame relay con el modelo de referencia OSI.

Frame relay puede funcionar sobre T1 o E1 y otras redes de alta velocidad desde 64 Kbps s. Es posible obtener servicios frame relay en una red pública, así como configurar redes privadas.

Frame relay ofrece ancho de banda personalizado y se adapta mejor a las necesidades de las LAN. El volumen de tráfico de los terminales es limitado, previsible y regular. El tráfico de las LAN puede variar espectacularmente entre periodos de poca actividad y otros mucho más activos derivados de actividades de elevado tráfico como las transferencias de archivos.

Los usuarios de una red pública Frame relay suelen adquirir un ancho de banda garantizado denominado tasa de información comprometida (CIR -Committed Information Rate). Ciertos servicios permiten que sus clientes excedan el CIR y aplican una tarifa. Los usuarios pueden adquirir servicios personalizados de Frame relay que se adapten a sus necesidades sin arriesgarse a quedar bloqueados en los momentos de mayor demanda.

La Figura 3-13 muestra una red frame relay. Las LAN están conectadas a la red mediante una interfaz Frame relay (FRI-Frame Relay Interface) generalmente incorporada a un encaminador.

El campo de datos de un marco frame relay se denomina payload. La implementación de la red define el tamaño del campo payload, por lo que las redes frame relay son configurables.

TESIS CON
FALLA DE

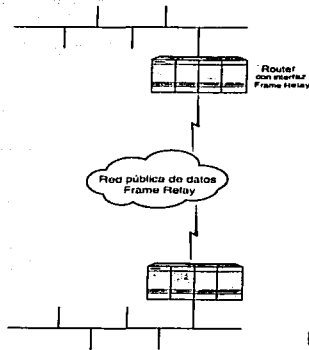


Figura 3-13 Una red Frame relay.

La tecnología Frame relay está orientada a conexiones y admite circuitos virtuales con mutados y circuitos virtuales permanentes (PVC). Un PVC establece una ruta fija en la red que permite una comunicación eficiente entre los dispositivos. Un PVC puede multiplexar un máximo de 1.024 conexiones lógicas. Se requiere un escaso nivel de proceso a medida que los marcos recorren la red, por tanto, Frame relay funciona a elevadas velocidades con poco retraso en la transmisión.

ATM

Se está produciendo un cambio en la naturaleza de los datos de las redes. Las tecnologías gráficas son cada vez más habituales y van asociadas a grandes archivos de datos de varios megabytes. La transferencia de datos gráficos puede sobrecargar una red, además, las nuevas aplicaciones utilizan cada vez más tecnologías que se consideraban punteras hace poco tiempo. Con frecuencia, las redes deben transportar vídeo y audio digitalizados que, además de consumir un considerable ancho de banda, requieren que los paquetes de datos lleguen sincronizados en tiempo real.

Tanto el vídeo como el audio pueden representarse en formato digital, pero los requisitos de este tipo de datos suelen exceder la capacidad habitual de las computadoras. La digitalización de

una señal de vídeo en movimiento puede requerir un ancho de banda mínimo de 6 Mbps aunque éste es tan solo uno de los problemas asociados con los datos de vídeo en una red. Las señales gráfica y de audio de una señal de vídeo constituyen dos corrientes de datos separadas que deben permanecer sincronizadas en tiempo real.

El modo de transferencia asíncrono (ATM -Asynchronous Transfer Mode) es una nueva tecnología que promete resolver estos problemas técnicos. ATM ofrece una flexibilidad sin precedentes y su diseño permite integrar datos, vídeo y voz en una red de alto rendimiento.

Varias organizaciones están involucradas en el proceso de normalización de ATM. Gran parte de la tecnología ATM proviene de la RDSI de banda ancha (B-ISDN), una extensión de la RDSI estándar desarrollada en 1988 por CCITT. Las normas de CCITT definen la arquitectura básica de B-ISDN pero omiten muchos aspectos de la implementación de ATM en las LAN.

El foro ATM es un consorcio industrial creado para dar soluciones a la interacción de ATM y las LAN. Este grupo ha desarrollado la arquitectura básica ATM LAN. El IETF está trabajando igualmente sobre la problemática de tráfico de las LAN sobre ATM.

Arquitectura de las LAN ATM

Las redes ATM constan de dos tipos de dispositivos: estaciones terminales y conmutadores (véase la Figura 3.14). El foro ATM ha establecido dos interfaces de red. La interfaz usuario-red (UNI -User-Network Interface) conecta una estación terminal a un conmutador. La interfaz red-red (NNI -Network-Network Interface) conecta un conmutador a otro.

Las LAN pueden comunicarse con una red ATM a través de un encaminador equipado con un interfaz ATM.



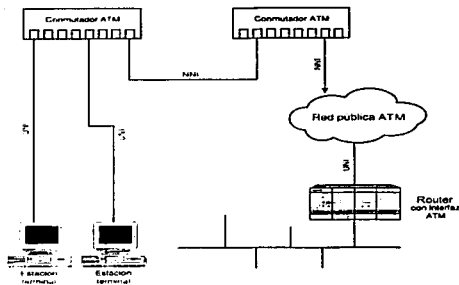


Figura 3-14 Una red ATM

Modos de transferencia: STM, PTM y ATM

El modo de transferencia sincrónico (STM -Synchronous Transfer Mode) utiliza multiplexión por división de tiempo asignando intervalos de tiempo a los canales de datos. El uso de intervalos fijos garantiza un ancho de banda dedicado y una transmisión sincrónica de los datos. Por ejemplo, es posible asegurar que la voz y la imagen permanezcan sincronizadas durante una transmisión de video. STM es el modo de transferencia más adecuado para datos de vídeo y voz.

El modo de transferencia de paquetes (PTM -Packet Transfer Mode) utiliza conmutación de paquetes para proporcionar servicios flexibles adecuados a la transmisión de datos. PTM se adapta a los paquetes de distintos formatos y tamaños y ofrece un ancho de banda flexible.

El modo de transferencia asincrónico (ATM -Asynchronous Transfer Mode) proporciona un método de transporte flexible que puede adaptarse a la voz, al vídeo y a los datos.

Al igual que X.25 y Frame relay, ATM dispone de un mecanismo para conmutar unidades de datos a través de las redes. A diferencia de estos protocolos de conmutación de paquetes, los cuales transmiten unidades de datos de tamaño variables, ATM opera con una unidad de datos de tamaño fijo denominada celda. Al estandarizar el tamaño de la unidad de datos, la eficiencia de los conmutadores aumenta significativamente.

ATM ofrece un servicio sincrónico de celda para satisfacer a las industrias de vídeo y de voz. De este modo ATM puede garantizar velocidades de transmisión sincronizando distintos canales

de datos. ATM puede proporcionar una velocidad de bits constante para compensar cualquier irregularidad que pueda producirse durante la transferencia de las celdas.

Las celdas ATM tienen una longitud de 53 bytes y constan de una cabecera de 5 bytes y un payload de 48 bytes (véase la Figura 3-15). A diferencia de otros protocolos descritos en este capítulo, una cabecera de 5 bytes ATM no puede contener dos direcciones de 48 bits. El reducido tamaño de esta cabecera es posible gracias a la estrategia utilizada para definir las rutas a través de las redes ATM.

ATM es una red orientada a conexiones. Los dispositivos que se comunican obtienen un circuito virtual definiendo la ruta seguida por las celdas a través de la red. Cualquier ruta entre dos dispositivos ATM queda definida por dos especificaciones. Un canal virtual (VC) específico se asigna al circuito virtual. Un canal virtual funciona sobre una ruta virtual (VP). Las rutas virtuales sólo son colecciones de canales virtuales.

Entre los dispositivos ATM se establecen una o más rutas virtuales. Un enlace T1 entre conmutadores ATM debería corresponder a una ruta virtual. La ruta es virtual debido a que no existe una ruta física dedicada a una conexión salvo cuando se transfiere una celda en la conexión. El resto del tiempo la ruta virtual está disponible para dar servicio a las celdas de otras conexiones. Cada ruta virtual puede dar servicio a muchos canales virtuales. Un circuito virtual ATM queda definido por un canal virtual específico que opera sobre una ruta virtual.

La ruta virtual de una celda entre dos conmutadores se representa por un identificador de ruta virtual (VPI -Virtual Path Identifier) de 8 bits situado en la cabecera de la celda ATM. Un identificador de canal virtual (VCI -Virtual Channel Identifier) de 16 bits codifica la información del canal virtual. La unión del VPI y del VCI identifican de manera única el circuito virtual asociado a una celda. ATM admite más de 16 millones de canales virtuales por conmutador utilizando un total de 24 bits, aunque la mayoría del hardware disponible no alcanza esa capacidad.

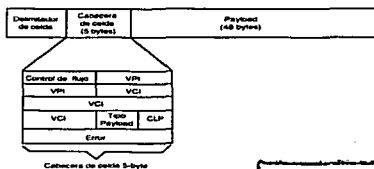


Figura 3-15 Formato de una celda ATM.

**TESIS CON
FALLA DE OMBEN**

Cada conmutador conserva la información de los VCI y de los VPI en una base de datos local de conexiones. Es posible que se seleccionen distintos valores VCI y VPI entre cada par de conmutadores de la ruta de la celda para una conexión. Los conmutadores consultan sus bases de datos para determinar el VPI y el VCI que deben utilizar en el siguiente paso. La Figura 3-16 ilustra el modo en que se utilizan los VPI y los VCI para encaminar las celdas a través de una red.

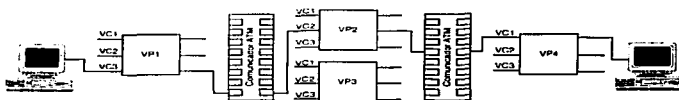


Figura 3-16 Conmutadores ATM y circuitos virtuales.

Protocolos ATM

El CCITT ha definido un modelo de tres niveles para B-ISDN. El modelo corresponde a las tres capas inferiores del modelo OSI. Los protocolos inferiores a la capa de red realizan toda la conmutación (el equivalente ATM del encaminamiento) para mejorar el rendimiento.

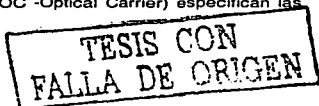
La capa de adaptación ATM (AAL -ATM Adaptación Layer) proporciona una interfaz para los protocolos de las capas superiores y lleva a cabo la fragmentación y el reensamblaje de los mensajes. Se utiliza la encapsulación LLC IEEE 802.2 cuando es necesario dar soporte a varios protocolos en el mismo VC. La AAL proporciona varios servicios que incluyen la conexión, la desconexión y la velocidad de bits constante y variable.

La capa ATM define los formatos y el comportamiento de las celdas. Admite canales virtuales permanentes (PVC) y canales virtuales conmutados (SVC).

La capa física ATM define el modo en que se transportan las celdas por la red y la señalización de varios tipos de medios. Sin embargo, no especifica la velocidad de los datos. ATM puede adaptarse a la práctica totalidad de velocidades y medios.

Medios ATM

ATM puede operar sobre una amplia variedad de medios cuyo único límite es el transporte físico. Una opción frecuente es la red óptica síncrona (SONET -Synchronous Optical Network) Desarrollada por BellCore. Los niveles de transporte óptico (OC -Optical Carrier) especifican las



velocidades de datos que están comprendidas entre OC-1 (52 Mbps) y OC-48 (2,5 Gbps). Las implementaciones actuales de SONET ofrecen un servicio OC-9 de 466 Mbps.

El foro ATM ha definido cuatro tipos de interfaces:

- Interfaz WAN DS3 de 45 Mbps
- SONET OC-3 de 155 Mbps.
- Modo múltiple de fibra óptica de 155 Mbps basado en Fiber Channel
- Modo múltiple de fibra óptica de 100 Mbps basado en FDDI

Una de las características más importantes de ATM es su capacidad para incorporar distintas velocidades de transmisión en una red extensa. Las conexiones ATM de 25 Mbps podrían pasar a 100 Mbps en una red principal ATM que a su vez se conectaría a una red pública de datos de 455 Mbps. Entre las tecnologías disponibles, ATM es la única que ofrece un nivel de flexibilidad suficiente para proporcionar ancho de banda según las necesidades de cada entorno.

Una tecnología emergente

Los expertos en redes piensan que ATM es la tecnología con mayores posibilidades de éxito, cifra considerablemente superior a la de las tecnologías competidoras como Ethernet de 100 Mbps. Lógicamente, el precio de ATM descenderá a medida que madure la tecnología y puede llegar el momento en que el factor económico pierda peso frente a las ventajas tecnológicas de ATM.

Un posible inconveniente reside en que ATM es una red orientada a conexiones que requiere una conexión entre cada par de nodos. Este tipo de redes no admiten directamente las transmisiones de difusión que TCP/IP y otros protocolos utilizan ampliamente. La industria ATM ha desarrollado una emulación LAN para superar este problema. Evita que TCP/IP deba modificarse para funcionar sin mensajes de difusión dotando a ATM de la apariencia de una LAN convencional como Ethernet o token ring. El costo de este método consiste en una pérdida significativa de ancho de banda consumido por el proceso de emulación LAN. Sin embargo, puede ayudar a acercar las ventajas de ATM a los entornos LAN existentes.

Por el momento, ATM es una tecnología emergente. Existen varios problemas sin solución relacionados con las LAN y todavía quedan por desarrollar varias normas. ATM es una tecnología para las organizaciones que necesitan de sus características únicas. Es probable que coexista con las tecnologías LAN y WAN actuales durante un largo período de tiempo.

Capítulo IV Tecnología de la conmutación (Switching)

En los anteriores capítulos se han presentado las tecnologías que existen para mantener y ampliar las redes LAN. Llegado a este punto estamos preparados para analizar y configurar un dispositivo comercial que da origen al este trabajo (**Configuración de un Switch Cisco 1900**) que, como sabemos, es un dispositivo que se utiliza para preservar el ancho de banda en una red aplicando una estrategia de segmentación.

En éste capítulo se introducen los conceptos de la tecnología de conmutación (Switching). Al finalizar esta revisión detallada, conoceremos la teoría necesaria para configurar el Switch.

Dominios de colisión y difusión

Como se mencionó anteriormente, todos los dispositivos de un segmento de red Ethernet están conectados a un mismo medio físico y las señales enviadas a través del cable son recibidas por todos ellos. Esto significa, además, que si dos dispositivos envían una señal al mismo tiempo se producirá una colisión entre ambas. La estructura de Ethernet, por lo tanto, dispone de reglas que permiten que solo un dispositivo tenga acceso al medio en un momento dado. También existe el método para detectar y corregir los errores conocidos como colisiones (cuando dos o más nodos tratan de transmitir al mismo tiempo).

Recordando, esta tecnología Ethernet se conoce como acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD). En la práctica, esto significa que varios nodos pueden tener acceso al medio y que, para que un nodo pueda acceder al medio, deberá "escuchar" (detectar la portadora) para asegurarse de que ningún otro nodo este utilizando el mismo medio. Si el medio se encuentra en uso, el nodo procederá a mantener en suspenso el envío de datos. En caso de que haya dos nodos que no detectan ningún otro tráfico, ambos tratarán de transmitir al mismo tiempo dando como resultado una colisión.

Cuando se trata de redes locales, es fundamental definir dos conceptos de suma importancia que nos ayudarán a comprender la estructura básica de los patrones de tráfico y nos facilitarán la definición de las necesidades relativas tales como el Switch:

- **Dominio de colisión.** Grupo de dispositivos conectados al mismo medio físico, de tal manera que si dos dispositivos acceden al medio al mismo tiempo, el resultado sea una colisión entre las dos señales.
- **Dominio de difusión.** Grupo de dispositivos de la red que envían y reciben mensajes de difusión entre ellos.

Nota: Los mensajes de difusión se generan cuando un dispositivo no funciona en forma adecuada por lo que la red difunde mensajes tratando de localizar los destinos. La difusión de éstos crea un problema que se denomina tormentas de difusión.

La mayoría de los segmentos de red que existen hoy en día son dispositivos conectados por medio de *hubs*. Los *hubs* permiten la concentración de muchos dispositivos Ethernet en un dispositivo centralizado, que conecta todos los dispositivos en una misma estructura de concentrador físico. Esto significa que todos los dispositivos conectados al hub comparten el mismo medio, y en consecuencia, comparten los mismos dominios de colisión, dominio de difusión y ancho de banda. La figura 4-1 muestra una conexión típica de hub.

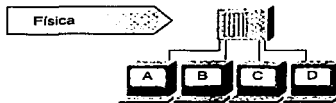


Figura 4-1 Hub Ethernet

El hub no manipula ni visualiza el tráfico del bus; se utiliza solo para extender el medio físico repletando la señal que recibe de un puerto a todos los demás puertos. Esto significa que un hub es un dispositivo de la capa física. Esta restringido exclusivamente a la propagación de señales físicas, sin ninguna función propia de capas superiores.

Debido a que todos los dispositivos están conectados al mismo medio físico, un hub es un dominio de colisión individual. Si un dispositivo envía una difusión, el hub lo propaga a todos los demás nodos, de manera que también se convierte en un dominio de difusión individual.

Veamos ahora La figura 4-2. Puede verse que los dos vehículos tratan de ocupar la misma carretera al mismo tiempo, llegando a la colisión. En una red la colisión resultante provoca algún tipo de daño. De hecho, las tramas dañadas se convierten en tramas de error, las cuales son detectadas por los nodos como una colisión, lo que obliga a ambas estaciones a volver a transmitir

TESIS CON FALLA DE ORIGEN

sus respectivas tramas. Existe un algoritmo de repetición que determina cuándo los host deben volver a transmitir, con el fin de minimizar la posibilidad de que tenga lugar otra colisión. Cuantas más host o estaciones haya en un segmento de Ethernet, mayor es la probabilidad de que tenga lugar una colisión. Estas colisiones excesivas son la razón principal por la cual las redes se segmentan en dominios de colisión más pequeños, mediante el uso de Switches.

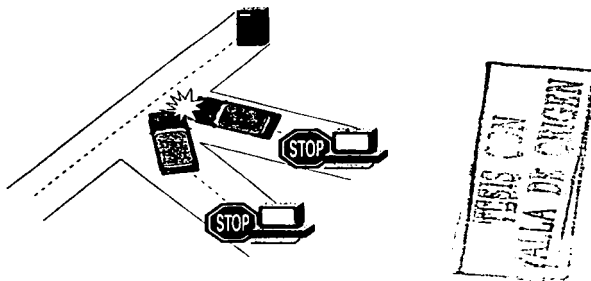
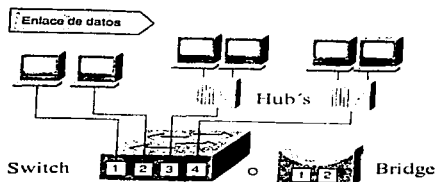


Figura 4-2 Colisiones en Ethernet

Dispositivos de la capa de enlace

Los bridges y switches de la Capa 2 son dispositivos que funcionan en la capa de enlace de datos de la pila del protocolo. La Figura 4-3 muestra los dispositivos que se encuentran habitualmente en la Capa 2. La conmutación o switcheo se basa en el puentado por hardware. En un switch, el reenvío de tramas se controla por medio de un hardware especial llamado *circuits integrados específicos de aplicaciones* (ASIC). La tecnología ASIC permite que un chip de silicio pueda ser programado para realizar una función específica durante el proceso de fabricación del mismo. Esta tecnología permite que las funciones puedan llevarse a cabo a una velocidad mucho mayor que si el chip estuviera programado por software. Debido a la tecnología ASIC, los switches proporcionan escalabilidad a velocidades de gigabits con una latencia baja.



TESIS CON
 FALLA DE ORIGEN

Figura 4-3 Dispositivos de la capa de enlace

Cuando un switch recibe una trama, utiliza la información del enlace de datos para procesar dicha trama. En un entorno de switches transparente, el switch procesa la trama determinando si ésta necesita ser copiada en otros segmentos conectados. Un switch transparente detecta todas las tramas que cruzan un segmento y visualiza cada trama y el campo de dirección de origen para determinar en qué segmento reside el nodo de origen. El switch transparente guarda esta información en memoria en lo que se conoce como **tabla de envío**. La tabla de envío contiene un listado de todos los nodos finales (desde los cuales el switch puede detectar una trama en un periodo de tiempo determinado y el segmento en que reside. Cuando un switch detecta una trama en la red, examina la dirección de destino y la compara con la tabla de envío para determinar si ha de filtrar, inundar o copiar la trama en otro segmento.

Este proceso de decisión tiene lugar como se indica a continuación:

- Si el dispositivo de destino está en el mismo segmento que la trama, el switch bloquea el paso de la trama a otro segmento. Este proceso se conoce como **filtrado**.
- Si el dispositivo de destino se encuentra en un segmento diferente, el switch envía la trama al segmento apropiado.
- Si la dirección de destino es desconocida para el switch, éste envía la trama a todos los segmentos excepto aquel de donde se ha recibido la información. Este proceso se denomina **inundación**.

Debido a que el switch aprende todos los nodos finales a partir de las direcciones de origen, nunca aprenderá la dirección de difusión. Por lo tanto, todas las difusiones serán inundadas a todos los segmentos del switch. En consecuencia, todos los segmentos de un entorno basado en switches se consideran residentes en el mismo dominio de difusión.

Una red puenteada/conmutada proporciona una excelente administración del tráfico. La finalidad del dispositivo de Capa 2 es reducir las colisiones, que no hacen sino desperdiciar ancho de banda y evitar que los paquetes lleguen a su destino. La parte A de la Figura 4-4 muestra cómo un switch es capaz de reducir las colisiones al asignar a cada segmento su propio dominio de colisión. La parte B de la Figura 4-4 muestra que cuando hay dos o más paquetes que necesitan entrar en un segmento, quedan almacenados en memoria hasta que el segmento esté disponible.

Las redes puenteadas/conmutadas poseen las siguientes características:

- Cada segmento posee su propio dominio de colisión.
- Todos los dispositivos conectados al mismo switch forman parte del mismo dominio de difusión.

Tecnología de conmutación.

Para poder configurar un switch de modo que pueda operar correctamente en un entorno de red, es necesario comprender antes cómo funciona. Los switches operan en la capa 2 del modelo OSI, segmentan la red en diferentes dominios de colisión. Los switches de la capa 2 poseen tres funciones principales :

- **Aprender direcciones.** Un switch aprende las direcciones MAC de los dispositivos asociados a cada uno de los puertos. Las asignaciones de direcciones a puertos se guardan en una base de datos MAC.
- **Reenviar/filtrar paquetes.** Cuando un switch ethernet recibe una trama, consulta la base de datos MAC para determinar que puerto puede alcanzar el nodo identificado como destino. Si se localiza la dirección, la trama será retransmitida.
- **Evitar bucles.** Cuando la red incluye bucles de redundancia, un switch Ethernet evita que estos bucles entren en la red, pero sin impedir vías de regreso en el caso de que se haya configurado un árbol de extensión.

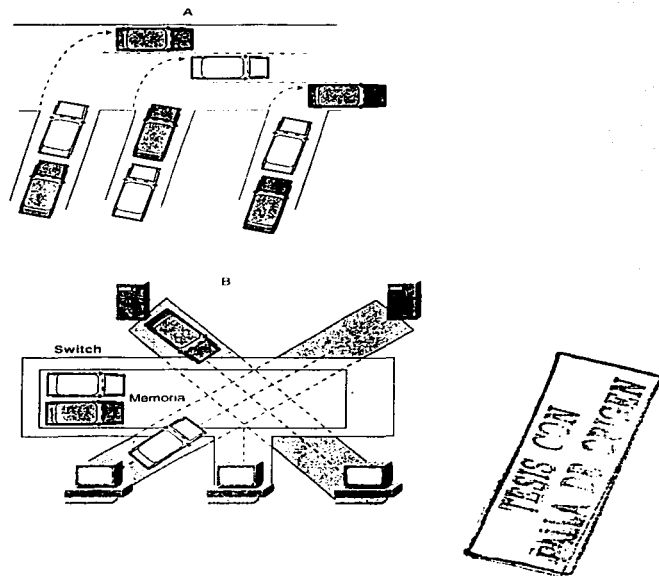


Figura 4-4 El switcheo reduce las colisiones

Aprendizaje de direcciones

Un switch Ethernet aprende direcciones y mantiene una tabla de direcciones MAC que se usa para registrar las ubicaciones de los dispositivos conectados al switch. A partir de aquí, utiliza dicha tabla para decidir que paquetes deben ser reenviados a otros segmentos. La figura 4-5 muestra una tabla de direcciones MAC inicial. Hay que tener en cuenta que, durante la inicialización, el switch no conoce la interfaz donde reside el host.

El objetivo del switch es segmentar el tráfico de manera que los paquetes destinados a un host en un dominio de colisión determinado no se propaguen a otro segmento. El switch consigue

esto "aprendiendo" las ubicaciones de los host. A continuación se esquematiza el proceso de aprendizaje y retransmisión:

- Cuando se inicia el switch, la tabla de direcciones MAC del mismo esta vacía, como ilustra la figura 4.5.



Figura 4-5 Aprendizaje de direcciones: tabla de direcciones MAC inicial

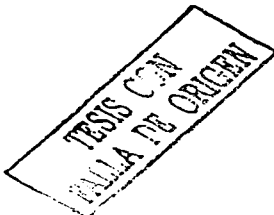
- Con una tabla de direcciones MAC vacía, no es posible tomar decisiones relativas al filtrado o retransmisión basándose en direcciones, por lo que el switch debe retransmitir cada trama a todos los nodos conectados, excepto a aquel de donde se ha recibido la trama.
- Enviar una trama a todos los nodos conectados se denomina **inundar la trama**.
- Inundar es el medio menos efectivo de transmitir datos a través de un switch, pues se malgasta el ancho de banda al enviar la trama a segmentos donde no se necesita.
- Debido a que los switches controlan el tráfico para múltiples segmentos al mismo tiempo, han de implementar memoria buffer para que puedan recibir y transmitir tramas independientemente en cada nodo o segmento.

Para comprender el proceso de aprendizaje, veamos en la figura 4-6, que ilustra una transacción entre dos nodos que se encuentran en segmentos distintos.

En la figura 4-6, el nodo A con dirección MAC 0260.8C01.1111 desea enviar tráfico al nodo C con dirección MAC 0260.8C01.2222. El switch recibe esta trama y lleva a cabo varias acciones:

Paso 1 La trama se recibe inicialmente a través del ethernet físico y se almacena en un espacio de memoria temporal.

Paso 2 Debido a que el switch no conoce aun que interfaz esta conectada al host de destino, se ve obligado a inundar la trama a través de todos los puertos.



Paso 3 Mientras se inunda la trama del nodo A, el switch aprende la dirección de origen y la asocia al puerto E0 en una nueva entrada de direcciones MAC.

Paso 4 Una entrada de la tabla pasa a memoria caché. Si dicha entrada no es actualizada por una nueva trama en un periodo de tiempo determinado, la entrada es descartada.

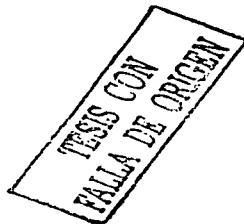
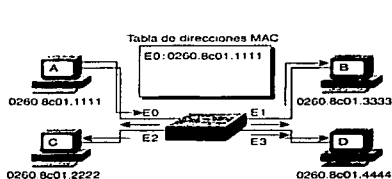


Figura 4-6 Aprendizaje de direcciones: paquete inundado

Los switches resultan eficientes precisamente por su capacidad de aprendizaje, como queda ilustrado en la figura 4-7.

En la figura 4-7, el nodo D con dirección MAC 0260.8c01.4444 envía tráfico al nodo C, con dirección MAC 0260.8c01.2222. El switch realiza aquí varias acciones:

Paso 1 La dirección de origen, 0260.8c01.4444, se añade a la tabla de direcciones MAC.

Paso 2 La dirección de destino incluida en la trama transmitida, nodo C, se compara con las entradas de la tabla de direcciones MAC.

Paso 3 Cuando el software determina que no existe aun asignación de nodo a dirección MAC para este destino, la trama es inundada a todos los nodos excepto aquel a través el cual ha sido recibida.

Paso 4 Cuando el nodo C envía de vuelta una trama al nodo A, el switch puede también aprender la dirección MAC de nodo C, en el puerto E2.

Paso 5 Cuando todos los nodos envían tramas dentro del periodo de vigencia de la tabla de direcciones MAC, se ira construyendo una tabla de direcciones MAC completa. Estas entradas se usaran posteriormente para tomar decisiones inteligentes de retransmisión y filtrado.

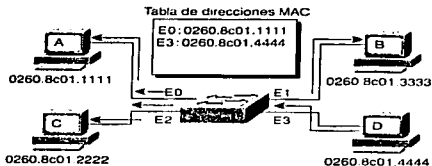


Figura 4-7 Aprendizaje de direcciones: respuesta del nodo

Decisiones de retransmisión y filtrado

Cuando una trama llega a una dirección de destino conocida, es transmitida solo al puerto específico conectada a dicho nodo, y no a los demás nodos.

En la figura 4-8 el nodo A envía una trama al nodo C. Cuando la dirección MAC de destino (dirección MAC del host C) se encuentra en la tabla de direcciones MAC, el switch retransmite la trama solo al puerto registrado.

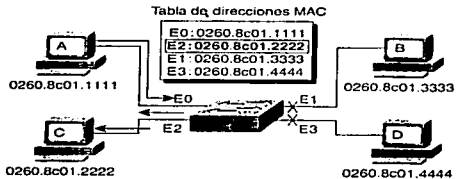


Figura 4-8 Decisión del filtrado del switch

La secuencia de acciones para cuando el host A envía una trama al host C es la siguiente:

Paso 1 La dirección MAC de destino incluida en la trama transmitida, 0260.8C01.2222, se compara con las entradas existentes en la tabla de direcciones MAC.

Paso 2 Cuando el switch determina que la dirección MAC puede ser alcanzada por el puerto E2, retransmite la trama sólo a este puerto.

TEST CON
 FALLA DE ORIGEN

Paso 3 El switch no retransmite la trama al puerto E1 ni al puerto E3, a fin de preservar el ancho de banda para estos enlaces. Esta acción se conoce como filtrado de tramas.

Si el puerto D de la figura 4-9 envía una trama de difusión, la trama es retransmitida a todos los puertos excepto al puerto que la ha originado.

El hecho de que todos los puertos reciban una trama de difusión significa que todos los segmentos de la red conmutada se encuentran en el mismo dominio de difusión.

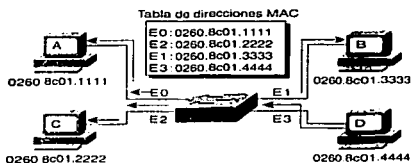


Figura 4-9 Trama de difusión

Evitar de bucles

La tercera función del switch es evitar los bucles. Las redes puentesadas, que incluyen las redes conmutadas, están diseñadas por lo general con enlaces y dispositivos redundantes. Estos diseños eliminan la posibilidad de que un punto de fallo dé como resultado la pérdida de funcionalidad en toda la red conmutada. La figura 4-10 ilustra una red conmutada diseñada con redundancia entre el segmento 1 y el segmento 2.

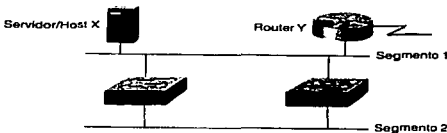


Figura 4-10 Topología redundante para una red conmutada

TESIS CON FALLA DE ORIGEN

Aunque los diseños conmutados redundantes permiten eliminar un punto de fallo individual, originan al mismo tiempo varios problemas que deben ser tenidos en cuenta:

- Sin algún servicio para evitar los bucles, cada switch inundaría las difusiones en un bucle infinito. Esta situación se conoce habitualmente como *bucle de puente*. La propagación continua de estas difusiones a través del bucle produce una tormenta de difusión, lo que da como resultado un desperdicio del ancho de banda, así como impactos serios en el rendimiento de la red.
- Podrían ser distribuidas múltiples copias de tramas sin difusión a los host de destino. Muchos protocolos esperan recibir una sola copia de cada transmisión. La presencia de múltiples copias de la misma trama podría ser causa de errores irrecuperables.
- Una inestabilidad en el contenido de la tabla de direcciones MAC da como resultado que se reciban varias copias de una misma trama en diferentes puertos del switch. La retransmisión de datos podría quedar interrumpida cuando el switch consume recursos al copiar direcciones MAC.

A continuación se describen cómo se pueden resolver todos estos problemas

Eliminación de tormentas de difusión

Los switches inundan tramas de difusión a todos los puertos excepto aquel de donde se ha recibido la trama. La figura 4-11 ilustra el problema de las tormentas de difusión, en que los switches propagan el tráfico de difusión de forma continua.

Una tormenta de difusión es una situación de extrema congestión debido a demasiadas difusiones en la red. Esto puede ser causado por un mal comportamiento de la tarjeta NIC, un diseño incorrecto de la red, o un bucle de puenteado/commutación. La tormenta de difusión ilustrada en la figura 4-11 esta causada por la siguiente secuencia de eventos:

Paso 1 Cuando el host X envía una trama de difusión (por ejemplo, un ARP para resolver su gateway predeterminada en el router Y) la trama es recibida por el switch A.

Paso 2 El switch A examina el campo que contiene la dirección de destino en la trama y determina que ésta debe ser inundada en el enlace Ethernet inferior, Segmento 2.

TESIS CON
FALLA DE ORIGEN

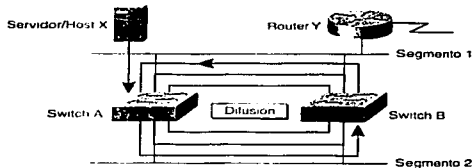


Figura 4-11 Tormentas de difusión

Paso 3 Cuando esta trama de la copia llega al switch B, el proceso se repite y se transmite una copia de la trama al Ethernet superior, Segmento 1.

Paso 4 Debido a que la copia original de la trama llega al switch B en el Segmento 1 en algún momento posterior a su recepción por el switch A, podría haber sido retransmitido por el switch B al segmento 2. En consecuencia, estas tramas viajarían alrededor de un bucle en ambas direcciones aunque el puerto de destino haya recibido ya una copia de la trama.

Una solución que evite los bucles eliminaría este problema impidiendo que una de las cuatro interfaces transmitiera o recibiera tramas durante operaciones normales. En la sección "Como funciona un Árbol de extensión" veremos cómo lleva a cabo esta tarea un Árbol de extensión.

Eliminación de transmisiones de tramas sin difusión duplicadas

La mayoría de los protocolos no están diseñados para reconocer ni hacer frente a transmisiones duplicadas. En general, los protocolos que utilizan un mecanismo de secuencia de numeración, suponen que hay muchas transmisiones que han fallado y que la secuencia de números ha sido reciclada. Hay otros protocolos que intentan gestionar las transmisiones duplicadas pasándolas al protocolo superior apropiado (lo que puede dar lugar a resultados impredecibles). La figura 4-12 ilustra como pueden tener múltiples transmisiones en una red conmutada.

TSIS CON
FALLA DE ENGEN

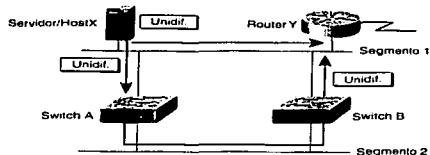


Figura 4-12 Múltiples copias de tramas

A continuación se explica cómo pueden tener lugar las transmisiones múltiples:

Paso 1 Cuando el Host X envía una trama de unidifusión al Router Y, se recibe una copia a través de la conexión Ethernet directa, Segmento 1. Mas o menos al mismo tiempo, el switch A recibe una copia y la coloca en sus búffers .

Paso 2 Si el Switch A examina el campo que contiene la dirección de destino en la trama y no encuentra una entrada en la tabla de direcciones MAC para el Router Y, el Switch inunda la trama en todos los puertos excepto en el que la originó.

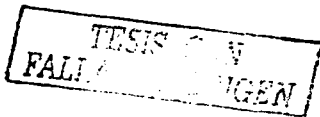
Paso 3 Cuando el Switch B recibe una copia de la trama a través del Switch A en el Segmento 2, el Switch B retransmite también una copia de la trama al Segmento 1 si no hay ninguna entrada en la tabla de direcciones MAC para el Router Y.

Paso 4 El router Y vuelve a recibir una copia de la misma trama.

Una solución que pase por la evitación de bucles eliminaría este problema impidiendo que alguna de las cuatro interfaces transmitiría o recibiera tramas durante su operación normal. Ésta es otra de las finalidades del protocolo Árbol de extensión.

Eliminación de la inestabilidad de la base de datos

La inestabilidad de la base de datos tiene lugar cuando llegan varias copias de una trama desde diferentes puertos de un switch. En la figura 4-13, el Switch B asigna el puerto de Segmento 1 al host X cuando llega la primera trama. Un poco después, cuando llega la copia de la trama transmitida a través del Switch A, el Switch B debe eliminar la primera entrada y asignar una dirección MAC del Host X al puerto del Segmento 2.



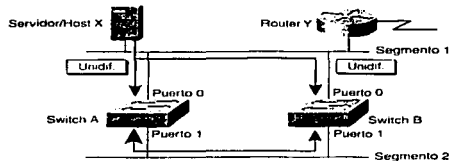


Figura 4-13 La inestabilidad de la base de datos tiene lugar cuando se reciben varias tramas en diferentes puertos del switch

En la figura 4-13, la ruta redundante sin la presencia de un Árbol de extensión crearía inestabilidad en la base de datos MAC. Esto ocurre cuando tienen lugar los siguiente eventos:

- Paso 1 El Host X envía una trama unidifusión al Router Y.
- Paso 2 La dirección MAC del Router Y aún no ha sido aprendida por ningún Switch.
- Paso 3 Los Switches A y B aprenden la dirección MAC del Host X en el puerto 0.
- Paso 4 La trama es inundada en el Router Y.
- Paso 5 Los Switches A y B aprenden incorrectamente la dirección MAC del Host X como puerto 1.

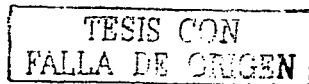
Dependiendo de la arquitectura interna del switch en cuestión, podría o no responder adecuadamente a rápidos cambios en su base de datos MAC.

También en este caso, una solución que evite los bucles eliminaría el problema impidiendo que alguna de las cuatro interfaces transmitiera o recibiera tramas durante su operación normal. Prevenir la inestabilidad de la base de datos es otra de las funciones del protocolo Árbol de extensión.

Bucles múltiples en una red conmutada

Una red amplia con una estructura compleja de switches podría dar lugar a la aparición de múltiples bucles en la red conmutada. Como se ilustra en la Figura 4.14, se puede caer en uno de los siguientes escenarios:

- Puede existir un bucle dentro de otro bucle.



- Una tormenta de difusión de paquetes en bucle podría atascar rápidamente la red con tráfico innecesario y evitar la conmutación de paquetes.

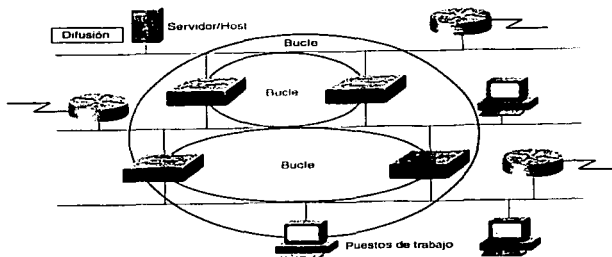


Figura 4.14 Múltiples bucles

Los protocolos de la capa 2, como Ethernet, carecen de un mecanismo capaz de reconocer y eliminar los paquetes en bucles no deseados. Algunos protocolos de la Capa 3, como IP, implementan un mecanismo denominado Tiempo de existencia (TTL), que limita el número de veces que un paquete puede ser retransmitido por los dispositivos de red. En ausencia de un mecanismo de este tipo, los dispositivos de la capa 2 continuarían retransmitiendo tráfico en un bucle infinito.

En consecuencia, debe existir un mecanismo para prevenir los bucles en las redes puenteadas (conmutadas). Este mecanismo para evitar los bucles es la razón principal de la existencia del protocolo Árbol de extensión.

Cómo funciona el Árbol de extensión

El protocolo Árbol de extensión es un protocolo desarrollado por DEC. El algoritmo Árbol de extensión de DEC fue revisado posteriormente por el organismo IEEE 802 y publicado en la especificación IEEE 802.1d. Los algoritmos DEC y el de IEEE 802.1d no son los mismos, pero sí son compatibles. Los switches Catalyst 1900 utilizan el protocolo árbol de extensión IEEE 802.1d.

El objetivo del protocolo árbol de extensión es mantener una red libre de bucles. Un camino libre de bucles se consigue cuando un dispositivo es capaz de reconocer un bucle en la topología y

TESIS CON
FALLA DE ORIGEN

bloquear uno o más puertos redundantes. Como ilustra la figura 4-15, tan solo hay un trayecto activo desde el Segmento 1 al segmento 2.

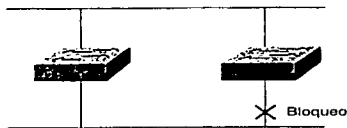


Figura 4-15 Bloqueo de puertos

El protocolo Árbol de extensión explora constantemente la red, de forma que cualquier fallo o adición en un enlace es detectado al instante. Cuando cambia la topología de red, el algoritmo árbol de extensión reconfigura los puertos del switch para evitar una pérdida total de la conectividad o la creación de nuevos bucles.

La figura 4-16 ilustra una red libre de bucles creada por el Árbol de extensión.

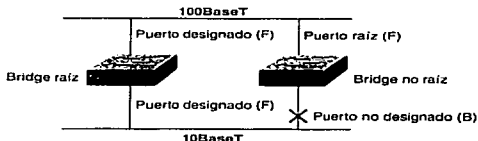


Figura 4-16 Operación del algoritmo Árbol de extensión

El protocolo Árbol de extensión proporciona una topología de red libre de bucles llevando a cabo las siguientes operaciones:

- **Se elige un bridge raíz.** En un dominio de difusión sólo puede existir un bridge raíz. Todos los puertos del bridge raíz se encuentran en un estado de retransmisión y se denominan puertos designados. Cuando está en este estado, un puerto puede enviar o recibir tráfico. En el ejemplo de la Figura 4.16, el Switch X ha sido elegido como bridge raíz.
- **Para cada bridge no raíz, hay un puerto raíz.** El puerto raíz corresponde a la ruta de menor costo desde el bridge no raíz hasta el bridge raíz. Los puertos raíz se encuentran en estado de retransmisión y proporcionan conectividad hacia atrás al bridge raíz. El costo

de la ruta del Árbol de extensión es un costo acumulado cuyo valor se basa en el ancho de banda. En el ejemplo de la Figura 4-16, la ruta de menor coste desde el Switch Y hasta el bridge raíz tiene lugar a través del enlace 100BaseT Fast Ethernet. En caso de igualdad de costos, el factor decisivo sería el número de puertos más bajo.

- **En cada segmento hay un solo puerto designado.** El puerto designado se selecciona en el bridge que posee el trayecto de menor costo hasta el bridge raíz. Los puertos designados se encuentran en estado de retransmisión y son responsables del reenvío del tráfico por el segmento. En la Figura 4.14, los puertos designados para ambos segmentos están en el bridge raíz, debido a que dicho bridge esta conectado directamente a ambos segmentos. El puerto 10BaseT Ethernet del Switch Y no es un puerto designado porque solo puede haber un puerto designado por segmento. Los puertos no designados se encuentran normalmente en estado de bloqueo con el fin de romper la topología de bucle. Cuando un puerto esta en estado de bloqueo, no retransmite trafico. Esto no significa que el puerto este inhabilitado. Significa que el Árbol de extensión esta impidiendo que este reenvié tráfico.

ID de bridge y estados de puerto

Los switches que ejecutan el algoritmo Árbol de extensión intercambian mensajes de configuración con otros switches a intervalos regulares usando una trama de multidifusión denominada Bridge Protocol Data Unit (BPDU). Por omisión, la BPDU se envía cada dos segundos. Uno de los elementos de información incluidos en la BPDU es el ID de bridge.

El Árbol de extensión llama a cada switch para asignarle un identificador único (ID de bridge). Normalmente, el ID de bridge está compuesto por una prioridad (2bytes) más la dirección MAC del bridge (6bytes). La prioridad predeterminada (IEEE 802.1d) es 32768, es decir, el valor correspondiente a la mitad del rango. El bridge raíz es el que tiene ID de bridge más bajo.

En la Figura 4-17, debido a que ambos switches están usando la misma prioridad predeterminada, el que tiene la dirección MAC más baja es el bridge raíz. Así, en este ejemplo, el switch X es el bridge raíz, con un ID de bridge de 8000.0C00.1111. El valor hexadecimal 8000 es la prioridad del bridge (32768 en decimal). El valor 0C00.1111.1111 es la dirección MAC del dispositivo.

**TESIS CON
FALLA DE ORIGEN**

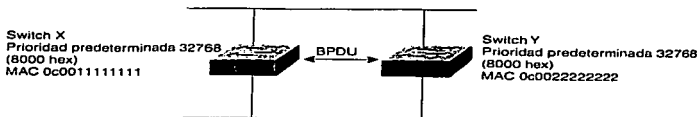


Figura 4-17 Comunicación de bridge

Una vez que la BDPDU ha sido intercambiada, los estados de los puertos de los switches serían los que se muestran en la Figura 4-18.

- Los puertos del Switch X, el bridge raíz, son puertos designados (retransmisores)
- El puerto Fast Ethernet del Switch Y es el puerto raíz (retransmisor) Éste posee una ruta de coste inferior hasta el bridge raíz que el puerto Ethernet.
- El puerto Ethernet del Switch Y es el puerto no designado (bloqueado). Sólo puede haber un puerto designado por segmento.

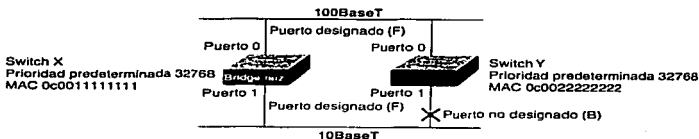


Figura 4-18 Estados de puerto en el Árbol de extensión

Costo de rutas en el árbol de extensión

El coste de una ruta en el Árbol de extensión es un coste acumulado basado en el ancho de banda de todos los enlaces de la ruta. La tabla 4.1 muestra algunos de los costos de ruta especificados en el estándar IEEE 802.1d.

TESIS CON
FALLA DE ORIGEN

| Velocidad del enlace | Costo (Especificación IEEE revisada) | Costo (Especificación IEEE previa) |
|----------------------|--------------------------------------|------------------------------------|
| 10 Gbps | 2 | 1 |
| 1 Gbps | 4 | 1 |
| 100 Mbps | 19 | 10 |
| 10 Mbps | 100 | 100 |

4.1. Coste de ruta en el Árbol de extensión

La especificación IEEE 802.1d fue objeto de revisión. En la nueva especificación se ha ajustado el cálculo para dar cabida a interfaces de velocidad superior, incluidas las de 1 y 10 Gbps.

Nota: La versión actual del software Catalyst 1900 utiliza la fórmula antigua para el cálculo del coste en el Árbol de extensión. Otros switches Catalyst. Como el 2900Xs, incorporan la fórmula revisada.

Veamos la Figura 4-19. Basándose en la red switchheada de esta figura, determinemos lo siguiente:

- ¿Cuál es el bridge raíz?
- ¿Cuáles son los puertos designados, no designados y raíz?
- ¿Cuáles son los puertos que retransmiten y cuáles están bloqueados?

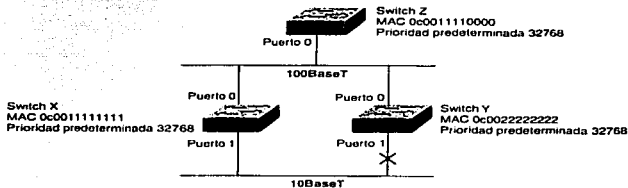


Figura 4-19 Ejemplo de Árbol de extensión

Usando el protocolo Árbol de extensión, podemos determinar lo siguiente para la red switchheada de la figura 4-19.

- **Bridge raíz.** El Switch Z, dado que posee el ID de bridge más bajo (prioridad y dirección MAC).
- **Puerto raíz.** Puertos 0 de los Switches X e Y, ya que están en la ruta hasta el raíz.
- **Puerto designado.** Puerto 0 del Switch Z. Todos los puertos del raíz son puertos no designados. El puerto 1 del Swtch X es un puerto designado. Dado que tanto el Swtch X como el Swtch Y poseen el mismo coste de ruta hasta el bridge raíz, el puerto designado ha sido elegido en el Switrch X, dado que posee un ID de bridge inferior que el Switch Y.
- **Bloqueado.** Puerto 1 del Switch Y. Se trata del puerto no designado dentro del segmento.
- **Retransmisión.** Todos los puertos designados y puertos raíz están en estado de retransmisión.

Estados de Árbol de extensión

Hay cuatro estados del Árbol de extensión:

- Bloqueo.
- Escucha.
- Aprendizaje
- Retransmisión.

El Árbol de extensión va cambiando de estado para mantener la topología libre de bucles.

Durante las operaciones normales, un puerto se encuentra en estado de retransmisión o de bloqueo. Los puertos de retransmisión proporcionan la ruta de costo mínimo hasta el bridge raíz. Cuando un dispositivo reconoce un cambio en la topología de la red, tienen lugar dos estados de transición. Durante un cambio en la topología, un puerto implementas temporalmente los estados de escucha y aprendizaje.

Todos los puertos se inician en el estado de bloqueo para evitar bucles. El puerto permanece en ese estado mientras el árbol de extensión determine que hay otra ruta bridge raíz que tiene asociado un menor costo. Los puertos bloqueados pueden seguir recibiendo BPDU.

Los puertos pasan del estado de bloqueo al estado de escucha. Cuando un puerto se encuentra en el estado de escucha, puede verificar si hay BPDU. Este estado se utiliza en realidad para indicar que el puerto esta a punto de quedar listo para transmitir, pero que le gustaría permanecer a la escucha algo más para garantizar que no se cree un bucle.

Cuando un puerto se haya en estado de aprendizaje, puede rellenar su tabla de direcciones MAC con direcciones escuchadas a través de sus puertos, pero no puede retransmitir tramas.

En el estado de retransmisión, el puerto puede enviar y recibir datos.

El tiempo que tarda normalmente un puerto en pasar normalmente en estado de bloqueo al estado de retransmisión es de 50 segundos. No obstante, es posible ajustar los temporizadores del Árbol de extensión para cambiar este valor predeterminado. Normalmente, los temporizadores deben fijarse es sus valores predeterminados. Los valores predeterminados han sido calculados para dar a la red el tiempo suficiente para recopilar toda la información correcta acerca de la topología de la misma. El tiempo que tarda un puerto en pasar del estado de escucha al estado de retransmisión, se denomina **retraso de retransmisión**. Los temporizadores del árbol de extensión son coherentes en el ámbito de la topología del bridge/switch y sus valores son establecidos por el bridge raíz. La tabla 4.2 muestra los valores predeterminados de los temporizadores del Árbol de extensión.

| Temporizador | Función primaria | Configuración predeterminada |
|------------------|--|------------------------------|
| Tiempo de saludo | Tiempo entre el envío de configuraciones BPDU por el bridge raíz | 2 segundos |
| Retraso de envío | Duración de los estados de escucha y aprendizaje | 30 segundos |
| Duración máxima | Tiempo de almacenamiento de la BPDU | 20 segundos |

Tabla 4.2. Temporizadores del Árbol de extensión

Recálculo de Árbol de extensión

Cuando se produce alguna modificación en la topología debida a un fallo en un bridge o en un enlace, el protocolo Árbol de extensión reajusta automáticamente la topología de la red para garantizar la conectividad, colocando puertos bloqueados en estado de retransmisión.

En el ejemplo que aparece ilustrado en la Figura 4-20, Si el Switch X (el bridge raíz) tuviera un fallo, el switch Y detectaría la BPDU ausente del bridge raíz. Uno de los temporizadores del Árbol de extensión se llama Duración Máxima. Cuando un temporizador de este tipo llega a su límite sin haberse recibido una nueva BPDU del entorno próximo, se reinicia un nuevo recálculo del

Árbol de extensión en su globalidad. El Puerto 1 pasaría sucesivamente al estado de escucha, después al de aprendizaje y, finalmente, al de retransmisión.

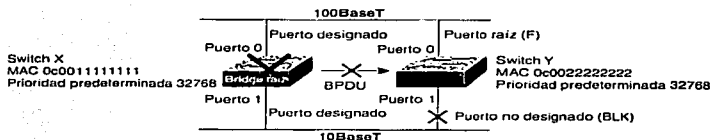


Figura 4-20 Recálculo del Árbol de extensión

Una vez recobrada la convergencia de la red, el Switch Y se convierte en el bridge raíz. Éste retransmite el tráfico entre los dos segmentos cuando sus puertos pasan al estado de retransmisión para convertirse en puertos designados.

Cómo permanecen informados de la topología los dispositivos

La convergencia es una necesidad para el normal funcionamiento de la red en un entorno puenteado/switchcado. Para una red puenteada o switchcada, el tema clave está en la cantidad de tiempo requerido para lograr la convergencia cuando cambia la topología de la red. La convergencia en el protocolo Árbol de extensión significa un estado donde los puertos de todos los switches y bridges pasan al estado de retransmisión o bloqueo.

Una capacidad de convergencia rápida es una característica muy deseable en la red, dado que reduce el periodo de tiempo que los switches tienen puertos en estado de transición, durante los cuales no envían tráfico. Aunque el término "rápido" no deja de ser ambiguo, lo que se quiere decir es que un cambio en la topología de una red puenteada/switchcada requiere un tiempo para reestablecer la conectividad completa. Es importante recordar esto cuando se diseñan redes puenteada/switchcadas.

Nota: Durante un cambio de topología, los dispositivos afectados no pueden comunicarse normalmente hasta que se alcance la convergencia del Árbol de extensión.

Cómo se transmiten las tramas

Para gestionar la conmutación de tramas se utilizan tres modos de operación primarios:

TESIS CON
FALLA DE ORIGEN

- **Guardar y retransmitir.** En el modo guardar y retransmitir, el switch debe recibir la trama completa para poder retransmitirla. Se leen las direcciones de origen y destino, se lleva a cabo la comprobación de redundancia cíclica (CRC), se aplican los filtros apropiados y se retransmite finalmente la trama. Si la CRC es incorrecta, la trama se descarta. La demora (o retraso) que tiene lugar en el switch depende de la longitud de la trama.
- **Modo de corte.** En el modo de corte, el switch verifica la dirección de destino (DA) en cuanto se recibe la cabecera y comienza de inmediato a enviar la trama. Dependiendo del protocolo de transporte de red utilizado (sin conexión u orientado a la conexión), existe una reducción significativa en el retardo entre el puerto de entrada y el de salida. El retardo en la conmutación basada en el modo de corte permanece constante con independencia del tamaño de la trama, debido a que en este modo, la retransmisión de la trama comienza en cuanto el switch lee la dirección de destino. (En algunos switches, sólo se lee la dirección de destino.) La desventaja de este modo es que el switch podría retransmitir una trama de colisión o una trama con un valor CRC incorrecto. Algunos switches continúan leyendo la CRC y guardan un registro de errores. Si la tasa de error es demasiado alta, el switch puede ser configurado (de forma automática o manual) para utilizar el modo de guardar y retransmitir.
- **Sin fragmentos.** En el modo sin fragmentos (conocido también como modo de corte modificado), el switch lee los primeros 64 bytes antes de retransmitir la trama. Normalmente, las colisiones tienen lugar en los primeros 64 bytes de una trama. Al leer esos 64 bytes, el switch puede filtrar las tramas que están libres de colisiones. La conmutación basada en el modo sin fragmentos es el modo operativo predeterminado del Catalyst 1900.

NOTA: La latencia se define como el retraso ocasionado por un dispositivo de red. Es importante mencionar que en los métodos de conmutación descritos aquí, la latencia se mide desde el primer bit que entra en el switch hasta el primer bit que sale del mismo. Esta medida ofrece una representación real del tiempo involucrado en conmutar un paquete. Sin embargo, cuando se leen valores de latencia para el modo de guardar y retransmitir, hay que tener en cuenta que dicho retraso se mide, por lo general, como el periodo que transcurre desde el último bit que entra hasta el primero que sale, debido a que, en este caso, no existe otra forma real de medir, a consecuencia de la variabilidad en los tamaños de las tramas. El tamaño de la trama no influye en los modos sin fragmentos o de corte, dado que siempre se trabaja con una cantidad fija de información.

Cómo dialoga el switch con otros dispositivos

Un switch de red proporciona conectividad entre los dispositivos de la red. Una de las principales razones para colocar switches en una red es mejorar la conectividad. Como dispositivo intermedio entre otros dispositivos, el switch cuenta con varios modos de comunicación entre él y los dispositivos de destino. Los modos, ilustrados en la Figura 4-21 usados para establecer comunicaciones entre el switch y el dispositivo de destino, son half-duplex y full-duplex. Estos son parámetros configurables que pueden afectar a la velocidad a la que un dispositivo puede enviar paquetes al switch para su retransmisión.

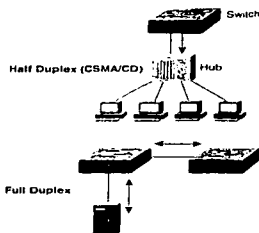


Figura 4-21 Visión general de la comunicación duplex

El modo de transmisión half-duplex implementa acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD). La LAN compartida tradicional opera en el modo half-duplex y es susceptible de colisiones de transmisión a través del cableado. Half-duplex es básicamente como un puente de un solo carril que cruza un río. Por el puente no pueden circular dos vehículos en direcciones opuestas al mismo tiempo. Ethernet Full-duplex mejora significativamente el rendimiento de la red sin el gasto de instalar un nuevo medio. La transmisión Full-duplex entre puestos se consigue usando conexiones Ethernet punto a punto y Fast Ethernet. Este esquema está exento de colisiones. Las tramas enviadas por dos nodos finales conectados no pueden colisionar, debido a que usan dos circuitos independientes de un cable de par trenzado. Es como un puente de dos carriles que cruza un río. Dicho de forma sencilla, significa que cada cable puede albergar el doble de la carga inicial, duplicando de forma efectiva el ancho de banda del medio. La conexión full-duplex consume un solo puerto.

Las conexiones de puertos Full-duplex pueden usar medios 10BaseT, 100BaseT y 100BaseFX para proporcionar enlaces punto a punto entre switches o nodos finales, pero no entre enlaces compartidos. Los nodos conectados directamente a un puerto de switch dedicado y con una tarjeta de red que soporte Full-duplex pueden ser conectados a puertos de switch configurados para operar en el modo Full-duplex. La mayoría de las tarjetas de red Ethernet y Fast Ethernet que se comercializan hoy día ofrece la posibilidad Full-duplex. En el modo Full-duplex, se desactiva el circuito de detección de colisiones.

Los nodos conectados a hubs, o los que comparten sus conexiones con un puerto de Switch, deben operar en el modo Half-duplex debido a que los puertos finales deben ser capaces de detectar colisiones. La eficiencia de la configuración Ethernet estándar se sitúa normalmente entre el 50 y el 60 por ciento del ancho de banda 10 Mbps. Ethernet full-duplex ofrece el 100 por ciento de eficiencia en ambas direcciones (se transmite a 10 Mbps y se recibe a 10 Mbps). En la Tabla 4.3 se resumen las diferencias entre las conexiones Full-duplex y Half-duplex.

| Half dúplex (CSMA/CD) | Full dúplex |
|-------------------------------|---|
| Flujo de datos unidireccional | Sólo punto a punto. |
| Mayor potencial de colisiones | Sin colisiones. |
| Conectividad a hub | <p data-bbox="519 645 907 683">Circuito de detección de colisiones desactivado.</p> <p data-bbox="519 708 871 724">Conectado a un puerto de switch dedicado.</p> <p data-bbox="519 750 832 802">Requiere soporte full-duplex en ambos extremos.</p> |

Tabla 4.3 Half-duplex comparado con full-duplex.


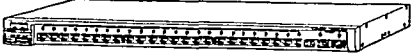
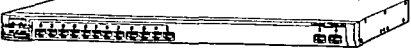


TESIS CON
FALLA DE ORIGEN

Capítulo V Configuración del Switch

Cisco Catalyst 1900

Interaces del switch.

Los switches Catalyst 1900 (mostrados en la figura 5-1) incrementan la funcionalidad en redes que utilizan estaciones de trabajo y servidores de altas prestaciones, aplicaciones que requieren un gran uso de ancho de banda, transferencia de grandes archivos de gráficos, audio y video y acceso a los mismos recursos de la red e Internet.

| Part Number | Description | |
|-----------------------------|--|---|
| WS-C1924-EN WS-C1924-A | 24 switched 10BaseT ports 1 switched AUI port (on rear panel) 2 switched 100BaseTX ports |  |
| WS-C1924C-EN WS-C1924C-A | 24 switched 10BaseT ports 1 switched AUI port (on rear panel) 1 switched 100BaseFX port 1 switched 100BaseTX port |  |
| WS-C1912-EN WS-C1912-A | 12 switched 10BaseT ports 1 switched AUI port (on rear panel) 2 switched 100BaseTX ports |  |
| WS-C1912C-EN WS-C1912C-A | 12 switched 10BaseT ports 1 switched AUI port (on rear panel) 1 switched 100BaseFX port 1 switched 100BaseTX port |  |
| WS-C1924F-A WS-C1924F-EN | 24 switched 10BaseT ports 1 switched AUI port (on rear panel) 2 switched 100-Mbps fiber ports |  |

Switches Catalyst 1900

En estos switches se dispone de hasta 25 puertos Ethernet 10BaseT (incluyendo el puerto AUI en la parte trasera), cada puerto suministra 10 Mbps de ancho de banda dedicados a los



usuarios o grupo de usuarios en la red. Estos puertos se conectan a otros dispositivos compatibles, ya sea una simple estación de trabajo o concentradores 10BaseT. Los switches cuentan también con dos puertos 100BaseT, que proporcionan las máximas prestaciones a servidores de alta velocidad y hacia grupo de switches y routers.

Cada switch está diseñado para operación plug and play, solamente requiere que se le asigne la información IP básica y conectarlo a otros dispositivos en la red. Si se requiere de necesidades específicas de la red, se puede también configurar a través de varias interfaces de administración.

En la figura 5-1 observamos el número de parte y la descripción de los diferentes modelos de la serie de switches Cisco Catalyst 1900. Los modelos que vienen con software estándar se indican con la letra "A" en el número de parte. Los modelos que vienen con el software "Enterprise edition" se indican con las letras "EN".

Descripción del panel frontal

El panel frontal de un switch catalyst nos proporciona 12 o 24 puertos de 10 Mbps y 2 de 100 Mbps (Figura 5-2) . También cuenta con un conjunto de LEDs y un botón de modo para monitorear el switch y sus puertos (Figura 5-4)

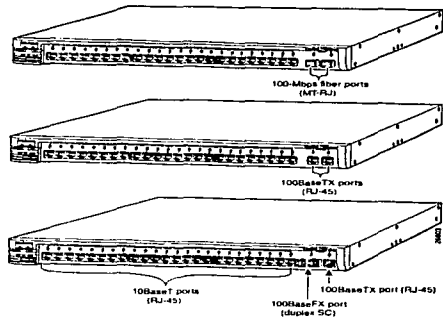


Figura 5-2 puertos del panel frontal

Puertos de 10 Mbps.

Los puertos 10BaseT en el switch (1x hasta 12x o 1x hasta 24x) utilizan conectores estándar RJ-45. Estos puertos conectan dispositivos 10BaseT compatibles, como estaciones de trabajo individuales y concentradores, con cableado de Categoría 3, 4, o 5. Utilizando este tipo de cableado la distancia entre el switch y el dispositivo conectado puede ser de hasta 100 metros.

Puertos de 100 Mbps

Dependiendo del modelo, el switch puede tener los siguientes puertos de red de alta velocidad:

- Dos puertos 100BaseTX
- Un puerto 100BaseTx y un puerto 100BaseFX
- Dos puertos para fibra óptica 100 Mbps

El modelo con puertos 100BaseTX (Ax y Bx) utiliza conectores estándar RJ-45. Estos puertos se pueden conectar a servidores, hubs, switches y routers 100BaseTX compatibles con cableado de categoría 5. La distancia entre el switch y los dispositivos conectados puede ser de hasta 100 metros.

El modelo con un puerto 100BaseFX (A) utiliza un conector duplex (SC). Este puerto se conecta a dispositivos 100BaseFX compatibles con cableado de fibra multimodo 50/125 o 62.5/125.

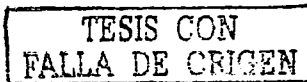
La conexión de fibra óptica entre el switch y el dispositivo conectado es como sigue:

- Si el puerto del switch del dispositivo conectado son configurados para operación half-duplex la conexión puede ser de distancias hasta los 412 metros.
- Si los puertos del switch y del dispositivo conectado son configurados para operación full-duplex puede alcanzar distancias de hasta 2 kilómetros.

El modelo con dos puertos de fibra óptica (A y B) utilizan conectores MT-RJ y tienen una longitud de onda de 1300 nanómetros.

Descripción de la parte trasera del switch

En la parte trasera del switch se localiza el conector de alimentación AC, un puerto de consola, y conector del sistema de potencia redundante y un puerto AUI (Figura 5-3)



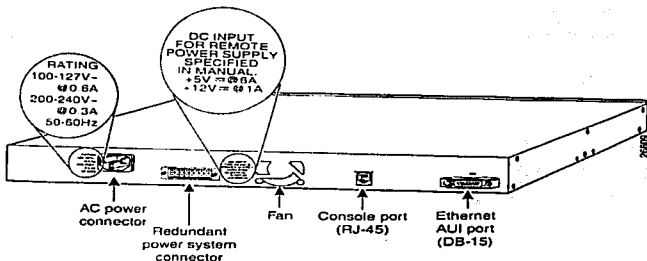


Figura 5-3 Puertos y conectores de la parte trasera

Conectores de alimentación

Se puede suministrar energía al switch ya sea usando la fuente de alimentación AC interna o conectando una fuente de alimentación redundante Cisco 6000W (RPS) al conector RPS .

El suministro interno de energía es una unidad que soporta voltajes de entrada del rango de 90 hasta 127 VAC o 200 a 250 VAC.

La fuente RPS suministra alimentación redundante hasta para cuatro dispositivos de 150 W cada uno..

Puerto de consola

Para configurar y administrar el switch a través de la consola de diagnóstico y administración y la interfaz de línea de comando (CLI) , se conecta el puerto de la consola a la estación de trabajo o MODEM con cable RJ-45 apropiado.

Puerto AUI

Se puede conectar el switch a cualquier dispositivo Ethernet 10 Mbps a través del puerto AUI mediante un Transceiver Ethernet

LEDs de estado

Los switches Catalyst poseen varios LEDs de estado (como se ilustra en la Figura 5-4) que están generalmente en verde cuando el switch funciona normalmente, y se vuelven ámbar cuando existe un mal funcionamiento.

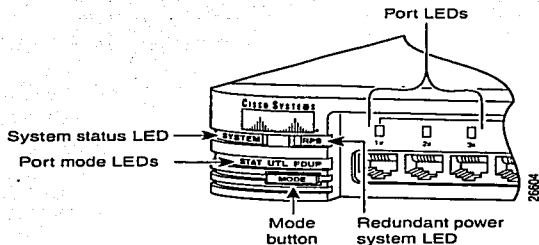


Figura 5-4 LEDs y Botón de Modo

La Tabla 5.1 explica las funciones de los LED System y del redundant power supply (RPS), o suministro redundante de energía, en un switch Catalyst, según los estados de las luces.

| LED del switch | Descripción |
|----------------------------------|--|
| LED System | Verde: el sistema está encendido y operativo. Ámbar: el sistema no funciona bien. |
| Suministro redundante de energía | Verde: RPS operativo. Ámbar: RPS instalado, pero no operativo. Verde intermitente: tanto el RPS como el suministro de energía interno están activados y la energía interna está alimentando al switch. |

Tabla 5.1. Descripción de los estados de los LED System y RPS en un switch Catalyst

Los LED de los puertos del switch Catalyst poseen varios modos de operación. Como se verá más adelante, las rutinas de arranque iniciales utilizan los LED para mostrar el estado de las pruebas al inicio (POST).

Si el switch está activado y en marcha, pulsando el botón MODE (véase la Figura 5-4), se conmuta entre los demás modos de los LED. Esos tres modos indican:

- Estado del puerto.
- Utilización de ancho de banda por parte del switch.
- Soporte full-duplex.

La Tabla 5.2 contiene una lista de los modos de los LED y lo que éstos indican en función de los distintos colores o tipo de iluminación.

| Modo LED de puerto | Descripción |
|-----------------------------|---|
| Estado LED de puerto (STAT) | Verde: enlace presente. Verde intermitente: actividad. Verde y ámbar alternativos: falta de enlace. Ámbar: el puerto no envía señales. |
| Utilización (UTL)* | LED del 1 al 8 activados: 0,1 a <6 Mbps. LED del 9 al 16 activados: 6 a <120 Mbps. LED del 17 al 24 activados: 120 a 280 Mbps |
| Full dúplex (FDUP) | Verde: puertos configurados en modo full-duplex. No verde: puertos en modo half-duplex. |

Tabla 5.2. Descripciones de los estados de los modos de LED de puerto de un switch Catalyst.

*Los valores de utilización mostrados corresponden a un switch de 24 puertos. Estos serían los valores para el switch de 12 puertos:

1 a 4: 0/1 a <1.5Mbps

5 a 8: 1,5 a 20 Mbps

9 a 12: 20 a 120 Mbps

El POST Catalyst se ejecuta sólo cuando se enciende el switch. El POST utiliza los LED de los puertos del switch para indicar el avance y estado de la prueba. Inicialmente los LED de todos los puertos están en verde. Esta condición indica el inicio del POST y que los LED funcionan correctamente. Cada uno de los 16 primeros LED de puerto (del 1x al 16x) están asociados con una de las pruebas POST, como indica la Tabla 5.3.



Después de cada test POST, el LED de dicha prueba indica los resultados de la misma:

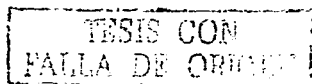
- Si la prueba se ha completado sin fallos, el LED correspondiente se apaga.
- Si la prueba ha revelado algún fallo, el LED correspondiente se vuelve ámbar; el LED del sistema también se vuelve ámbar en este caso.

Tras un proceso POST sin fallos, los LED se vuelven intermitentes y después se apagan.

Si hay fallos fatales, como se indica en la Tabla 5.3, el switch no es operativo. Con errores no fatales, el switch seguiría operativo, aunque con una funcionalidad limitada.

| LED | Componente verificado | Tipo de fallo |
|---------|---------------------------------------|--|
| LED 16x | ECU DRAM | Fatal. |
| LED 15x | No utilizado | |
| LED 14x | No utilizado | |
| LED 13x | No utilizado | |
| LED 12x | Motor enviando | Fatal. |
| LED 11X | Motor enviando SRAM | Fatal. |
| LED 10X | Paquete DRAM | Fatal. |
| LED 9x | ISLT ASIC | Fatal. |
| LED 8x | Control/estado del puerto | Fatal. |
| LED 7x | Interruptor de cronómetro del sistema | Fatal. |
| LED 6x | Contenido direccionable (CAM) SRAM | Fatal. |
| LED 5X | Reloj en tiempo real | No fatal: si falla esta prueba, el switch envía paquetes. Sin embargo, si el switch se viene abajo inesperadamente, no podrá iniciarse automáticamente. |
| LED 4X | Puerto de consola | No fatal: si falla esta prueba, no podrá acceder a la consola de administración a través del puerto de consola. Sin embargo, puede hacer un Telnet a la consola de administración. |
| LED 3X | CAM | Fatal. |
| LED 2X | Burued in address | No fatal: si falla esta prueba, el switch usa su Ethernet por omisión y comienza a enviar paquetes. |

Continúa en la siguiente página.....



LED 1X

Puerto loopback

No fatal: si falla esta prueba, se ha perdido parte de la funcionalidad de uno o más puertos. El switch desactiva los puertos que fallan en el test y el mensaje de error en el Menú Console Logon Screen indica el puerto o puertos que no han pasado la prueba. Utilice sólo puertos que hayan pasado la prueba.

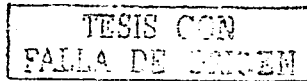
Tabla 5.3 Asociaciones de prueba LED/POST del Switch Catalyst 1924

Inicio de una sesión en un switch 1900 tras el arranque

Si se detectan fallos en la prueba POST durante el arranque inicial, serán informados a la consola. Si el POST se completa con éxito, la primera pantalla que aparezca será la Menu Console Logon Screen, o pantalla del menú de inicio de sesión en la consola, como muestra el Ejemplo 5.1.

Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc.1993-1998
All rights reserved.
Enterprise Edition Software
Ethernet Address: 00-50-BD-73-E2-C0
PCA Number: 73-3121-01
PCA Serial Number: FM0252A0QX
Model Number: WS-C1924-EN
System Serial Number: FM0304S0U3
Power Supply S/N: PH1025101F3

1 user-(s) now active on Management Console
user Interface Menu
[M] Menus
[K] Command Line
[I] IP Configuration
Enter Selection:



Ejemplo 5.1. Menu Console Logon Screen.

En la pantalla de inicio de sesión hay tres opciones:

- Teclee **M** para entrar en el modo menú.
- Teclee **K** para entrar en el modo de línea de comandos.
- Teclee **I** para entrar en el modo de configuración IP

El modo **M** es el modo menú. Este modo puede usarse para configurar todos los parámetros del switch. El modo menú proporciona descripciones y sugerencias relativas a los parámetros de configuración. Éste puede ser un modo útil cuando no se está familiarizado con los parámetros que se desea configurar. Es el único modo disponible en un switch 1900 estándar.

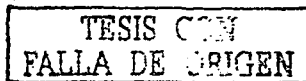
Cuando se configura el switch desde la interfaz de usuario que se ejecuta en una consola o terminal remotos, el software Cisco IOS proporciona una interfaz de línea de comandos (CLI), opción **K**, denominada comúnmente modo EXEC. El procedimiento EXEC interpreta los comandos introducidos y lleva a cabo las operaciones correspondientes. Para acceder a este modo es necesario haber iniciado la sesión previamente en el dispositivo.

Por razones de seguridad el proceso EXEC posee dos niveles de acceso a los comandos: el modo usuario y el modo privilegiado.

- **Modo usuario.** Entre las tareas típicas figuran la comprobación del estado del switch (modo sólo comprobar).
- **Modo privilegiado.** Entre las tareas típicas están el cambio de la configuración del switch.

El Ejemplo 5.2 muestra el proceso de paso entre los dos niveles EXEC, donde el símbolo > indica el modo usuario y el símbolo # indica el modo privilegiado.

```
>
> enable
Enter password:
#
# disable
> exit
```



Ejemplo 5.2. Cambio entre los niveles EXEC de usuario y privilegiado

Ayuda de teclado en la interfaz de línea de comandos del switch

El switch Catalyst utiliza software Cisco IOS con varias opciones de ayuda para entradas en la línea de comandos, incluidas las siguientes:

- **Ayuda relativa al contexto.** Proporciona una lista de comandos y argumentos asociados con cada comando específico.
- **Mensajes de error de consola.** Identifica problemas con los comandos del switch introducidos incorrectamente para que puedan ser corregidos.
- **Buffer de historial de comandos.** Permite volver a llamar largos y complicados comandos o entradas para volver a ejecutarlos, revisarlos o corregirlos.

Ayuda relativa al contexto para switches

Un signo de interrogación (?) durante una sesión EXEC proporciona siempre ayuda en pantalla. Hay dos tipos de ayuda relativa al contexto disponibles: ayuda de texto y ayuda relativa a la sintaxis de un comando.

Se puede usar ? para obtener una lista de todos los comandos que comienzan por una secuencia de caracteres determinada. Para ello, se escribe el carácter o caracteres seguidos del signo ?. No se incluye ningún espacio de separación delante del signo de interrogación. El switch mostrará una lista de los comandos que comienzan con los caracteres especificados. Por ejemplo, s? daría como resultado la salida que muestra el Ejemplo 5.3.

```
cisco 1900#s?  
session show  
cisco 1900#s
```

Ejemplo 5.3. Ejemplo de la característica de ayuda de comandos

También puede usar ? para conseguir ayuda acerca de la sintaxis específica de un comando. Se introduce ? en lugar de una palabra clave o argumento sobre cuya sintaxis no se está seguro. Recuerde que ha de incluir un espacio delante de ?. El dispositivo de red mostrará en pantalla una lista de las opciones disponibles para el comando en cuestión, donde <cr> representa un retorno de carro (cosa que no sucede en el Ejemplo 5.3). El Ejemplo 5.4 muestra un ejemplo de la salida obtenida al introducir show ? junto al símbolo de comandos.



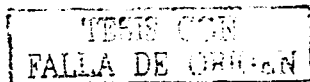
| | |
|-------------------|--|
| cisco 1900#show ? | |
| bridge-group | Display port grouping using bridge groups |
| cdp | cdp information |
| cgmp | Cgmp information |
| history | Display the session command history |
| interfaces | interface status and configuration |
| ip | Display IP configuration |
| line | Display console/RS-232 port configuration |
| mac-address-table | MAC forwarding table |
| Port | Display port information |
| running-config | Show current operating configuration |
| snmp | Display snmp related information |
| spantree | Spanning tree subsystem |
| spantree-option | Show STP port option parameter |
| spantree-template | Show STP bridge template parameters |
| storm-control | Show broadcast storm control configuration |
| tacacs | Shows tacacs+server configuration |
| terminal | Display console/RS-232 port configuration |
| tftp | TFTP configuration and status |
| trunk | Display trunk information |
| uplink-fast | Uplink Fast |
| usage | Display usage summaries |
| version | System hardware and software status |
| vlan | Show VLAN information |
| vlan-membership | Show VLAN membership information |
| vtp | VLAN trunk protocol |

Ejemplo 5.4. Salida de show ?

SUGERENCIA: Es posible abreviar los comandos en Cisco IOS introduciendo el número suficiente de caracteres. Por ejemplo, en lugar de teclear el comando `show interface`, bastaría introducir `sh int`.

Mensajes de error de consola para switches

Los mensajes de error de consola del sistema de ayuda del switch Catalyst permiten identificar problemas relativos a entradas de comandos incorrectas. La interpretación del mensaje nos ayudará a averiguar cómo se debe modificar la entrada de la línea de comandos para corregir el problema.



La tabla 5.4 muestra un listado donde se describen algunos errores CLI comunes y explica como obtener ayuda.

| Mensaje de error | Significado | Cómo obtener ayuda |
|--|---|---|
| %Ambiguous command: "show con" | No se han introducido suficientes caracteres para que el switch pueda reconocer la orden. | Vuelva a introducir la orden seguida de un signo de interrogación(?) sin espacio entre la orden y dicho signo |
| % Incomplete command | No se han introducido todas las palabras clave o valores requeridos por la orden. | Vuelva a introducir la orden seguida de un signo de interrogación (?) con un espacio entre la orden y dicho signo. |
| % Invalid input detected at (^) marker | Se ha introducido la orden incorrectamente. El circunflejo (^) marca el punto donde se ha detectado el error. | Introduzca un signo de interrogación(?) para obtener un listado de todas las órdenes que están disponibles en este modo de comando. |

Tabla 5.4. Mensajes de error CLI comunes

Buffer de historial de comandos para switches

Revisar el historial de comandos proporciona una lista del contenido del buffer de sustitución del switch. Se trata de una lista de comandos introducidos recientemente. Para ver dichos comandos, se introduce el comando history del software Cisco IOS.

Switch#history

A continuación verá una lista con el historial de comandos, lo que nos permitirá volver a utilizar cualquiera de ellos sin necesidad de teclearlo de nuevo.

Para volver a presentar un comando introducido con anterioridad, se pulsa la tecla flecha. Si se sigue pulsando esa misma tecla, accederá a otros comandos anteriores. La Tabla 5.5 describe las funciones del historial de comandos.

| Comando o combinación de teclas | Funcionalidad |
|---------------------------------|--|
| Ctrl-p o tecla flecha arriba | llamada al último comando (previo). |
| Ctrl-n o tecla flecha abajo | llamada al comando más reciente |
| Switch>show history | Muestra el contenido del búfer de comandos |

Tabla 5.5. Desplazamiento en el historial de comandos

Comandos para obtener información básica del switch

Hay ciertos comandos CLI que proporcionan información acerca de la configuración y el estado del switch. Estos comandos consisten básicamente en instrucciones show que hacen que el switch muestre información junto al símbolo de comandos. Hay muchos comandos show que pueden ser introducidos tanto en el modo EXEC de usuario como en el modo EXEC privilegiado. Algunas comandos están limitados al modo EXEC privilegiado.

Comando show versión

El comando show versión muestra información acerca del hardware del sistema, la versión del software, los nombres y fuentes de los archivos de configuración, así como las imágenes de arranque, como ilustra el Ejemplo 5.5.

```
wg_sw_c#show version
Cisco Catalyst 1900/2820 Enterprise Edition Software
Versión V8.01.01 written from 171.068.229.225
Copyright (c) Cisco Systems, Inc. 1993-1998
wg_sw_c uptime is 15day(s)21hour(s)53minute(s)11second(s)
cisco Catalyst 1900 (486sx)processor with 2048K/1024K bytes of memory
Hardware board revision is 5
Upgrade Status:No upgrade currently in progress.
```

TESIS CON
FALLA DE ORIGEN

Continúa en la siguiente página

Config File Status: No configuration upload/download is in progress
27 Fixed Ethernet/IEEE 802.3 interface(s)
Base Ethernet Address: 00-50-BD-73-E2-C0

TESIS CON
FALLA DE ORIGEN

Ejemplo 5.5. Salida de show versión en un switch Catalyst.

Show versión permite determinar el sistema operativo actual del switch. Esta información puede ser de utilidad para determinar la capacidad del switch, así como para corregir problemas. La Tabla 5.6 muestra los campos clave de salida de este comando.

| Salida | Descripción |
|---------------------|---|
| Versión de software | Información que identifica el software por su nombre y número de versión, incluida la fecha y hora de compilación. Especifique siempre el número completo de versión cuando tenga que informar de algún problema surgido con el software. |
| Switch uptime | Número de días, horas, minutos y segundos desde que el sistema fue iniciado por última vez. |
| Cisco... | El resto de la salida muestra información del hardware y opciones del software no estándar. |

Tabla 5.6. Campos clave de la salida de show versión.


NOTA: La serie de switches 1900 soporta dos versiones de software: estándar y enterprise. La versión enterprise es la que está siendo objeto de estudio en este trabajo, debido a que posee funciones mejoradas. El software estándar no soporta la opción de intertaz de línea de comandos para su configuración. Algunos switches de la serie 1900 pueden ser actualizados a la versión de software enterprise

Comando show running-configuration

Show running-configuration es un comando privilegiado que muestra el archivo de configuración activo del switch, incluidos la contraseña, el nombre del sistema y la configuración de

las interfaces, consola y puertos auxiliares. El Ejemplo 5.6 muestra la salida obtenida al ejecutar el comando show running-configuration en un Catalyst 1924 y después en un Catalyst 1912.

```
wg_sw_c#show run
Building configuration...
Current configuration:
hostname "wg_sw_c"
ip address 10.1.1.33 255.255.255.0
ip default-gateway 10.3.3.3
interface Ethernet 0/1
< texto omitido>
interface Ethernet 0/24
!
Interface Ethernet 0/25
!
interface FastEthernet 0/26
interface FastEthernet 0/27
wg_sw_c#show run
Building configuration...
Current configuration:
!
hostname "wg_sw_c"
!
ip address 10.1.1.33 255.255.255.0
ip default-gateway 10.3.3.3
!
interface Ethernet 0/1
< texto omitido>
interface Ethernet 0/12
!
Interface Ethernet 0/25
!
interface FastEthernet 0/26
!
interface FastEthernet 0/27
```



Ejemplo 5.6. show running-configuration en un Catalyst 1924 y un Catalyst 1912.

NOTA: Los archivos de configuración Cisco IOS muestran generalmente información de configuración no predeterminada. Por ejemplo, no es posible saber si está activado el Protocolo de árbol de extensión examinando el contenido de dicho archivo, aunque la configuración por omisión dicta que esté activado.

Comando show interfaces

El comando `show interfaces` muestra estadísticas de todas las interfaces configuradas en el switch. La salida resultante varía en función de la red para la que haya sido configurada una interfaz. Normalmente, este comando se introduce con las opciones `type` y `slotnumber`, donde `type` permite valores tales como Ethernet y FastEthernet, y `slotnumber` indica la ranura y número de puerto en la interfaz seleccionada. Para switches de la serie 1900, la ranura es siempre 0. El Ejemplo 5.7 muestra algunas salidas obtenidas al ejecutar el comando `show interfaces`.

```
wg_sw_c#show interfaces ethernet 0/1
Ethernet 0/1 is Enabled
Hardware is Built-in 10Base-T
Address is 0050.BD73.E2C1
MTU 1500 bytes, BW 10000 Kbits
802.1d STP State: Forwarding Forward Transitions: 1
Port monitoring: Disabled
Unknown unicast flooding: Enabled
Unregistered multicast flooding: Enabled
Description:
Duplex setting: Half duplex
Back pressure: Disabled
---- More-----
```

Ejemplo 5.7. Salida de `show interfaces`.

El comando `Show interfaces` resulta muy útil al configurar y resolver conflictos en el switch. La Tabla 5.7 muestra los detalles del significado de algunos de los campos más significativos de esta salida.

| Salida | Descripción |
|--------------------------------------|---|
| Ethernet 0/1 is Enabled | Indica el estado actual del hardware de la interfaz. Enabled significa una interfaz activa. |
| Hardware is ... 10BaseT | Muestra las características físicas del puerto del switch |
| Continúa en la siguiente página..... | |

| | |
|------------------------------|---|
| Address is 0050.DB73.E2C1 | Dirección de Control de acceso al medio (MAC) que identifica este puerto de switch en el segmento LAN |
| MTU 1500 bytes | Tamaño de la unidad máxima de transmisión para la interfaz |
| 802-1d STP State: Forwarding | Indica el estado del Protocolo de árbol de extensión. En este caso, el Árbol de extensión permite que el puerto envíe tramas. |

Tabla 5.7. Campos clave de la salida de show interfaces

Observemos que en esta salida están representadas las dos capas del modelo OSI: **Hardware is 10BaseT** (física) y **Address is 0050.DB73.E2C1** (enlace de datos). Como sabemos estos switches operan en la Capa 2 del modelo OSI.

Comando show ip

El comando Show ip muestra la configuración IP actual del switch. El Ejemplo 5.8 muestra algunas salidas obtenidas al ejecutar el comando Show ip.

```

Wg_sw_a#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#

```



Ejemplo 5.8. Salida de show ip.

La salida del comando `show ip` muestra la dirección IP, máscara de subred, dirección de puerta de enlace (gateway) y otros parámetros IP configurables.

Configuración del switch desde la línea de comandos

La mayoría de las funciones de un switch están implementadas en el firmware del dispositivo para mejorar el rendimiento. Debido a esto y al hecho de que el switch opera independientemente de cualquier información de protocolo de la Capa 3, el switch puede ser implementado con una configuración mínima. Sin embargo, hay muchos parámetros del switch que pueden ser modificados para personalizarlo con arreglo a las necesidades de la red. Para poder configurar un switch, es necesario pasar al modo de línea de comandos, para así poder cambiar los parámetros de configuración. El modo del switch que permite hacer esto es el modo de configuración. Existen muchos modos de configuración disponibles para configurar distintos parámetros del switch. Para configurar parámetros del Switch pasaremos del modo EXEC privilegiado a los distintos modos de configuración.

La siguiente sintaxis corresponde al modo de configuración global:

```
wg_sw_a# conf term
```

```
wg_sw_a (config)#
```

El modo de configuración de la interfaz tiene este aspecto:

```
wg_sw_a(config)# interface e0/1
```

```
wg_sw_a (config.if)#
```

Observemos el cambio del símbolo cuando pasamos de un modo a otro. Como siempre, podemos acceder a ayuda relativa a este nivel de la CLI usando el signo de interrogación (?). Es importante mencionar que los cambios realizados en la configuración del switch son inmediatos. En cuanto se pulsa **Enter** en cualquier modo de configuración, el parámetro queda modificado y la acción se ejecuta en la memoria activa.

Uno de los primeros aspectos que se deben configurar en el switch es el nombre del sistema. Asignar un nombre al switch facilita la administración de la red al poder identificar con facilidad cada switch. El nombre del switch pasa a considerarse como nombre de host y su nombre aparece junto al símbolo de comandos. La siguiente instrucción muestra el proceso de asignar un nombre a un switch (observemos que el cambio es inmediato):


```
(config)#hostname wg_sw_c
```

```
wg_sw_c(config)#
```

Otro parámetro que se deberá configurar en el switch es una dirección IP. La dirección IP es un parámetro global establecido en el switch y se requiere para realizar Telnet hacia y desde el switch. La instrucción para configurar la dirección IP (para el switch denominado wg_sw_a sería wg_sw_a(config)#ip address mascara_de_direccion_ip.

Por ejemplo, se podría realizar la siguiente asignación de dirección IP:

```
wg_sw_a(config)#ip address 10.5.5.11 255.255.255.0
```

Ejemplos de configuración del switch

Resumiendo, el switch Catalyst 1900 ofrece los tres modos de configuración que figuran a continuación:

- Interfaz controlada por menús desde el puerto de consola
- Administrador de switch visual (VSM) basado en la Web
- Uso de la interfaz de línea de comandos (CLI) IOS

Todos los modos de configuración permiten llevar a cabo el mismo conjunto de tareas. El uso de VSM requiere que el switch posea una dirección IP y tenga configurada una conectividad con la red que le permita comunicarse con un navegador web como Netscape o Microsoft Internet Explorer. También es necesario asignar una dirección IP si se va a conectar al switch a través de Telnet o si se va a usar SNMP para administrar dicho dispositivo.

Este trabajo se centra en el uso de CLI para configurar el switch.

Opciones de configuración predeterminadas

El switch Catalyst 1900 viene de fábrica con una configuración predeterminada. Para muchos parámetros, dicha configuración puede resultar apropiada. Sin embargo, probablemente se desee modificar algunos de los valores por omisión para adaptarlos a la topología específica de la red. Los valores predeterminados varían en función de las características de cada switch. La siguiente lista muestra algunos de los parámetros predeterminados del switch Catalyst 1900.

- Dirección IP: 0.0.0.0
- CDP: habilitado.
- Modo de conmutación: sin fragmentos.
- Puerto 100BaseT: negociación automática del modo dúplex.
- Puerto 10BaseT: half dúplex.
- Árbol de extensión: habilitado.
- Contraseña de consola: ninguna.

**TESIS CON
FALLA DE ORIGEN**

Configuración del puerto determinado

Como vimos anteriormente los modelos 1912 y 1924 son dos componentes de la familia Catalyst 1900. La Tabla 5.8 muestra un resumen de los puertos existentes en ambos switches.

| | Catalyst 1912 | Catalyst 1924 |
|------------------------|-------------------------------|-------------------------------|
| Puertos 10BaseT | 12 en total (de e0/1 a e0/12) | 24 en total (de e0/1 a e0/24) |
| Puerto AUI | e0/25 | e0/25 |
| Puertos Uplink | Fa0/26 (puerto A) | Fa0/26 (puerto A) |
| 100BaseT | Fa0/27 (puerto B) | Fa0/27 (puerto B) |

Tabla 5.8. Puertos de Catalyst 1912 y 1924.

Los puertos del Catalyst 1900 se denominan tanto puertos como interfaces. Por ejemplo, para e0/1, se tendría lo siguiente:

- La salida de **show run** (véase el Ejemplo 5.9) se refiere a e0/1 como interfaz Ethernet 0/1.
- La salida de **show spantree** (véase el Ejemplo 5.10) se refiere a e0/1 como Port Ethernet 0/1.
- La salida de **Show vlan-membership** (véase el Ejemplo 5.11) se refiere a e0/1 simplemente como Port 1.

```
wg_sw_d#sh run
Building configuration...
!
!
Current configuration:
interface Ethernet 0/1
!
interface Ethernet 0/2
```

Ejemplo 5.9. La salida de show run se refiere a e0/1 como interface Ethernet 0/1.

```
wg_sw_d#show spantree
Port Ethernet 0/1 of VLAN1 is Forwarding
Port path cost 100, Port priority 128
Designated root has priority 32768, address 0090.8673.3340
Designated bridge has priority 32768, address 0090.8673.3340
Designated port is Ethernet 0/1, path cost 0
Timers: message age 20, forward delay 15, hold 1
```

Ejemplo 5.10. La salida de show spantree se refiere a e0/1 como Designated Port Ethernet 0/1.

Ejemplo 5.11 La salida de show vlan-membership se refiere al puerto e0/1 como Port 1.

```
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 |

Ejemplo 5.11 La salida de show vlan-membership se refiere al puerto e0/1 como Port 1.

Modos de configuración

El switch Catalyst 1900 posee varios modos de configuración. Para parámetros de configuración global como el nombre de host del switch o la dirección IP, se debe usar el modo de configuración global, cuyos símbolos presentan el siguiente aspecto:

```
wg_sw_a# conf term
```

```
wg_sw_a(config)#
```

Para configurar un puerto específico, se ha de usar el modo de configuración de interfaz/ cuyos símbolos son como se indica a continuación:

```
wg_sw_a(config)# interface e0/1
```

```
wg_sw_a(config.if)#
```

Configuración de la dirección IP , Máscara de Subred Y Gateway Predeterminada

Para configurar una dirección IP y una máscara de subred en el switch, se utiliza el comando de configuración global `ip address`, cuya sintaxis se muestra a continuación:

```
wg_sw_a(config)#ip address dirección_de_máscara
```

Por ejemplo, para configurar un switch con dirección IP 10.5.5.11 y máscara de subred 255.255.255.0, se tendría que introducir el siguiente comando:

```
wg_sw_a(config)#ip address 10.5.5.11 255.255.255.0
```

Es necesario configurar una dirección IP en el switch para poder llevar a cabo tareas administrativas. Por ejemplo, el uso de VSM requiere que el switch tenga configurada una dirección IP, así como conectividad IP para poder comunicarse con un navegador web, como Netscape o Microsoft Internet Explorer. Asimismo, es necesario asignar una dirección IP si se piensa establecer una conexión con el switch por medio de Telnet, o si piensa usar SNMP para administrar el dispositivo. Esta dirección se asigna para el switch en su totalidad y es la conexión de administración. Se utiliza el comando de configuración global `no ip address` para restablecer la dirección IP a su valor predeterminado de fábrica, 0.0.0.0.

Se utiliza el comando de configuración global `ip default-gateway` para regresar a la configuración de gateway predeterminada. El comando `ip default-gateway` posee la siguiente sintaxis:

```
wg_wd_a(config)#ip default-gateway dirección ip
```

Por ejemplo, para configurar la puerta de enlace predeterminada con la dirección IP 10.5.5.3 para un switch, debería introducir el siguiente comando:

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

Al switch se le asigna una dirección IP con vistas a realizar tareas administrativas. Si el switch necesita enviar tráfico a una red IP diferente de aquella en la que se encuentra actualmente, el switch enviaría el tráfico a la gateway predeterminada, que suele ser el router. El router se usa para dirigir el tráfico entre distintas redes. Utilice el comando `no ip default-gateway` para suprimir una gateway predeterminada previamente configurada y devolver a la dirección de gateway el valor predeterminado, 0.0.0.0.

Para verificar la dirección IP, máscara de subred y la configuración de la gateway predeterminada, utilice el comando `show ip` desde el modo EXEC privilegiado, como muestra el Ejemplo 5.12.

```
wg_sw_a#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#
```

Ejemplo 5.12. El comando `show ip` verifica la dirección IP máscara de subred y configuración de gateway predeterminada para un switch Catalyst 1900.

Configuración del modo duplex para una interfaz del switch

Se Utiliza el comando de configuración de interfaz dúplex para cambiar el modo dúplex de una interfaz concreta. La sintaxis de este comando (en la interfaz e0/1 por ejemplo), sería como se indica a continuación:

```
wg_sw_a(config)#interface e0/1
```

```
wg_sw_a(config.if)#duplex {auto | full | full-flow-control | half}
```

Estas son las opciones del comando de configuración de interfaz dúplex:

- **auto.** Establece el modo dúplex de negociación automática, auto es la opción predeterminada para los puertos TX de 100 Mbps.
- **full.** Establece el modo full-duplex.
- **full-flow-control.** Establece el modo full-duplex sin control de flujo.
- **half.** Establece el modo half-duplex. half es la opción predeterminada para los puertos TX de 10 Mbps.

Por ejemplo, si se tuviera que establecer el modo half-duplex para la interfaz e0/1 en el Switch A, tendría que ejecutar los siguientes comandos:

```
wg_sw_a(config)#interface e0/1
```

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

Para verificar la configuración dúplex de una interfaz, se utiliza el comando **show interface**. Para mostrar estadísticas del estado de todas o una serie de interfaces específicas, se utiliza el comando **show interfaces** en el modo EXEC privilegiado, como en el Ejemplo 5.13

Como puede verse en la primera línea resaltada del Ejemplo 5.13, la configuración dúplex de una interfaz dada puede determinarse usando del comando **show interface**.

La negociación automática puede producir a veces resultados impredecibles. Si un dispositivo conectado no soporta el modo de negociación automática y opera en full-duplex, el switch Catalyst establecerá el modo half-duplex para el puerto correspondiente. Esta configuración (half-duplex en un extremo y full-duplex en el otro) causaría errores de colisión en el extremo full-duplex. Para evitar estas situaciones, se deben configurar manualmente los parámetros dúplex del switch, de modo que coincidan con los correspondientes a cada dispositivo conectado.

```

wg_sw_a#sh interfaces
Ethernet 0/1 is Enabled
Hardware is Built-in 10Base-T
Address is 0090.8673.3341
MTU 1500 bytes, BW 10000 Kbits
802.1d STP State: Forwarding   Forward Transitions: 1
Port monitoring: Disabled
Unknown unicast flooding: Enabled
Unregistered multicast flooding: Enabled

```

Description:

Duplex setting: Half duplex

Back pressure: Disabled

Receive Statistics

| | |
|----------------------------|---------|
| Total good frames | 44841 |
| Total octets | 4944550 |
| Broadcast/multicast frames | 3101 |
| Broadcast/multicast octets | 3685029 |
| Good frames forwarded | 44832 |
| Frames filtered | 9 |
| Runt frames | 0 |
| No buffer discards | 0 |

Errors:

| | |
|--------------------|---|
| FCS errors | 0 |
| Alignment errors | 0 |
| Giant frames | 0 |
| Address violations | 0 |

Transmit Statistics

| | |
|----------------------------|----------|
| Total frames | 404502 |
| Total octets | 29591574 |
| Broadcast/multicast frames | 390913 |
| Broadcast/multicast octets | 28478154 |
| Deferrals | 0 |
| Single collisions | 0 |
| Multiple collisions | 0 |
| Excessive collisions | 0 |
| Queue full discards | 0 |

Errors:

| | |
|-----------------------|---|
| Late collisions | 0 |
| Excessive deferrals | 0 |
| Jabber errors | 0 |
| Other transmit errors | 0 |

Ejemplo 5.13. La salida de show interfaces muestra estadísticas y el estado de todas las interfaces especificadas del switch.

Si el puerto del switch está en el modo full-duplex y el dispositivo asociado se encuentra en el modo half-duplex, compruebe errores en la Secuencia de verificación de trama (FCS) y colisiones en el puerto full-duplex del switch.

Se utiliza el comando show interfaces para verificar FCS y errores de colisión. Un número elevado de errores de colisión suele ser indicativo de una configuración dúplex incorrecta. La falta de ajuste en el modo dúplex de los dispositivos puede traer como consecuencia una respuesta

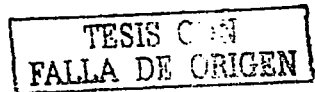
más lenta en los clientes de la red. En la segunda línea resaltada del Ejemplo 5.13 puede ver los contadores de colisiones.

Direcciones MAC e interfaces de puerto del switch

Los switches utilizan la tabla de direcciones MAC para retransmitir tráfico entre puertos. La tabla MAC incluye direcciones dinámicas, permanentes y estáticas. Introduciendo el comando `show mac-address-table` se obtiene la tabla de direcciones MAC y se puede saber cuántas direcciones dinámicas, permanentes y estáticas existen, así como el tipo usado en cada interfaz (véase el Ejemplo 5.14).

```
wg_sw_a#sh mac-address-table
Number of permanent addresses : 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 |
| 00D0.588F.B600 | FastEthernet 0/26 | Dynamic | All |
| 00D0.5892.38C4 | FastEthernet 0/27 | Dynamic | All |



Ejemplo 5.14. La salida de `show mac-address-table` muestra la tabla de direcciones MAC para las interfaces de puerto en un switch específico.

Direcciones MAC dinámicas

Las direcciones dinámicas son direcciones de origen del Control de acceso al medio (MAC) que son aprendidas por el switch y descartadas posteriormente cuando dejan de usarse. El switch proporciona aprendizaje de direcciones dinámicas anotando las direcciones de origen de cada paquete que es recibido en cada puerto, y agregando la dirección y el número del puerto asociado a la tabla de direcciones. Conforme se agregan o quitan puestos de la red, el switch actualiza la tabla de direcciones, agregando nuevas entradas y descartando las que dejan de estar en uso.

Direcciones MAC permanentes

Un administrador puede asignar específicamente direcciones permanentes a ciertos puertos usando el comando `mac-address-table permanent`, cuya sintaxis se muestra a continuación:

```
wg_sw_a(config)#mac-address-table permanent direc. mac tipo módulo/puerto
```

En la Tabla 5.9 están descritos los argumentos del comando `mac-address-table permanent`.

| Argumento del comando | Significado |
|-----------------------|---|
| dirección mac | Una dirección MAC de unidifusión |
| tipo | Tipo de interfaz: ethernet, fastethernet, fddi/ atm o port-channel. |
| Módulo/puerto | Número de módulo: 0 para la serie Catalyst 1900 Número de puerto: 1-24 Ethernet 26 y 27 Fast Ethernet 28 Port-channel |

Tabla 5.9. Argumentos del comando `mac-address-table permanent`.

A diferencia de las direcciones dinámicas, las direcciones permanentes no tienen fecha de expiración.

El Catalyst 1900 puede guardar un máximo de 1024 direcciones MAC en la tabla de direcciones MAC. Cuando la tabla de direcciones MAC se llena, se inundan todas las direcciones nuevas hasta que expire alguna de las existentes.

Para garantizar que una dirección se encuentre siempre en la tabla MAC, puede usar el comando de configuración global `mac-address-table permanent` para asociar una dirección MAC permanente a un interfaz de puerto conmutado concreto (especificada por su tipo módulo/puerto). Se utiliza el comando `no mac-address-table permanent` para borrar una dirección MAC permanente.

Una dirección permanente en la tabla de direcciones MAC está configurada para no expirar, y todas las interfaces pueden enviar tráfico a ese puerto, aunque el dispositivo sea trasladado.

Por ejemplo, al introducir el siguiente comando:

```
wg_sw_a(config)#mac-address-table permanent 2222.2222.2222 ethernet 0/3
```

se está especificando que las tramas con la dirección de destino 2222.2222.2222 deben ser reenviadas a la interfaz ethernet 0/3, y todas las interfaces pueden enviar tráfico a 2222.2222.2222.

Para verificar que la asignación de una dirección MAC permanente se ha llevado a cabo con éxito, se introduce el comando `show mac-address-table` como se muestra en el Ejemplo 5.15.

```
wg_sw_a#sh mac-address-table
Number of permanent addresses : 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 |
| 00D0.588F.B604 | FastEthernet 0/26 | Dynamic | All |
| 00E0.1E5D.AE2B | FastEthernet 0/26 | Dynamic | All |
| 00D0.5892.38C4 | FastEthernet 0/27 | Dynamic | All |

Ejemplo 5.15. La salida de `show mac-address-table` permite verificar las direcciones MAC permanentes.

Direcciones MAC estáticas

Una dirección MAC estática permite restringir el tráfico a una dirección MAC particular desde una interfaz de origen específica.

Se utiliza el comando de configuración global `mac-address-table restricted static` para asociar una dirección estática restringida a una interfaz de puerto conmutado específico. La sintaxis de este comando es como se indica a continuación:

```
wg_sw_a(config)#mac-address-table restricted static dirección mac tipo modulo/puerto lista
interfaces origen
```

En la Tabla 5.10 se describen los argumentos del comando `mac-address-table restricted static`.

| Argumento del comando | Significado |
|-------------------------|---|
| dirección mac | Una dirección MAC de unidifusión |
| tipo | Tipo de interfaz: ethernet, fastethernet, fddi/ atm o port-channel. |
| módulo/puerto | Número de módulo: 0 para la serie Catalyst 1900 Número de puerto: 1-24 Ethernet 26 y 27 Fast Ethernet 28 Port-channel |
| Lista interfaces origen | Lista de interfaces aceptables, separadas por espacios |

Tabla 5.10. Argumentos del comando `mac-address-table restricted static`

Se utiliza el comando `no mac-address-table restricted static` para borrar direcciones estáticas restringidas.

Introduciendo el siguiente comando:

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

el switch haría que el tráfico quedara restringido a la dirección estática 1111.1111.1111 en e0/4, sólo desde la interfaz de origen e0/1. Para verificar que la asignación de dirección MAC estática restringida se ha realizado con éxito, se introduce el comando `show mac-address-table`, como se muestra en el Ejemplo 5.16

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

| Address | Dest Interface | Type | Source Interface List |
|----------------|-------------------|-----------|-----------------------|
| 1111.1111.1111 | Ethernet 0/4 | Static | E0/1 |
| 00E0.1E5D.AE2F | Ethernet 0/2 | Dynamic | All |
| 2222.2222.2222 | Ethernet 0/3 | Permanent | All |
| 00D0.588F.B604 | FastEthernet 0/26 | Dynamic | All |
| 00E0.1E5D.AE2B | FastEthernet 0/26 | Dynamic | All |
| 00D0.5892.38C4 | FastEthernet 0/27 | Dynamic | All |

Ejemplo 5.16. La salida del comando `show mac-address-table` permite verificar las direcciones MAC estáticas restringidas.

Configuración de seguridad de puertos del Switch

Otra restricción basada en MAC disponible como opción del switch es la seguridad de puerto. La seguridad de puerto posee las siguientes ventajas:

- Configura una interfaz como puerto seguro, de tal forma que sólo puedan conectarse a un puerto dado determinados dispositivos.
- Identifica el número máximo de direcciones MAC permitidas en la tabla de direcciones para dicho puerto (en un rango de 1 a 132, siendo 132 es el valor predeterminado).

Se utiliza el comando de configuración de interfaz **port secure** para habilitar la seguridad de direcciones. La sintaxis de este comando es como se indica a continuación:

```
wg_se_a(config-If)#port secure [max-mac-count contador]
```

El valor **contador** estipulado para **max-mac-count** estipula el número máximo de direcciones permitidas en el puerto. Por ejemplo, para establecer en 1 el número máximo de direcciones permitidas para conectarse a la interfaz e0/4 podría introducir el siguiente comando:

```
wg_se_a(config-If)#interface e0/4
```

```
wg_se_a(config-If)#port secure max-mac-count 1
```

Se utiliza el comando **no port secure** para inhabilitar la seguridad de direcciones, o establecer el número de direcciones en su valor predeterminado (132).

Los puertos asegurados restringen el uso de un puerto a un grupo de usuarios o puestos definido. El número de dispositivos para un puerto asegurado puede variar desde 1 hasta 132. Las direcciones MAC para los dispositivos en un puerto seguro son asignadas estáticamente por un administrador, o bien son aprendidas con fijación. El aprendizaje con fijación tiene lugar cuando la tabla de direcciones para un puerto seguro no contiene un complemento de direcciones estáticas. El puerto aprende con fijación la dirección de origen de las tramas entrantes y las asigna de manera automática como direcciones permanentes.

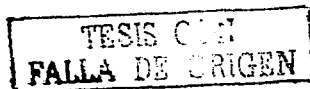
Se utiliza el comando **show mac-address-table security** del modo EXEC privilegiado cuando desee obtener un listado donde verificar las configuraciones de seguridad de puertos. El Ejemplo 5.17 muestra algunos casos de salida del comando **Show mac-address-table security**.

```
wg_sw_a#show mac-address-table security
```

```
Action upon address violation : Suspend
```

```
Interface      Addressing Security  Address Table Size
```

| | | |
|--------------|----------|-----|
| Ethernet 0/1 | Disabled | N/A |
| Ethernet 0/2 | Disabled | N/A |
| Ethernet 0/3 | Disabled | N/A |
| Ethernet 0/4 | Enabled | 1 |
| Ethernet 0/5 | Disabled | N/A |
| Ethernet 0/6 | Disabled | N/A |
| Ethernet 0/7 | Disabled | N/A |
| Ethernet 0/8 | Disabled | N/A |
| Ethernet 0/9 | Disabled | N/A |



Ejemplo 5.17 La salida de show mac-address-table security permite verificar las configuraciones de seguridad de puertos.

Cuando un puerto asegurado recibe una dirección de origen que ha sido asignada a otro puerto asegurado o cuando un puerto trata de aprender una dirección que supera el tamaño máximo de su tabla de direcciones, tiene lugar una violación de dirección. Cuando esto ocurre, las opciones a adoptar en relación al puerto incluyen suspender, ignorar o inhabilitar el puerto. Cuando un puerto es suspendido, se vuelve a habilitar cuando se recibe un paquete que contenga una dirección válida. Cuando un puerto se inhabilita, debe ser rehabilitado manualmente. Si la acción es ignorada, el switch ignora la violación de seguridad y mantiene el puerto habilitado.

Se utiliza el comando de configuración global **address-violation** para especificar la acción que se debe adoptar cuando tiene lugar una violación de dirección. La sintaxis de este comando es como se indica a continuación:

```
wg_sw_a(config)#address-violation {suspend | disable | ignore}
```

Se utiliza el comando no **address-violation** para devolver al switch su configuración predeterminada (**suspend**).

Cómo mostrar información IOS del switch

El IOS es el software funcional que ejecuta la mayoría de las operaciones principales del switch, al tiempo que provee la interfaz administrativa para su configuración.

Se utiliza el comando EXEC de usuario `show versión` para mostrar información básica acerca del hardware y la versión del software IOS, como muestra el Ejemplo 5.18.

```
wg_sw_a#show versión
Cisco Catalyst 1900/2820 Enterprise Edition Software
Versión V8.01.01
Copyright (c) Cisco Systems, Inc. 1993-1998
ROM: System Bootstrap, Versión 3.03
wg_sw_d uptime is 8day(s)17hour(s)53minute(s)25second(s)
cisco Catalyst 1900 (486sx1)processor with 2048K/1024K bytes of memory
Hardware board revisión is 1
Upgrade Status: No upgrade currently in progress
Config File Status: File wgs wd.cfg downloaded from 10.1.1.1
27 Fixed Ethernet/IEEE 802.3 interface(s)
Base Ethernet Address: 00-90-86-73-33-40
wg_sw_a#
```

Ejemplo 5.18. La salida del comando `show versión` muestra información del hardware y del software IOS.

Como muestra el Ejemplo 5.18, el comando `show versión` contiene información importante relativa a la operatividad del software del switch, incluido el número de versión, información de la memoria y tiempo de actividad.

Administración de archivos de configuración del switch

Es importante también tener la posibilidad de administrar los archivos de configuración del switch. Resulta muy útil poder copiar dichos archivos en o desde un servidor TFTP.

Se utiliza el comando EXEC privilegiado `copy nvram tftp` para cargar la configuración actualmente en ejecución en un servidor TFTP. La sintaxis correcta es la que se muestra a continuación:

```
wg_sw_a#copy nvram tftp://host/archivo_destino
```

Por ejemplo, para cargar el archivo de configuración en uso del Switch A en un servidor TFTP con dirección IP 10.1.1.1, asignando el nombre `wgs wd.cfg` al archivo de destino, podría introducir el siguiente comando:

```
wg_sw_a#copy nvram tftp://10.1.1.1/wgs wd.cfg
```

Configuration upload is successfully completed

Se utiliza el comando EXEC privilegiado `copy tftp nvram` para descargar un archivo de configuración de un servidor TFTP. La sintaxis de esta orden es como se indica a continuación:

`wg_sw_a#copy tftp://host/archivo origen nvram`

Por ejemplo, para descargar un archivo de configuración del servidor TFTP con dirección IP 10.1.1.1 en la NVRAM del Switch A, podría introducir el siguiente comando:

`wg_sw_a#copy tftp://10.1.1.1/wgswd.cfg nvram`

TFTP successfully downloaded configuration file

NOTA: En el Catalyst 1900, la configuración en ejecución se guarda en NVRAM de forma automática cada vez que se produce un cambio en la configuración actual.

Resumen de comandos del switch Catalyst 1900

En la Tabla 5.11 se ofrece un listado de algunos de los comandos más útiles examinados en este trabajo.

| Comando | Descripción |
|---|--|
| <code>ip address dirección máscara</code> | Establece la dirección IP para la administración dentro de banda del switch. |
| <code>ip default-gateway</code> | Configura la gateway predeterminada para poder acceder a la interfaz de administración desde una red remota. |
| <code>Show ip</code> | Muestra la configuración de direcciones IP |
| <code>Show interfaces</code> | Muestra información sobre las interfaces |
| <code>mac-address-table permanent dirección mac tipo módulo/puerto</code> | Establece una dirección MAC permanente |
| <code>mac-address-table restricted static dirección mac tipo módulo/puerto lista interfaces origen</code> | Establece una dirección MAC estática restringida |
| <code>port secure [max-mac-count contador]</code> | Establece seguridad para un puerto |
| <code>Show mac-address-table (security)</code> | Muestra la tabla de direcciones MAC. La opción security hace que se muestre información acerca de la configuración estática o restringida. |
| <code>address Violation</code> | Establece la acción a llevar a cabo por el switch cuando se produce una violación de dirección de seguridad. |
| <code>Show versión</code> | Muestra información sobre la versión |
| <code>copy tftp://10.1.1.1/config.cfg nvram</code> | Copia un archivo de configuración del servidor TFTP con dirección IP 10.1.1.1. |
| <code>copy nvram tftp://10.1.1.1/Config.Cfg</code> | Guarda un archivo de configuración en el servidor TFTP con dirección IP 10.1.1.1. |
| <code>delete nvram</code> | Borra todos los parámetros de configuración y regresa a la configuración de fábrica predeterminada. |

Tabla 5.11 Comandos para la configuración del switch Catalyst 1900.

Glosario de términos

100Base-FX: Especificación Fast Ethernet de banda base de 100 Mbps que utiliza dos hebras de cable de fibra óptica multimodo por enlace. Para garantizar una correcta temporización de la señal, un enlace 100BaseFX no puede superar los 400 metros de longitud. Se basa en el estándar IEEE 802.3.

100Base-TX: Especificación Fast Ethernet de banda base de 100 Mbps que utiliza dos pares de cableado UTP o STP. El primer par de cables se utiliza para recibir datos y el segundo para transmitir. Para garantizar una correcta temporización de las señales, un segmento 100 BaseTX no puede superar los 100 metros de longitud. Se basa en el estándar IEEE 802.3. V

10Base2: Especificación Ethernet de banda base de 10 Mbps que utiliza un cable coaxial delgado de 50 ohmios. 10Base2, que forma parte de la especificación IEEE 802.3, tiene un límite de distancia de 185 metros por segmento.

10Base5: Especificación Ethernet de banda base de 10 Mbps que utiliza un cable coaxial de banda base estándar (grosso) de 50 ohmios. 10Base5 forma parte de la especificación de capa física de banda base IEEE 802.3 y tiene un límite de distancia de 500 metros por segmento.

10Base-T: Especificación Ethernet de banda base de 10 Mbps que utiliza dos pares de cableado de par trenzado (Categoría 3, 4 ó 5): un par para transmitir datos y otro para recibirlos. 10BaseT, que forma parte de la especificación IEEE 802.3, tiene un límite de distancia aproximado de 100 metros por segmento.

10Broad36: Especificación Ethernet de banda ancha de 10 Mbps que utiliza cable coaxial de banda ancha. 10Broad36 forma parte de la especificación IEEE 802.3 y tiene un límite de distancia de 3600 metros por segmento.

Algoritmo del árbol de extensión (spanning tree algorithm): Algoritmo usado para impedir ciclos o bucles de puenteo mediante la creación de un árbol de extensión

Ancho de Banda: La máxima cantidad de datos que un cable de red puede transportar, medido en bits por segundo (bps). Anchura de la banda de paso de un canal de comunicación. El ancho de banda de la voz humana es de 9.97 Khz (30 a 10Khz). El oído puede escuchar de 20 a 20 Khz (ancho de banda d 19.98 Khz). (ver pag 8 RDSI para el bucle local *)

API (Application Programming Interface): Interfaz para programas de aplicación. Especificación

de convenciones de llamadas a funciones para definir la interfaz con un usuario

Aprendizaje de la dirección MAC: Servicio que caracteriza a un switch de aprendizaje en el que se guarda la dirección MAC origen de cada paquete recibido, de modo que los paquetes que se envían en el futuro a esa dirección se pueden enviar solamente a la interfaz de switch en la que está ubicada esa dirección. Los paquetes cuyo destino son direcciones de broadcast o multicast no reconocidas se envían desde cada interfaz de switch salvo la de origen. Este esquema ayuda a reducir el tráfico en las LAN conectadas. El aprendizaje de las direcciones MAC se define en el estándar IEEE 802.1.

Árbol de extensión (spanning tree): Grupo de dispositivos sin bucles en una red

ARP (Protocolo de Resolución de Direcciones): Protocolo de Internet que se utiliza para asignar una dirección IP a una dirección MAC. Se define en RFC 826.

ARPANET: Red de la Agencia de proyectos de Investigación Avanzada. Una red de conmutación de paquetes de gran importancia establecida en 1969. ARPANET fue desarrollada durante los años 70 financiada por ARPA (y luego DARPA). Con el tiempo dio origen a la Internet. El término ARPANET se declaró oficialmente en desuso en 1990.

ARQ (Automatic Repeat Request): Pedido automático de repetición. Técnica de comunicaciones en la cual el receptor detecta errores y solicita retransmisiones

ASCII (American Standar Code for Information Interchange): Código estándar norteamericano para intercambio de información. Código de ocho bits para representar caracteres.

ASIC -Circuitos Integrados Específicos de Aplicaciones Tecnología que permite que un chip de silicio pueda ser programado para realizar una función específica durante el proceso de fabricación

ATM (Modo de Transferencia Asíncrona): Estándar internacional para relay de celdas en el que varios tipos de servicios (por ejemplo, transmisión de voz, vídeo o datos) se transmiten en celdas de longitud fija (53 bytes). Las celdas de longitud fija permiten que el procesamiento de las celdas se produzca en el hardware, reduciendo así los retardos de tránsito. ATM se encuentra diseñado para aprovechar los medios de transmisión de alta velocidad como E3, SONET y T3.

Banda ancha: Técnica de transmisión de alta velocidad y alta capacidad que permite la transmisión integrada y simultánea de diferentes tipos de señales (voz, datos, imágenes, etcétera).

Banda base: Característica de la tecnología de las redes en donde sólo se emplea una frecuencia portadora. La banda base se diferencia de la banda amplia, en la cual se emplean múltiples frecuencias portadoras. Ethernet es un ejemplo de red en banda base

Banda de paso: La banda de paso en un canal es el rango de frecuencias que pueden ser

transportadas por ese canal

BPDU (Unidad de Datos de Protocolo de Puente): Paquete del protocolo árbol de extensión que se envía a intervalos configurables para intercambiar información entre los switches de la red.

Bucle local: cable de un par de hilos con el que los usuarios están conectados a un central local (CO) en la red telefónica pública conmutada

Bucle: Ruta donde los paquetes nunca alcanzan su destino, sino que pasan por ciclos repetidamente a través de una serie constante de nodos de red.

Cabecera (header): Parte inicial de un paquete de datos a transmitir, que contiene la información sobre los puntos de origen y de destino de un envío y sobre el control de errores. Esta expresión se aplica con frecuencia, y de manera errónea, sólo a envío de correo electrónico, por lo que recibe el nombre de "mailheader", pero normalmente cualquier paquete de datos que se transmite de computadora a computadora contiene una "header".

CCITT: Comité Consultivo Internacional de Telegrafía y Telefonía (siglas en francés). Organización internacional que desarrolla estándares de comunicaciones, como la recomendación X.25. Actualmente ha pasado a llamarse UIT-T..

CIR (Committed Information Rate): Tasa comprometida de información. Es el ancho de banda garantizado que un usuario obtiene de una red pública Frame Relay. Es la velocidad en bits por segundo, a la que el switch Frame Relay acepta transferir datos.

CLI: Interfaz de línea de comandos. Método que nos permite acceder al sistema operativo para configurar los dispositivos Cisco a través de una consola

CODEC (Codificador-Decodificador): Dispositivo que realiza la conversión de una señal analógica a digital por medio de la técnica de muestreo

Colisión: En Ethernet, el resultado de dos nodos que transmiten simultáneamente. Las tramas de cada dispositivo impactan y se dañan cuando se encuentran en el medio físico.

Congestión : Tráfico que supera la capacidad de la red.

Comutación : Proceso de interconexión de dos dispositivos en una red usando recursos compartidos. En toda red, las unidades de datos deben conmutarse a través de varios dispositivos intermedios hasta que se entregan a sus destinos.

Comutación de circuito : Sistema de conmutación en el que un circuito físico dedicado debe existir entre el emisor y el receptor durante la "llamada". Se usa ampliamente en la red de la compañía telefónica.

Commutación de paquetes: : Método de transmisión de datos en una red en el cual los nodos comparten el ancho de banda entre sí enviando paquetes en forma intermitente. En contraste, una red de conmutación de circuitos dedica un circuito a la vez para la transmisión de datos.

Costo: Valor arbitrario, basado normalmente en el número de saltos, ancho de banda del medio, u otras medidas, que es asignado por un administrador de red y utilizado para comparar diversas rutas a través de un entorno de internetwork de redes. Los valores de costo utilizados por los protocolos de enrutamiento determinan la ruta más favorable hacia un destino en particular; cuanto menor el costo, mejor es la ruta

CRC (Cyclic Redundancy Test): Técnica de verificación de errores en la cual el receptor del marco calcula el residuo de dividir el contenido del marco entre un divisor binario primo y lo compara con el valor previo que el nodo emisor almacenó en el marco mismo

CSMA/CD (Carrier Sense Multiple Acces with Collision): Detección. Acceso múltiple con detección de portadora y detección de colisiones. Mecanismo de acceso al canal en el cual los dispositivos que desean transmitir primero verifican la existencia de portadora en el canal. Si no se detecta portadora en un lapso de tiempo, los dispositivos pueden transmitir. Si dos de ellos transmiten a la vez, ocurre una colisión, que es detectada por los dispositivos, que entonces retardan la retransmisión por un período aleatorio. el acceso CSMA/CD es empleado por ethernet.

CSU/DSU: Unidad de servicio de canal/unidad de servicio de datos. Dispositivo de interfaz digital que conecta el equipamiento del usuario final al par telefónico digital local.

Datagrama: Agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual. Los datagramas IP son las unidades de información primaria de la Internet. Los términos celda, trama, mensaje, paquete y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos

Demultiplexión: Separación en múltiples corrientes de entrada que han sido multiplexadas en una señal física común en múltiples corrientes de salida. Ver también multiplexión

Difusión (Broadcast): Paquete de datos enviado a todos los nodos de una red. Los broadcasts se identifican por una dirección broadcast. Comparar con multicast y unicast. Ver también dirección broadcast, dominio de broadcast y tormenta de broadcast.

Dirección de red : Dirección de capa de red que se refiere a un dispositivo de red lógico, en lugar de físico. También denominada dirección de protocolo

Dirección de subred : Parte de una dirección IP especificada como la subred por la máscara de subred.

Dirección IP : Dirección de 32 bits asignada a los hosts mediante TCP/IP. Una dirección IP corresponde a una de cinco clases (A, B, C, D o E) y se escribe en forma de 4 bytes separados por puntos (formato decimal con punto). Cada dirección consta de un número de red, un número opcional de subred, y un número de host. Los números de red y de subred se utilizan conjuntamente para el enrutamiento, mientras que el número de host se utiliza para el direccionamiento a un host individual dentro de la red o de la subred. Se utiliza una máscara de subred para extraer la información de la red y de la subred de la dirección IP. También denominada dirección de Internet (dirección IP)

Dirección MAC (Control de Acceso al Medio) : Dirección de capa de enlace de datos estandarizada que se necesita para cada puerto o dispositivo que se conecta a una LAN. Otros dispositivos de la red usan estas direcciones para ubicar dispositivos específicos en la red y para crear y actualizar las tablas de enrutamiento y las estructuras de los datos. Las direcciones MAC tienen 6 bytes de largo, y son controladas por el IEEE. También se denominan direcciones de hardware, dirección de capa MAC o dirección física. Comparar con dirección de red.

DoD (Departamento de Defensa) : Organización gubernamental de los EE.UU. responsable por la defensa nacional. El Departamento de Defensa ha financiado con frecuencia el desarrollo de protocolos de comunicación.

Dominios de colisión: En Ethernet, el área de la red en la que las tramas que colisionan se propagan. Los dispositivos conectados al mismo medio físico se encuentran en un dominio de difusión. Los repetidores y los hubs propagan las colisiones, mientras que los switches de LAN y routers no lo hacen..

Dominios de difusión (Dominio de broadcast) : Conjunto de todos los dispositivos que reciben tramas de broadcast que se originan en cualquier dispositivo dentro de ese conjunto. Los dominios de broadcast normalmente se encuentran limitados por routers porque los routers no envían tramas de broadcast. Ver también Difusión (Broadcast)

DSAP (Destintion Access PointDSAP): Punto de acceso al servicio destino. SAP del nodo de red designado en el campo Destino de un paquete. Comparar con SSAP. Ver también SAP (punto de acceso al servicio).

E1: Esquema de transmisión digital de área amplia utilizado especialmente en Europa, que lleva datos a una velocidad de 2,048 Mbps (32 canales de 64kbs multiplexados). Las líneas E1 pueden ser dedicadas para el uso privado de carriers comunes.

EBCDIC (Extended Binary Coded Decimal Interchange Code): Código extendido de intercambio decimal binario. Código de caracteres de 8 bits desarrollado por IBM para representntación de datos en sus grandes sistemas de cómputo

Encapsulación: Colocación en los datos de un encabezado de protocolo en particular. Por ejemplo, a los datos de capa superior se les coloca un encabezado específico de Ethernet antes de iniciar el tránsito de red. Además, al puentear redes que no son similares, toda la trama de una red se puede ubicar simplemente en el encabezado usado por el protocolo de capa de enlace de datos de la otra red. Ver también tunneling.

Enlace dedicado : Enlace de comunicaciones que se reserva indefinidamente para transmisiones, en lugar de conmutarse según lo requiera la transmisión.

Enlace punto a punto : Enlace que proporciona una sola ruta preestablecida de comunicaciones de WAN desde las instalaciones del cliente a través de una red de carrier, como, por ejemplo, la de una compañía telefónica, a una red remota. También denominado **enlace dedicado**

Ethernet: Especificación de 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 funcionan con una variedad de tipos de cable a 10 Mbps. Ethernet se asemeja a la serie de estándares IEEE 802.3.

Fast Ethernet: Cualquiera de varias especificaciones de Ethernet de 100-Mbps. Fast Ethernet ofrece un incremento de velocidad diez veces mayor que el de la especificación de Ethernet 10BaseT, aunque preserva características tales como formato de trama, mecanismos MAC, y MTU. Estas similitudes permiten el uso de herramientas de administración de red y aplicaciones 10BaseT existentes en redes Fast Ethernet. Se basa en una extensión de la especificación IEEE 802.3.

FDDI. (Interfaz de datos distribuida por fibra):: Estándar de LAN, definido por ANSI X3T9.5, que especifica una red de transmisión de tokens de 100 Mbps que utiliza cable de fibra óptica, con distancias de transmisión de hasta 2 km. FDDI usa una arquitectura de anillo doble para brindar redundancia

FDM. Multiplexación por división de frecuencia: Metodo de transmisión de varias señales analógicas en un canal común en el que se divide las frecuencias disponibles entre todos los usuarios, y cada usuario tiene asignado un canal todo el tiempo que sea necesario

Foro ATM : Organización internacional fundada en 1991 de forma conjunta por Cisco Systems, NET/ADAPTIVE, Northern Telecom y Sprint, con el fin de desarrollar y promover acuerdos de implementación basados en estándares para tecnología de ATM. El Foro ATM expande los estándares oficiales desarrollados por ANSI y UIT-T, y desarrolla acuerdos de implementación antes de los estándares oficiales.

Frame Relay: Es una norma para redes de área extensa de conmutación de paquetes y banda ancha. Frame relay no se encarga de la corrección de errores ni del control de flujo (como en

X.25). Se limita a detectar los errores, a descartar los marcos y a notificar los errores a los protocolos de las capas superiores. Frame Relay es más eficiente que X.25, el protocolo para el cual se considera por lo general un reemplazo

FRI -Frame Relay Interlece

FTP (Protocolo de Transferencia de Archivos) : Protocolo de aplicación, parte de la pila de protocolo TCP/IP, utilizado para transferir archivos entre nodos de red. FTP se define en la RFC 959.

Full-duplex. Capacidad para la transmisión simultánea de datos entre la estación emisora y la estación receptora.

Gateway: .En la comunidad IP, término antiguo que se refiere a un dispositivo de enrutamiento. Actualmente, el término router se utiliza para describir nodos que desempeñan esta función, y gateway se refiere a un dispositivo especial que realiza conversión de capa de aplicación de la información de una pila de protocolo a otro

Half-duplex: Capacidad de transmisión de datos en una sola dirección a la vez entre una estación transmisora y otra receptora.

Host: Computador en una red. Similar a nodo, salvo que el host normalmente implica un computador, mientras que nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores y routers.

HUB: Dispositivo de la capa física que permite la concentración de muchos dispositivos Ethernet en un dispositivo centralizado. Todos los dispositivos conectados al hub comparten el mismo medio, y en consecuencia, comparten los mismos dominios de colisión, dominio de difusión y ancho de banda.1 En general, dispositivo que sirve como centro de una topología en estrella. También denominado repetidor multipuerto. 2. Dispositivo de hardware o software que contiene múltiples módulos de red y equipos de red independientes pero conectados. Los hubs pueden ser activos (cuando repiten señales que se envían a través de ellos) o pasivos (cuando no repiten, sino que simplemente dividen las señales enviadas a través de ellos).

IEEE 802.3: Protocolo IEEE para LAN que especifica la implementación de la capa física y de la subcapa MAC de la capa de enlace de datos. IEEE 802.3 utiliza el acceso CSMA/CD a varias velocidades a través de diversos medios físicos. Las extensiones del estándar IEEE 802.3 especifican implementaciones para Fast Ethernet. Las variaciones físicas de la especificación IEEE 802.3 original incluyen 10Base2, 10Base5, 10BaseF, 10BaseT y 10Broad36. Las variaciones físicas para Fast Ethernet incluyen 100BaseTX y 100BaseFX.

IEEE 802.5: Protocolo de LAN de IEEE que especifica la implementación de la capa física y la subcapa MAC de la capa de enlace de datos. IEEE 802.5 usa acceso de transmisión de tokens a 4

ó 16 Mbps en cableado STP o UTP y desde el punto de vista funcional y operacional es equivalente a Token Ring de IBM. Ver también Token Ring.

IEEE: Organización profesional cuyas actividades incluyen el desarrollo de estándares de comunicaciones y redes. Los estándares de LAN de IEEE son los estándares de mayor importancia para las LAN de la actualidad.

IETF(Fuerza de Tareas de Ingeniería de Internet): Fuerza de tareas compuesta por más de 80 grupos de trabajo responsables por el desarrollo de estándares de Internet.

Interredes (Internetworking): Agrupamiento de redes interconectadas por routers y otros dispositivos que funciona (de modo general) como una sola red.

Inundación (flooding): Técnica de transmisión de tráfico utilizada por switches y puentes, en la cual el tráfico recibido por una interfaz se envía a todas las interfaces de ese dispositivo, salvo a la interfaz desde la cual se recibió originalmente la información.

IOS Software Cisco IOS (Sistema Operativo de Internetwork): Software de sistema de Cisco que proporciona funcionalidad, escalabilidad y seguridad comunes a todos los productos bajo la arquitectura Cisco fusión. El software Cisco IOS permite la instalación y administración centralizada, integrada y automatizada de internetwork, garantizando al mismo tiempo la compatibilidad con una amplia variedad de protocolos, medios, servicios y plataformas.

ISO (Organización Internacional para la Normalización) : Organización internacional que tiene a su cargo una amplia gama de estándares, incluyendo aquellos referidos al networking. ISO desarrolló el modelo de referencia OSI, un modelo popular de referencia de networking

ITU-T. International Telecommunication Union Sector de normalización de las telecomunicaciones . Comité de la ITU que crea recomendaciones respecto a la telegrafía, telefonía y redes de datos públicas originado originalmente en 1965 como Comité consultivo internacional de telegrafía y telefonía (CCITT)

LAN (red de área local): Red de datos de alta velocidad y bajo nivel de errores que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LAN conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un solo edificio u otra área geográficamente limitada. Los estándares de LAN especifican el cableado y señalización en las capas físicas y de enlace de datos del modelo OSI. Ethernet, FDDI y Token Ring son tecnologías LAN ampliamente utilizadas

LAPB (Link Access Procedures Balance): Procedimiento de Acceso al Enlace Balanceado Protocolo de capa de enlace de datos en la pila de protocolo X.25. LAPB es un protocolo orientado a bit derivado de HDLC.

Latencia: Retardo entre el momento en que un dispositivo solicita acceso a una red y el momento en que se le concede el permiso para transmitir. Intervalo de tiempo que toma el procesamiento de una tarea.

LLC (Logical Link Control): Control de enlace lógico. La más alta de las dos subcapas de enlace de datos definidas por el IEEE. La subcapa LLC maneja el control de errores, control del flujo, entramado y direccionamiento de subcapa MAC. El protocolo LLC más generalizado es IEEE 802.2, que incluye variantes no orientado a conexión y orientadas a conexión.

MAC (Medium Access Control): Control de Acceso al Medio. Parte de la capa de enlace de datos que incluye la dirección de 6 bytes (48 bits) del origen y del destino, y el método para obtener permiso para transmitir.

Máscara de subred: Máscara utilizada para extraer información de red y subred de la dirección IP.

Multidifusión (Multicast): Paquetes únicos copiados por una red y enviados a un conjunto de direcciones de red. Estas direcciones están especificadas en el campo de dirección del destino. Comparar con broadcast y unicast.

Multiplexión: Esquema que permite que varias señales lógicas se transmitan de forma simultánea a través de un canal físico exclusivo. Comparar con demultiplexión.

NFS (Network File System): Se utiliza comúnmente para designar un conjunto de protocolos de sistema de archivos distribuido, desarrollado por Sun Microsystems, que permite el acceso remoto a archivos a través de una red. En realidad, NFS es simplemente un protocolo del conjunto.

NIC (Network Interface Card). Tarjeta que brinda capacidades de comunicación de red hacia y desde un computador. También denominada adaptador

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

PAD Ensamblador - Desensamblador de paquetes. Interfaz entre los dispositivos de un cliente y una red X25.

Paquete : Agrupación lógica de información que incluye un encabezado que contiene la información de control y (generalmente) los datos del usuario. Los paquetes se usan a menudo para referirse a las unidades de datos de capa de red. Los términos datagrama, trama, mensaje y segmento también se usan para describir agrupamientos de información lógica en las diversas capas del modelo de referencia OSI y en varios círculos tecnológicos.

PDU: Unidad de datos de protocolo. Término OSI equivalente a paquete

POST: Pruebas al inicio. Conjunto de diagnósticos de hardware que se ejecutan en un dispositivo de hardware cuando se enciende.

Puente: Dispositivo que conecta dos segmentos de una red y pasa por paquetes entre ellos. Los puentes operan en el nivel 2 del modelo de referencia OSI y nos son sensibles a los protocolos de niveles superiores.

Puerto AUI: El término AUI hace referencia al puerto del panel posterior al que se puede conectar un cable AUI, como los que se encuentran en los dispositivos Cisco

PVC (Circuito virtual permanente): Circuito virtual que se establece de forma permanente. Este tipo de servicio se establece en tiempo de suscripción y permanece disponible durante una cantidad de tiempo predeterminado, no se requiere procedimientos de establecimiento o terminación de llamada para usar un PVC. Los PVC son soportados por Frame Relay y X.25, y ATM. Comparar con SVC.

RDSI : Red digital de servicios integrados. Red digital que proporciona una amplia variedad de servicios de comunicaciones, un conjunto estándar de mensajes usuario-red y acceso integrado a la red. Protocolo de comunicaciones que ofrecen las compañías telefónicas y que permite que las redes telefónicas transmitan datos, voz y tráfico de otros orígenes.

Repetidor: Dispositivo que regenera y propaga las señales eléctricas entre dos segmentos de red.

Router: Dispositivo de capa de red que usa una o más métricas para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes de una red a otra basándose en la información de capa. Denominado a veces gateway (aunque esta definición de gateway se está volviendo obsoleta).

SAP: Protocolo de Publicación de Servicio. Protocolo IPX que suministra un medio para informar a los clientes, a través de routers y servidores, acerca de los recursos y los servicios de red disponibles.

Segmentación : Proceso de división de un solo dominio de colisión en dos o más dominios de

colisión para reducir las colisiones y la congestión de la red

Simplex (Unidireccional): Capacidad de transmisión en una sola dirección entre una estación emisora y una estación receptora. La televisión es un ejemplo de tecnología unidireccional. Comparar con full dúplex y semidúplex.

SNMP (Protocolo simple de administración de redes): Protocolo de administración de redes utilizado casi con exclusividad en redes TCP/IP. El SNMP brinda una forma de monitorear y controlar los dispositivos de red y de administrar configuraciones, recolección de estadísticas, desempeño y seguridad.

SONET Synchronous Optical Network.

SONET: Synchronous Optical Network. Red Óptica Síncrona. Jerarquía de portadoras digitales basadas en fibra óptica; el incremento base es 51.84 Mbps y es referido como una portadora óptica 1(OC-1) (OC- Optical Carrier) hasta OC-48 de 2.5 Gbps. Este estándar se especifica para los Estados Unidos, y sus equivalente internacional (Europa) es conocido como la Jerarquía Digital Síncrona (SDH). La principal diferencia de formato entre las dos es que la velocidad básica es SDH es de 155.52 Mbps (STM-1)

SSAP (Source Service Access Point): Punto de acceso al servicio origen. SAP del nodo de red designado en el campo Origen de un paquete. Comparar con DSAP. Ver también SAP.

SVC (Circuito virtual conmutado): Circuito virtual que se establece de forma dinámica a pedido y que se desconecta cuando la transmisión se completa. Los SVC se usan en situaciones en las que la transmisión de datos es esporádica. Este tipo de servicio requiere de procedimientos de control de llamada para el establecimiento y la liberación de la llamada. Los SVC son soportados por frame Relay y X.25, y son llamados *conexiones bajo demanda* en ATM.

Switch: Dispositivo que conecta computadoras. El switch actúa de manera inteligente. Puede agregar ancho de banda, acelerar el tráfico de paquetes y reducir el tiempo de espera. Los switches son más "inteligentes" que los "Hubs" y ofrecen un ancho de banda más dedicado para los usuarios o grupos de usuarios. Un switch envía los paquetes de datos solamente a la computadora correspondiente, con base en la información que cada paquete contiene. Para aislar la transmisión de una computadora a otra, los switches establecen una conexión temporal entre la fuente y el destino, y la conexión termina una vez que la conversación se termina.

Switch LAN: Switch de alta velocidad que envía paquetes entre segmentos de enlace de datos. La mayoría de los switches de LAN envían tráfico basándose en las direcciones MAC. Los switches LAN a menudo se clasifican según el método utilizado para enviar tráfico: conmutación de paquetes por método de corte o conmutación de paquetes por almacenamiento y envío. Un

ejemplo de switch de LAN son los Cisco Catalyst .

T1: Servicio de portadora digital que transmite datos formateados DS-1 a 1,544 Mbps (24 canales de 64kbs multiplexados) a través de la red de conmutación telefónica, usando la codificación AMI o B8ZS. Comparar con E1.

Tabla de envío (Buffer de memoria) : Área de la memoria donde el switch almacena los datos destino y de transmisión.

TCP. (Protocolo de Control de Transmisión) : Protocolo de capa de transporte orientado a conexión que provee una transmisión confiable de datos de dúplex completo. TCP es parte de la pila de protocolo TCP/IP.

TCP/IP (Protocolo de Control de Transmisión /Protocolo Internet) : Nombre común para el conjunto de protocolos desarrollados por el DoD de EE.UU. en los años '70 para promover el desarrollo de internetwork de redes a nivel mundial. TCP e IP son los dos protocolos más conocidos del conjunto.

Telnet: Protocolo de emulación de terminal estándar de la pila de protocolo TCP/IP. Telnet se usa para la conexión de terminales remotas, permitiendo que los usuarios se registren en sistemas remotos y utilizan los recursos como si estuvieran conectados a un sistema local.

TFTP (Protocolo de Transferencia de Archivos Trivial) : Versión simplificada de FTP que permite la transferencia de archivos de un computador a otro a través de una red.

Token Ring: LAN de transmisión de tokens desarrollada y soportada por IBM. Token Ring se ejecuta a 4 ó 16 Mbps a través de una topología de anillo. Similar a IEEE 802.5.

Tormenta de difusión (Tormenta de broadcast): Suceso de red no deseado, en el que se envían varios broadcasts simultáneamente a todos los segmentos de red. Una tormenta de broadcast usa una parte considerable del ancho de banda de la red y normalmente hace que se agoten los tiempos de espera de la red.

UDP (Protocolo de Datagrama de Usuario): Protocolo no orientado a conexión de la capa de transporte de la pila de protocolo TCP/IP. UDP es un protocolo simple que intercambia datagramas sin confirmación o garantía de entrega y que requiere que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos.

UNI (Interfaz de Red a Usuario): Especificación que define un estándar de interoperabilidad para la interfaz entre productos (un router o un switch) ubicados en una red privada y los switches ubicados dentro de las redes de carriers públicas. También utilizado para describir conexiones similares en redes Frame Relay.

Unidifusión. (unicast) : Mensaje que se envía a un solo destino de red.

UTP (Par trenzado no blindado) : Medio de cable de cuatro pares que se emplea en varias redes.. Hay cinco tipos de cableado UTP de uso común: cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4 y cableado de Categoría 5.

VC (Círculo virtual): En redes de almacenamiento y reenvío (redes de conmutación de paquetes) es la conexión extremo a extremo lógica entre dos host; el VC debe ser establecido por el usuario en tiempo de suscripción o bajo demanda, pero la red no dedica recursos de transmisión para esta conexión.

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

X.25 : Es una red de datos de conmutación de paquetes, los dispositivos se comunican a través de ella estableciendo circuitos virtuales ya sea de duración limitada o dedicados. Proviene de una época en que las líneas digitales eran lentas y poco fiables por lo que el protocolo X.25 se encarga de la detección de errores y de su corrección. Frame Relay ha reemplazado en cierta medida a X.25.

Conclusiones.

La configuración del Switch Cisco Catalyst 1900 fue un buen tema de investigación que me permitió desarrollar y ampliar los conocimientos adquiridos en el seminario de titulación.

Al seleccionar el material para la realización de éste trabajo se ha intentado ofrecer la información que nos permita comprender los conceptos sobre las tecnologías para la interconexión de las redes de computadoras.

En éste trabajo se presentan los conceptos, comandos y prácticas necesarias para configurar los switches. Para entender la terminología que implica la configuración de un Switch se llevó a cabo una revisión, desde los conceptos generales sobre redes, hasta el proceso por el cual los datos son transferidos desde una aplicación a través de la red.

Se presentan las funciones de los distintos dispositivos para la interconexión de redes, como son los Repetidores, Concentradores (hub's), Puentes, Conmutadores (Switches) y Routers. Todo lo anterior se explica mediante el modelo de referencia OSI.

Se pretende que este trabajo sirva, ante todo, como un referencia general para todos aquellos estudiantes y profesores interesados en el tema.

Finalmente quiero agradecer a las personas que me apoyaron y animaron para la realización de este trabajo que me permitió, finalmente, obtener el título Ingeniero Mecánico Electricista.

José Ignacio Chávez Saladino

Referencias.

Interconexión de dispositivos de red cisco

Steve McQuerry

CISCOPRESS

Routers Cisco

Joe Habraken

Prentice Hall

Redes con Microsoft TCP/IP

Drew Heywood

Prentice may

Telecomunicaciones para PC

John C. Dvorak

McGraw Hill

RDSI, Conceptos, funciones y servicios

Gary Kessler, Peter Southwick

McGraw Hill

<http://www.cisco.com>

<http://www.Itnetworking\Catalyst\Catalyst 1900 Series Installation and Configuration Guide.htm>

<http://www.Itnetworking\Catalyst\Howstuffworks How LAN Switches Work.htm>

<http://www.Itnetworking\Catalyst\Quick Start Guide Catalyst 1900 Series Ethernet Switches.htm>

<http://www.Cisco Small Medium Business Center - Networking Essentials for Small Businesses.htm>

<http://www.HowEverythingWorks\How LAN Switches Work.htm>