UNIVERSIDAD NACIONAL AUTONOMA
DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
CUAUTITLÁN

INTERCONEXIÓN DE REDES

TESIS

QUE PARA OBTENER EL TITULO DE:

INGENIERO MECANICO ELECTRICISTA

P R E S E N T A:

JUAN CARLOS RAMOS FLORENTINO

ASESOR:ING. JOSE LUIS RIVERA LOPEZ

CUAUTITLAN IZCALLI, EDO. DE MEX. 2008

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

ASUNTO: EVALUACION DEL INFORME
DEL DESARROLLO PROFESIONAL

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN

DEPARTAMENTO DE EXAMENES PROFESIONALES

DRA. SUEMI RODRIGUEZ ROMO
DIRECTOR DE LA FES CUAUTITLAN
P R E S E N T E

ATN: L. A. ARACELI HERRERA HERNANDEZ
Jefe del Departamento de Exámenes
Profesionales de la FES Cuautitlán

Con base en el art. 26 del Reglamento General de Exámenes y el art. 66 del Reglamento de Exámenes Profesionales de FESC. nos permitimos comunicar a usted que revisamos LA TESIS

Interconexion de Redes

que presenta el pasante: Juan Carlos Ramos Florentino
con número de cuenta: 09635885-2 para obtener el título de :
Ingeniero Mecanico Electricista

Considerando que dicho trabajo reune los requisitos necesarios, otorgamos nuestra ACEPTACION

A T E N T A M E N T E
"POR MI RAZA HABLARA EL ESPIRITU"
Cuautitlán Izcalli, Méx. a 29 de Julio de 2008

PRESIDENTE	Ing. Jose Luis Rivera Lopez	
VOCAL	M.C. Vicente Magaña Gonzalez	
SECRETARIO	Ing. Jose Luis Barbosa Pacheco	
PRIMER SUPLENTE	Ing. Luis Raul Flores Coronel	
SEGUNDO SUPLENTE	Ing. Fernando Patlan Vargas	

AGRADECIMIENTOS

Este trabajo se lo dedico de forma muy especial a mi madre, por todo el apoyo que me ha brindado en todo momennto, por confiar siempre en mi y por tenerme tanta paciencia.

“Gracias mamá por tu gran ejemplo de siempre trabajar para lograr lo que se quiere.”

A Mary:

Por esperarme todo este tiempo con amor y paciencia y por sus palabras de aliento que no dejaron caer mi animo, por que siempre ha estado a mi lado.

A mi hermano:

Porque siempre esta conmigo cuando lo necesito y por que siempre ha creído en mí

A mis profesores:

Por ayudarme a cumplir mi meta.

Y en general a todos aquellos amigos que de una u otra manera han estado conmigo ayudándome a dar un paso mas.

INDICE

PRÓLOGO

El objetivo de la siguiente tesis es presentar los conceptos básicos de los sistemas utilizados en las redes de comunicaciones convencionales y tratar de ampliar estos conceptos con los sistemas de redes mas modernos que se están desarrollando hoy en dia , ya que como sabemos, el continuo crecimiento de las redes de voz y datos ha propiciado el nacimiento de tecnologías que permiten brindar rapidez, flexibilidad, administración y sobre todo la integración de estos diferentes tipos de tráfico. Dentro de las tecnologías más importantes y actuales que hoy en día proporcionan todas estas características se encuentran Frame Relay, ATM, Gigabit Ethernet, y mas recientemente han aparecido tecnologías que son capaces de integrar casi cualquier tipo de trafico de forma instantánea en una sola línea como lo es RDSI.
Todas estas tecnologías se basan en la conmutación (tanto de paquetes como de celdas), por lo que en la presente Tesis se analizan las características y ventajas de las nuevas tecnologías de conmutación que nos permiten conformar una nueva generación de redes.

Hoy por hoy, el tema de las redes informáticas abarca un campo cada vez mayor de conocimientos. Incluye un amplio rango de funciones y capacidades, es por eso que en esta Tesis se tratara el tema desde los tipos básicos de señalización y los circuitos utilizados para permitir a las computadoras intercambiar datos así como las distintas topologías utilizadas para diferentes necesidades, hasta los tipos de cables (par trenzado, coaxial, fibra óptica, etc.) o técnicas inalámbricas de banda ancha utilizados para transportar datos desde el emisor al receptor.
El tema de las redes también abarca diversos conjuntos de reglas para la comunicación entre el emisor y el receptor en diversos niveles abstractos de intercambio de datos. Estos niveles van desde los simples y limitados flujos de bits empleados para enviar datos desde un emisor a un receptor, hasta los diversos esquemas de identificación, direccionamiento, encaminamiento y procesamiento de mensajes, a medida que estos viajan a través de diversos tipos de medios de transmisión. Para que las distintas redes del mundo puedan comunicarse entre sí, se ha creado un conjunto de protocolos llamados TCP/IP los cuales permiten que redes de diferentes tamaños y tecnologías puedan interconectarse sin ningún problema, ya que los paquetes IP son capaces de viajar por cualquier tipo de red.

INTRODUCCIÓN

La teoría de las redes informáticas no es algo reciente. La necesidad de compartir recursos e intercambiar información fue una inquietud permanente desde los primeros tiempos de la informática. Los comienzos de las redes de datos se remontan a los años ’60, en los cuales se perseguían exclusivamente fines militares o de defensa. Paulatinamente, estas redes se fueron adoptando para fines comerciales.

Obviamente en esa época no existían las PCs, por lo cual los entornos de trabajo resultaban centralizados y lo común para cualquier red era que el procesamiento quedara delegado a una única computadora central o main frame y los usuarios accedieran a la misma mediante terminales consistentes en sólo un monitor y un teclado.

Los tiempos han cambiado y ya prácticamente todos los usuarios acceden a los recursos desde computadoras personales. Sin embargo, la teoría, los principios básicos, los protocolos han mantenido vigencia y si bien es cierto, se va produciendo obsolescencia de parte de ellos, es muy conveniente partir de los principios y de la teoría básica. Resulta difícil comprender las redes actuales si no se conocen los fundamentos de la teoría de redes.

Comenzamos el estudio de esta tesis haciendo una definición de red así como una breve clasificación de las redes según su extensión geográfica, que como sabemos, cada uno de los tipos requiere de tecnologías y topologías específicas.

La topología de una red se refiere a la forma que ésta toma al hacer un diagrama del medio físico de transmisión y los dispositivos necesarios para regenerar la señal o manipular el tráfico. Las topologías generales son: anillo, bus, estrella, árbol y completas.

Al crear una red, se toman en cuenta dos factores principales: el medio físico de transmisión y las reglas que rigen la transmisión de datos. Al primer factor le llamamos nivel físico y al segundo protocolos.

En el nivel físico generalmente encontramos señales de voltaje que tienen un significado preconcebido. Esas señales se agrupan e interpretan para formar entidades llamadas paquetes de datos. La forma como se accesan esos paquetes determinan la tecnología de transmisión pudiendo ser difusión o punto a punto.

El modelo OSI (Open System Interconnection) es el comienzo de cualquier estudio de redes. Es un modelo idealizado de 7 capas o niveles que representa la subdivisión de tareas teórica que se recomienda tener en cuenta para el estudio o diseño de un sistema.

A cada capa se le asigna una función bien específica y las mismas se apilan desde la inferior a la superior de forma que cada una depende de la inmediata inferior para su funcionamiento.

Esto no significa que todas las redes cumplan o deban cumplir exactamente con este modelo y de hecho, normalmente no lo hacen pero de todas formas se recomienda siempre tener en cuenta el modelo OSI como referencia , ya que el conocimiento del mismo posibilita la correcta

comprensión de cualquier red e inclusive facilita el poder realizar la comparación entre sistemas diferentes.

En esta tesis estudiaremos desde el sistema X.25, que trabaja sobre redes analógicas, es decir líneas telefónicas dedicadas. Hoy en día este sistema tiene pocas aplicaciones, como por ejemplo en cajeros automáticos, validación de tarjetas de crédito, etc; pero su robustez, seguridad y confiabilidad han hecho que se mantenga como un estándar para las redes públicas y privadas durante una gran cantidad de años. Además sus principios y su teoría de funcionamiento aporta conceptos sumamente importantes que nos ayudarán a comprender el sistema Frame Relay que es una mejora de X.25 . Se trata de un sistema mucho más simple y eficiente, el cual tiene plena vigencia hoy en día en redes de área amplia. Trabaja sobre enlaces digitales generalmente punto a punto. Nos ayudara también en el mejor entendimiento del sistema de mayor auge en nuestros días, base indispensable del funcionamiento de Internet: TCP/IP.

Ya estando en este punto aprovecharemos para dar una descripción detallada de lo que es la tecnología de la voz sobre IP y la telefonía IP la cual esta teniendo un crecimiento acelerado en la época actual que a pesar de ser una tecnología muy joven ha empezado ya a revolucionar la forma de comunicarnos tanto que se prevé que aproximadamente en los próximos 10 años un 60 % de la población mundial tendrá acceso a este recurso.

Estudiaremos también la tecnología llamada Asynchronous Transfer Mode (ATM) Modo de Transferencia Asíncrona que es el corazón de los servicios digitales integrados que ofrecerán las nuevas redes digitales de servicios integrados de Banda Ancha (B-ISDN).

Por último veremos el funcionamiento de los diferentes dispositivos con que cuenta una red tales como concentradores, repetidores, puentes, routers, conmutadores, pasarelas y modems.

CAPITULO 1.

QUE ES UNA RED

1. QUE ES UNA RED

Una red de computadoras es un sistema de comunicación de datos que enlaza varias computadoras y periféricos como impresoras, sistemas de almacenamiento masivo, bibliotecas de CD-ROM, módem, fax y muchos otros dispositivos.

Al crear una red, se toman en cuenta dos factores principales: el medio físico de transmisión y las reglas que rigen la transmisión de datos. Al primer factor le llamamos nivel físico y al segundo protocolos.
En el nivel físico generalmente encontramos señales de voltaje que tienen un significado preconcebido:esas señales se agrupan e interpretan para formar entidades llamadas paquetes de datos. La forma como de accesan esos paquetes determinan la tecnología de transmisión y se aceptan dos tipos: broadcast y point-to-point.

Redes según la direccionalidad de los datos (modos de transmisión).

Simplex: la transmisión de datos es unidireccional; únicamente se puede mandar información en un sentido.

half-duplex: la transmisión de datos es posible en ambas direcciones, pero no al mismo tiempo.

full-duplex: las transmisiones se hacen en forma simultánea en ambas direcciones, pero deben ser entre las mismas dos estaciones.

1.1 Por Localización

El universo de las redes, puede clasificarse según la extensión que abarcan. Cada uno de los tipos requiere de tecnologías y topologías específicas.

1.1.1 Red de Area Personal (PAN)

Una personal área network (PAN / Red de Área Personal) es una red de ordenadores para la comunicación entre distintos dispositivos (tanto ordenadores, puntos de acceso a Internet, teléfonos móviles, PDA, dispositivos de audio, impresoras) cercanos al punto de acceso. Estas redes normalmente son de unos pocos metros y para uso personal.

Una red PAN de dispositivos Bluetooth es llamada piconet, y esta compuesta por al menos 2 dispositivos activos en una relación jerárquica (o maestro-esclavo) con un máximo de 8. El primer dispositivo Bluetooth conectado a la piconet es el maestro, y todos los demás serán los

que dependen de él (los esclavos)que se comunican con el primero. Normalmente tienen un rango de alcance de 10 metros aunque en condiciones ideales podría (teóricamente) llegar hasta los 100 metros.

1.1.2 Red de Area Local (LAN)

LAN es la abreviatura de Local Área Network (Red de Área Local o simplemente Red Local). Una red local es la interconexión de varios ordenadores y periféricos. Su extensión esta limitada físicamente a un edificio o a un entorno de unos pocos kilómetros. Su aplicación más extendida es la interconexión de ordenadores personales y estaciones de trabajo en oficinas, fábricas, etc.; para compartir recursos e intercambiar datos y aplicaciones. En definitiva, permite que dos o más máquinas se comuniquen.

En los días anteriores a los ordenadores personales, una empresa podía tener solamente un ordenador central, accediendo los usuarios a este vía terminales de ordenador sobre un cable simple de baja velocidad. Las redes como SNA de IBM (la Arquitectura de Red de Sistemas) fueron diseñadas para unir terminales u ordenadores centrales a sitios remotos sobre líneas alquiladas. Las primeras LAN fueron creadas al final de los años 1970 y se solían crear líneas de alta velocidad para conectar grandes ordenadores centrales a un solo lugar. Muchos de los sistemas fiables creados en esta época, como Ethernet y Arcnet fueron los más populares.

Ventajas

En una empresa suelen existir muchos ordenadores, los cuales necesitan de su propia impresora para imprimir informes (redundancia de Hardware), los datos almacenados en uno de los equipos es muy probable que sean necesarios en otro de los equipos de la empresa por lo que será necesario copiarlos en este, pudiéndose producir desfases entre los datos de un usuario y los de otro, la ocupación de los recursos de almacenamiento en disco se, los ordenadores que trabajen con los mismos datos tendrán que tener los mismos programas para manejar dichos datos etc. La red de área local permite compartir bases de datos, programas y periféricos como puede ser un módem, una tarjeta RDSI, una impresora, etc...; poniendo a nuestra disposición otros medios de comunicación como pueden ser el correo electrónico y el Chat. Nos permite realizar un proceso distribuido, es decir, las tareas se pueden repartir en distintos nodos y nos permite la integración de los procesos y datos de cada uno de los usuarios en un sistema de trabajo corporativo. Tener la posibilidad de centralizar información o procedimientos facilita la administración y la gestión de los equipos.

Características

Tecnología broadcast (difusión) Con el medio de transmisión compartido.

Cableado específico instalado normalmente a propósito.

Capacidad de transmisión comprendida entre 1 Mbps y 1 Gbps.

Extensión máxima no superior a 3 km (Una FDDI *puede llegar a 200 km)*

Uso de un medio de comunicación privado.

*La simplicidad del medio de transmisión que utiliza (*cable coaxial*, cables telefónicos y* fibra óptica*).*

La facilidad con que se pueden efectuar cambios en el hardware *y el* software*.*

Gran variedad y número de dispositivos conectados.

Posibilidad de conexión con otras redes.

1.1.2.1 Topología de las redes de área local

La topología de una red se refiere a la forma que ésta toma al hacer un diagrama del medio físico de transmisión y los dispositivos necesarios para regenerar la señal o manipular el tráfico. Las topologías generales son: anillo (ring), dorsal (bus), dorsal dual (dual bus), estrella (star), árbol (tree) y completas.

1.1.2.2 Topologías físicas

Una topología de bus usa un solo cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este backbone.

La topología de anillo conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.

La topología en estrella conecta todos los cables con un punto central de concentración.

Una topología en estrella extendida conecta estrellas individuales entre sí mediante la conexión de HUBs o switches. Esta topología puede extender el alcance y la cobertura de la red.

Una topología jerárquica es similar a una estrella extendida. Pero en lugar de conectar los HUBs o switches entre sí, el sistema se conecta con una computadora que controla el tráfico de la topología.

La topología de malla se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio. El uso de una topología de malla en los sistemas de control en red de una planta nuclear sería un ejemplo excelente.

También hay otra topología denominada árbol.

Componentes

- Servidor: El servidor es aquel o aquellos ordenadores que van a compartir sus recursos hardware y software con los demás equipos de la red. Sus características son potencia de cálculo, importancia de la información que almacena y conexión con recursos que se desean compartir.
- Estación de trabajo: Los ordenadores que toman el papel de estaciones de trabajo aprovechan o tienen a su disposición los recursos que ofrece la red así como los servicios que proporcionan los Servidores a los cuales pueden acceder.
- Gateways o pasarelas: Es un Hardware y software que permite las comunicaciones entre la red local y grandes ordenadores (mainframes). El gateway adapta los protocolos de comunicación del mainframe (X25, SNA, etc.) a los de la red, y viceversa.
- Bridges o puentes: Es un Hardware y software que permite que se conecten dos redes locales entre sí. Un puente interno es el que se instala en un servidor de la red, y un puente externo es el que se hace sobre una estación de trabajo de la misma red. Los puentes también pueden ser locales o remotos. Los puentes locales son los que conectan a redes de un mismo edificio, usando tanto conexiones internas como externas. Los puentes remotos conectan redes distintas entre sí, llevando a cabo la conexión a través de redes públicas, como la red telefónica, RDSI o red de conmutación de paquetes.
- Tarjeta de red: También se denominan NIC (Network Interface Card). Básicamente realiza la función de intermediario entre el ordenador y la red de comunicación. En ella se encuentran grabados los protocolos de comunicación de la red. La comunicación con el ordenador se realiza normalmente a través de las ranuras de expansión que éste dispone, ya sea ISA, PCI o PCMCIA. Aunque algunos equipos disponen de este adaptador integrado directamente en la placa base.
- El medio: Constituido por el cableado y los conectores que enlazan los componentes de la red. Los medios físicos más utilizados son el cable de par trenzado, par de cable, cable coaxial y la fibra óptica (cada vez en más uso esta última).
- Concentradores de cableado: Una LAN en bus usa solamente tarjetas de red en las estaciones y cableado coaxial para interconectarlas, además de los conectores, sin embargo este método complica el mantenimiento de la red ya que si falla alguna conexión toda la red deja de funcionar. Para impedir estos problemas las redes de área local usan concentradores de cableado para realizar las conexiones de las estaciones, en vez de distribuir las conexiones el concentrador las centraliza en un único dispositivo manteniendo indicadores luminosos de su estado e impidiendo que una de ellas pueda hacer fallar toda la red.

Existen dos tipos de concentradores de cableado:

Concentradores pasivos: Actúan como un simple concentrador cuya función principal consiste en interconectar toda la red.

Concentradores activos: Además de su función básica de concentrador también amplifican y regeneran las señales recibidas antes de ser enviadas.

Los concentradores de cableado tienen dos tipos de conexiones: para las estaciones y para unirse a otros concentradores y así aumentar el tamaño de la red. Los concentradores de cableado se clasifican dependiendo de la manera en que internamente realizan las conexiones y distribuyen los mensajes. A esta característica se le llama topología lógica.

Existen dos tipos principales:

Concentradores con topología lógica en bus (HUB): Estos dispositivos hacen que la red se comporte como un bus enviando las señales que les llegan por todas las salidas conectadas.

Concentradores con topología lógica en anillo (MAU): Se comportan como si la red fuera un anillo enviando la señal que les llega por un puerto al siguiente.

1.1.3 Red de Area Metropolitana (MAN)

Una red de área metropolitana (*Metropolitan Area Network* o *MAN*, en inglés) es una red de alta velocidad que dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado de cobre a velocidades que van desde los 2 Mbit/s hasta 155 Mbit/s.

El concepto de red de área metropolitana representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas mayores que en algunos casos no se limitan a un entorno metropolitano sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana.

Aplicaciones

Las redes de área metropolitana tienen muchas y variadas aplicaciones, las principales son:

Interconexión de redes de área local (LAN)
Interconexión de centralitas telefónicas digitales (PBX y PABX)
Interconexión ordenador a ordenador
Transmisión de vídeo e imágenes
Transmisión CAD/CAM
Pasarelas para redes de área extensa (WAN)

1.1.3.1 MAN Pública y Privada

Una red de área metropolitana puede ser pública o privada. Un ejemplo de MAN privada sería un gran departamento o administración con edificios distribuidos por la ciudad, transportando todo el tráfico de voz y datos entre edificios por medio de su propia MAN y encaminando la información externa por medio de los operadores públicos. Los datos podrían ser transportados entre los diferentes edificios, bien en forma de paquetes o sobre canales de ancho de banda fijos..

Un ejemplo de MAN pública es la infraestructura que un operador de telecomunicaciones instala en una ciudad con el fin de ofrecer servicios de banda ancha a sus clientes localizados en esta área geográfica.

VENTAJAS

Ancho de banda

El elevado ancho de banda requerido por grandes ordenadores y aplicaciones compartidas en red es la principal razón para usar redes de área metropolitana en lugar de redes de área local.

Nodos de red

Las redes de área metropolitana permiten superar los 500 nodos de acceso a la red, por lo que se hace muy eficaz para entornos públicos y privados con un gran número de puestos de trabajo.

Extensión de red

Las redes de área metropolitana permiten alcanzar un diámetro en torno a los 50 km, dependiendo el alcance entre nodos de red del tipo de cable utilizado, así como de la tecnología empleada. Este diámetro se considera suficiente para abarcar un área metropolitana. Abarcan una ciudad y se pueden conectar muchas entre sí, formando mas redes.

Distancia entre nodos

Las redes de área metropolitana permiten distancias entre nodos de acceso de varios kilómetros, dependiendo del tipo de cable. Estas distancias se consideran suficientes para conectar diferentes edificios en un área metropolitana o campus privado.

Trafico en tiempo real

Las redes de área metropolitana garantizan unos tiempos de acceso a la red mínimos, lo cual permite la inclusión de servicios síncronos necesarios para aplicaciones en tiempo real, donde es importante que ciertos mensajes atraviesen la red sin retraso incluso cuando la carga de red es elevada. Entre nodo y nodo no se puede tener, por ejemplo más de 100 kilómetros de cable.

Integración de voz/datos/vídeo

Los servicios síncronos requieren una reserva de ancho de banda; tal es el caso del tráfico de voz y vídeo. Por este motivo las redes de área metropolitana son redes óptimas para entornos de tráfico multimedia, si bien no todas las redes metropolitanas soportan tráficos isócronos (transmisión de información a intervalos constantes).

Alta disponibilidad

Disponibilidad referida al porcentaje de tiempo en el cual la red trabaja sin fallos. Las redes de área metropolitana tienen mecanismos automáticos de recuperación frente a fallos, lo cual permite a la red recuperar la operación normal después de uno. Cualquier fallo en un nodo de acceso o cable es detectado rápidamente y aislado. Las redes MAN son apropiadas para entornos como control de tráfico aéreo, aprovisionamiento de almacenes, bancos y otras aplicaciones comerciales donde la indisponibilidad de la red tiene graves consecuencias.

Alta fiabilidad

Fiabilidad referida a la tasa de error de la red mientras se encuentra en operación. Se entiende por tasa de error el número de bits erróneos que se transmiten por la red. En general la tasa de error para fibra óptica es menor que la del cable de cobre a igualdad de longitud. La tasa de error no detectada por los mecanismos de detección de errores es del orden de 10-20. Esta característica permite a la redes de área metropolitana trabajar en entornos donde los errores pueden resultar desastrosos como es el caso del control de tráfico aéreo.

Alta seguridad

La fibra óptica ofrece un medio seguro porque no es posible leer o cambiar la señal óptica sin interrumpir físicamente el enlace. La rotura de un cable y la inserción de mecanismos ajenos a la red implica una caída del enlace de forma temporal.

Inmunidad al ruido

En lugares críticos donde la red sufre interferencias electromagnéticas considerables la fibra óptica ofrece un medio de comunicación libre de ruidos.

1.2 Por Relación Funcional

1.2.1 Cliente-Servidor

Esta arquitectura consiste básicamente en que un programa, el Cliente informático realiza peticiones a otro programa, el servidor, que les da respuesta.

Aunque esta idea se puede aplicar a programas que se ejecutan sobre una sola computadora es más ventajosa en un sistema multiusuario distribuido a través de una red de computadoras.
En esta arquitectura la capacidad de proceso está repartida entre los clientes y los servidores, aunque son más importantes las ventajas de tipo organizativo debidas a la centralización de la gestión de la información y la separación de responsabilidades, lo que facilita y clarifica el diseño del sistema.
La separación entre cliente y servidor es una separación de tipo lógico, donde el servidor no se ejecuta necesariamente sobre una sola máquina ni es necesariamente un sólo programa.
Una disposición muy común son los sistemas multicapa en los que el servidor se descompone en diferentes programas que pueden ser ejecutados por diferentes computadoras aumentando así el grado de distribución del sistema. La arquitectura cliente-servidor sustituye a la arquitectura monolítica en la que no hay distribución, tanto a nivel físico como a nivel lógico.

Ventajas de la arquitectura cliente-servidor

Centralización del control: los accesos, recursos y la integridad de los datos son controlados por el servidor de forma que un programa cliente defectuoso o no autorizado no pueda dañar el sistema.
Escalabilidad: se puede aumentar la capacidad de clientes y servidores por separado.

El servidor de cliente es la arquitectura de red que separa al cliente (a menudo un uso que utiliza un interfaz utilizador gráfico) de un servidor. Cada caso del software del cliente puede enviar peticiones a un servidor. Los tipos específicos de servidores incluyen los servidores de la web, los servidores del uso, los servidores de archivo, los servidores terminales, y los servidores del correo. Mientras que sus propósitos varían algo, la arquitectura básica sigue siendo igual.

1.2.2 Igual-a-Igual (P2P)

A grandes rasgos, una red informática entre iguales (en inglés *peer-to-peer* y más conocida como P2P) se refiere a una red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores de los demás nodos de la red. Este modelo de red contrasta con el modelo cliente-servidor el cual se rige de una arquitectura monolítica donde no hay distribución de tareas entre sí, solo una simple comunicación entre un usuario y una terminal en donde el cliente y el servidor no pueden cambiar de roles.

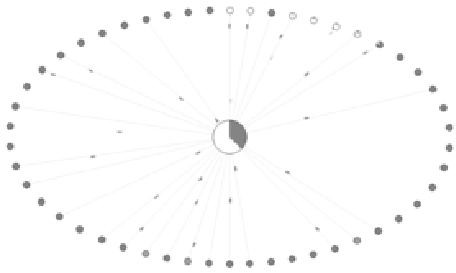


Gráfico de un enjambre mostrando la distribución de los peers con sus respectivas transmisiones y recepciones de datos dentro de un torrent en Azureus

Cualquier nodo puede iniciar, detener o completar una transacción compatible. La eficacia de los nodos en el enlace y transmisión de datos puede variar según su configuración local, velocidad de proceso y disponibilidad de ancho de banda de su conexión a la red

Características

Seis características deseables de las redes P2P:

1. Escalabilidad. Las redes P2P tienen un alcance mundial con cientos de millones de usuarios potenciales. En general, lo deseable es que cuantos más nodos estén conectados a una red P2P mejor será su funcionamiento. Así, cuando los nodos llegan y comparten sus propios recursos, los recursos totales del sistema aumentan.
2. Robustez. La naturaleza distribuida de las redes *peer-to-peer* también incrementa la robustez en caso de haber fallos en la réplica excesiva de los datos hacia múltiples destinos, y —-en sistemas P2P puros—- permitiendo a los peers encontrar la información sin hacer peticiones a ningún servidor centralizado de indexado.
3. Descentralización. Estas redes por definición son descentralizadas y todos los nodos son iguales. No existen nodos con funciones especiales, y por tanto ningún nodo es imprescindible para el funcionamiento de la red
4. Los costes están repartidos entre los usuarios. Se comparten o donan recursos a cambio de recursos. Según la aplicación de la red, los recursos pueden ser archivos, ancho de banda, ciclos de proceso o almacenamiento de disco.

Aplicaciones de las redes P2P

En la actual Internet, el ancho de banda o las capacidades de almacenamiento y cómputo son recursos caros. En aquellas aplicaciones y servicios que requieran una enorme cantidad de recursos pueden utilizarse las redes P2P.

Algunos ejemplos de aplicación de las redes P2P:

Intercambio y búsqueda de ficheros. Quizás sea la aplicación más extendida de este tipo de redes

Sistemas de ficheros distribuidos, como CFS o Freenet.

Sistemas de telefonía por Internet, como Skype.

A partir del año 2006 cada vez más compañías europeas y americanas, como Warner Bros o la BBC, empezaron a ver el P2P como una alternativa a la distribución convencional de películas y programas de televisión, ofreciendo parte de sus contenidos a través de tecnologías como la de BitTorrent [1].

Cálculos científicos que procesen enormes bases de datos, como los bioinformáticos.

1.3 Por Estructura

1.3.1 Modelo OSI

Modelo de referencia OSI

El modelo en sí mismo no puede ser considerado una arquitectura, ya que no especifica el protocolo que debe ser usado en cada capa, sino que suele hablarse de modelo de referencia. Este modelo está dividido en siete capas:

Capa fisica (capa 1)

La Capa Física del modelo de referencia OSI es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico (medios guiados: cable coaxial, cable de par trenzado, fibra óptica y otros tipos de cables; medios no guiados: radio, infrarrojos, microondas, láser y otras redes inalámbricas); características del medio (p.e. tipo de cable o calidad del mismo; tipo de conectores normalizados o en su caso tipo de antena; etc.) y la forma en la que se transmite la información (codificación de señal, niveles de tensión/intensidad de corriente eléctrica, modulación, tasa binaria, etc.)

Es la encargada de transmitir los bits de información a través del medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si ésta es uni o bidireccional (símplex, dúplex o full-dúplex). También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas/electromagnéticas.

Se encarga de transformar una trama de datos proveniente del nivel de enlace en una señal adecuada al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable) o electromagnéticos (transmisión sin cables). Estos últimos,

dependiendo de la frecuencia / longitud de onda de la señal pueden ser ópticos, de microondas o de radio. Cuando actúa en modo recepción el trabajo es inverso; se encarga de transformar la señal transmitida en tramas de datos binarios que serán entregados al nivel de enlace.

Sus principales funciones se pueden resumir como:

Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados (o no, como en RS232/EIA232), coaxial, guías de onda, aire, fibra óptica.

Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.

Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).

Transmitir el flujo de bits a través del medio.

Manejar las señales eléctricas/electromagnéticas

Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.

Garantizar la conexión (aunque no la fiabilidad de ésta).

Codificación de la señal

El nivel físico recibe una trama binaria que debe convertir a una señal eléctrica, electro magnética u otra dependiendo del medio, de tal forma que a pesar de la degradación que pueda sufrir en el medio de transmisión vuelva a ser interpretable correctamente en el receptor.

En el caso más sencillo el medio es directamente digital, como en el caso de las fibras ópticas, dado que por ellas se transmiten pulsos de luz.

Cuando el medio no es digital hay que codificar la señal, en los casos más sencillos la codificación puede ser por pulsos de tensión . Otros medios se codifican mediante presencia o ausencia de corriente. Cuando se quiere sacar más partido al medio se usan técnicas de modulación más complejas, y suelen ser muy dependientes de las características del medio concreto.

Topología y medios compartidos

Indirectamente el tipo de conexión que se haga en la capa física puede influir en el diseño de la capa de Enlace. Atendiendo al número de equipos que comparten un medio hay dos posibilidades:

Conexiones punto a punto: que se establecen entre dos equipos y que no admiten ser compartidas por terceros

Conexiones multipunto: en las que dos o más equipos pueden usar el medio.

Capa de enlace de datos (capa2)

Cualquier medio de transmisión debe ser capaz de proporcionar una transmisión sin errores, es decir, un tránsito de datos fiable a través de un enlace físico. Debe crear y reconocer los límites de las tramas, así como resolver los problemas derivados del deterioro, pérdida o duplicidad de las tramas. También puede incluir algún mecanismo de regulación del tráfico que evite la saturación de un receptor que sea más lento que el emisor.

La capa de enlace de datos se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

Capa de red (capa 3)

El cometido de la capa de red es hacer que los datos lleguen desde el origen al destino, aún cuando ambos no estén conectados directamente. Es decir que se encarga de encontrar un camino manteniendo una tabla de enrutamiento y atravesando los equipos que sea necesario, para hacer llevar los datos al destino. Los equipos encargados de realizar este encaminamiento se denominan en castellano encaminadores, aunque es más frecuente encontrar el nombre inglés *routers* y, en ocasiones enrutadores.

Adicionalmente la capa de red debe gestionar la congestión de red, que es el fenómeno que se produce cuando una saturación de un nodo tira abajo toda la red (similar a un atasco en un cruce importante en una ciudad grande). La PDU de la capa 3 es paquetes.

Capa de transporte (capa 4)

Su función básica es aceptar los datos enviados por las capas superiores, dividirlos en pequeñas partes si es necesario, y pasarlos a la capa de red. También se asegura que lleguen correctamente al otro lado de la comunicación. Otra característica a destacar es que debe aislar a las capas superiores de las distintas posibles implementaciones de tecnologías de red en las capas inferiores, lo que la convierte en el corazón de la comunicación. En esta capa se proveen servicios de conexión para la capa de sesión que serán utilizados finalmente por los usuarios de la red al enviar y recibir paquetes. Estos servicios estarán asociados al tipo de comunicación empleada, la cual puede ser diferente según el requerimiento que se le haga a la capa de transporte. Por ejemplo, la comunicación puede ser manejada para que los paquetes sean entregados en el orden exacto en que se enviaron, asegurando una comunicación punto a punto libre de errores, o sin tener en cuenta el orden de envío. Una de las dos modalidades debe establecerse antes de comenzar la comunicación para que una sesión determinada envíe paquetes, y ése será el tipo de servicio brindado por la capa de transporte hasta que la sesión

finalice. De la explicación del funcionamiento de esta capa se desprende que no está tan encadenada a capas inferiores como en el caso de las capas 1 a 3, sino que el servicio a prestar se determina cada vez que una sesión desea establecer una comunicación. Todo el servicio que presta la capa está gestionado por las cabeceras que agrega al paquete a transmitir.
Para finalizar, podemos definir a la capa de transporte como:
Capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la destino, independizándolo del tipo de red física que se esté utilizando.
La PDU de la capa 4 se llama Segmentos.

Capa de sesión (capa 5)

Esta capa ofrece varios servicios que son cruciales para la comunicación, como son: 1 Control de la sesión a establecer entre el emisor y el receptor (quién transmite, quién escucha y seguimiento de ésta). 2 Control de la concurrencia (que dos comunicaciones a la misma operación crítica no se efectúen al mismo tiempo). 3 Mantener puntos de verificación (checkpoints), que sirven para que, ante una interrupción de transmisión por cualquier causa, la misma se pueda reanudar desde el último punto de verificación en lugar de repetirla desde el principio. Por lo tanto, el servicio provisto por esta capa es la capacidad de asegurar que, dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcialmente, o incluso, totalmente prescindibles.

En conclusión esta capa es la que se encarga de mantener el enlace entre las dos computadoras que estén trasmitiendo archivos.

Capa de presentación (capa 6)
El objetivo de la capa de presentación es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC), números (little-endian tipo Intel, big-endian tipo Motorola), sonido o imágenes, los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

Por lo tanto, podemos resumir definiendo a esta capa como la encargada de manejar las estructuras de datos abstractas y realizar las conversiones de representación de datos necesarias para la correcta interpretación de los mismos. Esta capa también permite cifrar los datos y comprimirlos.

Capa de aplicación (capa 7)

Ofrece a las aplicaciones (de usuario o no) la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP). Hay tantos protocolos como aplicaciones distintas y puesto que continuamente se desarrollan nuevas aplicaciones el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente. Así por ejemplo un usuario no manda una petición "HTTP/1.0 GET index.html" para conseguir una página en html, ni lee directamente el código html/xml.

Entre los protocolos (refiriéndose a protocolos genéricos, no a protocolos de la capa de aplicación de OSI) más conocidos destacan:

- HTTP (HyperText Transfer Protocol) el protocolo bajo la www.
- FTP (File Transfer Protocol) (FTAM, fuera de TCP/IP) transferencia de ficheros
- SMTP (Simple Mail Transfer Protocol) (X.400 fuera de tcp/ip) envío y distribución de correo electrónico
- POP (Post Office Protocol)/IMAP: reparto de correo al usuario final
- SSH (Secure SHell) principalmente terminal remoto, aunque en realidad cifra casi cualquier tipo de transmisión.

Hay otros protocolos de nivel de aplicación que facilitan el uso y administración de la red:

- SNMP (Simple Network Management Protocol)
- DNS (Domain Name System)

Unidades de datos

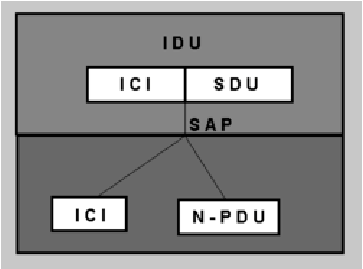
El intercambio de información entre dos capas OSI consiste en que cada capa en el sistema fuente la agrega información de control a los datos, y cada capa en el sistema de destino analiza y remueve la información de control de los datos como sigue:

Si un ordenador (host A) desea enviar datos a otro (host B), en primer término los datos deben empaquetarse a través de un proceso denominado encapsulamiento, es decir, a medida que los datos se desplazan a través de las capas del modelo OSI**,** reciben encabezados, información final y otros tipos de información.

N-PDU (Unidad de datos de protocolo)

Es la información intercambiada entre entidades pares, es decir, dos entidades pertenecientes a la misma capa pero en dos sistemas diferentes, utilizando una conexión(N-1).

Esta compuesta por:



N-SDU (Unidad de datos del servicio)

Son los datos que se necesitan las entidades(N) para realizar funciones del servicio pedido por la entidad(N+1).

N-PCI (Información de control del protocolo)

Información intercambiada entre entidades (N) utilizando una conexión (N-1) para coordinar su operación conjunta.

N-IDU (Unidad de datos del interface)

Es la información transferida entre dos niveles adyacentes, es decir, dos capas contiguas.

Esta compuesta por:

N-ICI (Información de control del interface)

Información intercambiada entre una entidad (N+1) y una entidad (N) para coordinar su operación conjunta.

Datos de Interface-(N)

Información transferida ente una entidad-(N+1) y una entidad-(N) y que normalmente coincide con la (N+1)-PDU.

Transmisión de datos

La capa de aplicación recibe el mensaje del usuario y le añade una cabecera constituyendo así la PDU de la capa de aplicación. La PDU se transfiere a la capa de aplicación del nodo destino, este elimina la cabecera y entrega el mensaje al usuario.

Para ello ha sido necesario todo este proceso:

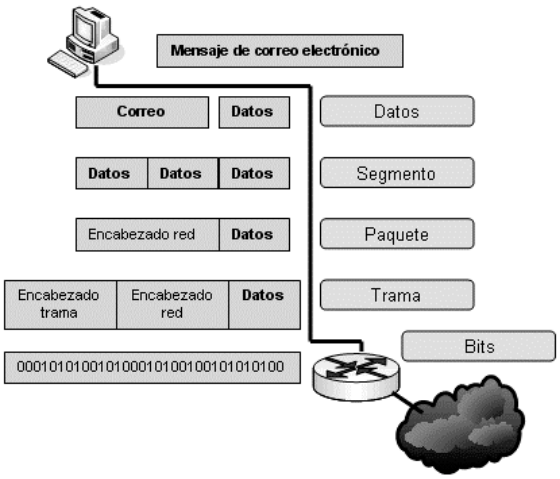
1-Ahora hay que entregar la PDU a la capa de presentación para ello hay que añadirla la correspondiente cabecera ICI y transformarla así en una IDU, la cual se transmite a dicha capa.

2-La capa de presentación recibe la IDU, le quita la cabecera y extrae la información, es decir, la SDU, a esta le añade su propia cabecera (PCI) constituyendo así la PDU de la capa de presentación.

3- Esta PDU es transferida a su vez a la capa de sesión mediante el mismo proceso, repitiéndose así para todas las capas.

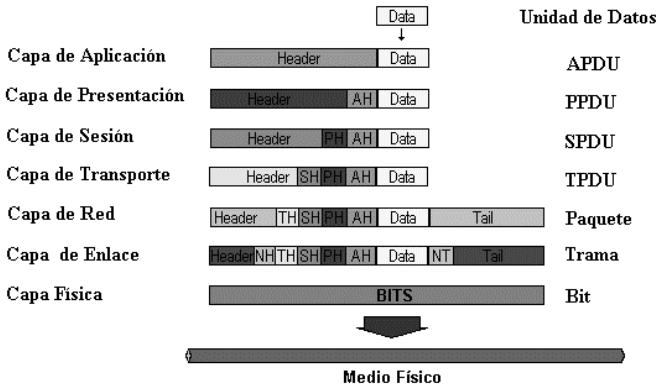
4-Al llegar al nivel físico se envían los datos que son recibidos por la capa física del receptor.

5-Cada capa del receptor se ocupa de extraer la cabecera, que anteriormente había añadido su capa homóloga, interpretarla y entregar la PDU a la capa superior.
6-Finalmente llegará a la capa de aplicación la cual entregará el mensaje al usuario.



Formato de datos

Estos datos reciben una serie de nombres y formatos específicos en función de la capa en la que se encuentren, debido a como se describió anteriormente la adhesión de una serie de encabezados e información final. Los formatos de información son los siguientes:



APDU: Unidad de datos en la Capa de aplicación.

PPDU: Unidad de datos en la Capa de presentación.

SPDU: Unidad de datos en la capa de sesión.

TPDU: Unidad de datos en la capa de transporte.

Paquete: Unidad de datos en el Nivel de red.

Trama: Unidad de datos en la capa de enlace.

Bits: Unidad de datos en la capa física.

Operaciones sobre los datos

En determinadas situaciones es necesario realizar una serie de operaciones sobre las PDU para facilitar su transporte, bien debido a que son demasiado grandes o bien porque son demasiado pequeñas y estaríamos desaprovechando la capacidad del enlace.

SEGMENTACIÓN Y REENSAMBLAJE

Hace corresponder a una (N)-SDU sobre varias (N)-PDU.

El reensamblaje hace corresponder a varias (N)-PDUs en una (N)-SDU.

BLOQUEO Y DESBLOQUEO

El bloqueo hace corresponder varias (N)-SDUs en una (N)-PDU.

El desbloqueo identifica varias (N)-SDUs que están contenidas en una (N)-PDU.

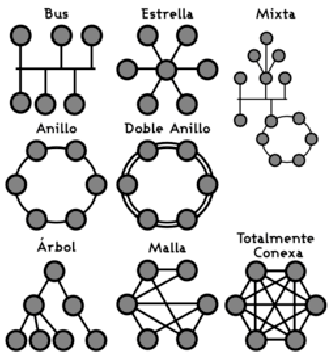
CONCATENACIÓN Y SEPARACIÓN

La concatenación es una función-(N) que realiza el nivel-(N) y que hace corresponder varias (N)-PDUs en una sola (N-1)-SDU.

La separación identifica varias (N)-PDUs que están contenidas en una sola (N-1)-SDU.

1.4 Por Topología de Red

1.4.1 Topologìas



La arquitectura o topología de red es la disposición física en la que se conectan los nodos de una red de ordenadores o servidores, mediante la combinación de estándares y protocolos.

La topología de red la determina únicamente la configuración de las conexiones entre nodos. La distancia entre los nodos, las interconexiones físicas, las tasas de transmisión y/o los tipos de señales no pertenecen a la topología de la red, aunque pueden verse afectados por la misma.

Componentes

Describe los componentes de una red, así como la forma en que se relacionan y coordinan para alcanzar el objetivo final de la red.

Hay que tener en cuenta:

Hardware.

Software.

Operatividad.

Escenarios.

Interconexión.

Compatibilidad.

Análisis y diseño.

Al principio, la transmisión de datos era un gran problema, que fue resuelto dividiéndolo los procesos en capas, ordenadas de forma piramidal. Mientras más inferior sea una capa, se tratará de un proceso más físico, y mientras más se ascienda, se tratará de un proceso más lógico. La principal arquitectura de capas es el Modelo OSI.

En una arquitectura de capas, cada capa realiza unas funciones y ofrece unos servicios.

a) Una capa N ofrece sus servicios a la capa superior N+1. Una capa N+1 solo "ve" los servicios de la capa N.

b) Las capas de un componente se comunican entre si usando interfaces (que no pertenecen a la arquitectura).

c) Una capa de un componente se comunica con su homóloga de otro componente mediante un protocolo.

d) En cada capa existen entidades (generalmente procesos) que realizan las funciones de esa capa..

1.4.2 Redes Centralizadas

La topología en estrella reduce la posibilidad de fallo de red conectando todos los nodos a un nodo central. Cuando se aplica a una red basada en bus, este concentrador central reenvía todas las transmisiones recibidas de cualquier nodo periférico a todos los nodos periféricos de la red, algunas veces incluso al nodo que lo envió. Todos los nodos periféricos se pueden comunicar con los demás transmitiendo o recibiendo del nodo central solamente. Un fallo en la línea de conexión de cualquier nodo con el nodo central provocaría el aislamiento de ese nodo respecto a los demás, pero el resto de sistemas permanecería intactos.

Si el nodo central es pasivo, el nodo origen debe ser capaz de tolerar un eco de su transmisión. Una red en estrella activa tiene un nodo central activo que normalmente tiene los medios para prevenir problemas relacionados con el eco.

Una topología en árbol (también conocida como topología jerárquica) puede ser vista como una colección de redes en estrella ordenadas en una jerarquía. Éste árbol tiene nodos periféricos individuales que requieren transmitir a y recibir de otro nodo solamente y no necesitan actuar como repetidores o regeneradores. Al contrario que en las redes en estrella, la función del nodo central se puede distribuir.

Como en las redes en estrella convencionales, los nodos individuales pueden quedar aislados de la red por un fallo puntual en la ruta de conexión del nodo. Si falla un enlace que conecta con un nodo hoja, ese nodo hoja queda aislado; si falla un enlace con un nodo que no sea hoja, la sección entera queda aislada del resto.

Para aliviar la cantidad de tráfico de red que se necesita para retransmitir todo a todos los nodos, se desarrollaron nodos centrales más avanzados que permiten mantener un listado de las identidades de los diferentes sistemas conectados a la red. Éstos switches de red "aprenderían" cómo es la estructura de la red transmitiendo paquetes de datos a todos los nodos y luego observando de dónde vienen los paquetes respuesta.

1.4.3 Redes Descentralizadas

En una topología en malla, hay al menos dos nodos con dos o más caminos entre ellos. Un tipo especial de malla en la que se limite el número de saltos entre dos nodos, es un hipercubo. El número de caminos arbitrarios en las redes en malla las hace más difíciles de diseñar e implementar, pero su naturaleza descentralizada las hace muy útiles.

Una red totalmente conectada o completa, es una topología de red en la que hay un enlace directo entre cada pareja de nodos. En una red totalmente conexa con n nodos, hay enlaces directos. Las redes diseñadas con esta topología, normalmente son caras de instalar, pero son muy fiables gracias a los múltiples caminos por los que los datos pueden viajar. Se ve principalmente en aplicaciones militares.

1.4.4 Redes Híbridas

Las redes híbridas usan una combinación de dos o más topologías distintas de tal manera que la red resultante no tiene forma estándar. Por ejemplo, una red en árbol conectada a una red en árbol sigue siendo una red en árbol, pero dos redes en estrella conectadas entre sí (lo que se conoce como estrella extendida) muestran una topología de red híbrida. Una topología híbrida, siempre se produce cuando se conectan dos topologías de red básicas.

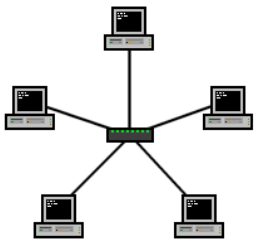
1.4.5 Red de Bus

La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente, aunque la ruptura del cable hace que los host queden desconectados.

Red en topología de bus

La topología de bus permite que todos los dispositivos de la red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si desea que todos los dispositivos obtengan esta información. Sin embargo, puede representar una desventaja, ya que es común que se produzcan problemas de tráfico y colisiones, que se pueden paliar segmentando la red en varias partes. Es la topología más común en pequeñas LAN, con hub o switch final en uno de los extremos.

1.4.6 Red de Estrella



Red en topología de estrella

Una red en estrella es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de este. Todas las estaciones están conectadas por separado a un centro de comunicaciones, concentrador o nodo central, pero no están conectadas entre sí.

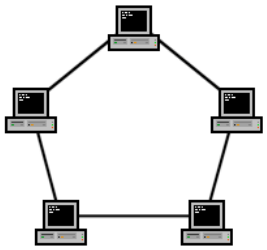
Esta red crea una mayor facilidad de supervisión y control de información ya que para pasar los mensajes deben pasar por el *hub* o concentrador, el cual gestiona la redistribución de la información a los demás nodos. La fiabilidad de este tipo de red es que el mal funcionamiento

de un ordenador no afecta en nada a la red entera, puesto que cada ordenador se conecta independientemente del *hub*, el costo del cableado puede llegar a ser muy alto.

Cabe destacar que cuando se utiliza un hub o concentrador como punto central en una topología de estrella, se dice que la red funciona con una topología de bus lógico, ya que el hub enviará la información a través de todos sus puertos haciendo que todos los host conectados reciban la información (incluso cuando no está destinada a ellos). Actualmente se han sustituido los hubs o concentradores, por switches o conmutadores.

Creando así una topología en estrella tanto física como lógica debido a las propiedades de segmentación y acceso al medio que nos ofrecen estos dispositivos capa 2.

1.4.7 Red en Anillo



Red con topología de anillo

Topología de red en la que las estaciones se conectan formando un anillo. Cada estación está conectada a la siguiente y la última está conectada a la primera. Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación del anillo.

En este tipo de red la comunicación se da por el paso de un token o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evitan eventuales pérdidas de información debidas a colisiones.

Cabe mencionar que si algún nodo de la red se cae (término informático para decir que esta en mal funcionamiento o no funciona para nada) la comunicación en todo el anillo se pierde.

En un anillo doble, dos anillos permiten que los datos se envíen en ambas direcciones. Esta configuración crea redundancia (tolerancia a fallos), lo que significa que si uno de los anillos falla, los datos pueden transmitirse por el otro.

1.4.8 Red Malla

La topología en malla es una topología de red en la que cada nodo está conectado a uno o más de los otros nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos. Si la red de malla está completamente conectada no puede existir

absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás servidores.

Funcionamiento

El establecimiento de una red de malla es una manera de encaminar datos, voz e instrucciones entre los nodos. Las redes de malla se diferencian de otras redes en que las piezas de la red (nodo) están conectadas unas con otras por uno u otro camino, mediante cables separados. Las redes de malla son autoregenerables: la red puede funcionar incluso cuando un nodo desaparece o la conexión falla, ya que el resto de nodos evitan el paso por ese punto. Consecuentemente, se forma una red muy confiable, es una opción aplicable a las redes sin hilos (Wireless), a las redes con cable (Wired), y a la interacción del software.

CAPITULO 2 .- SEÑALIZACIÓN POR CANAL COMÚN

Un sistema de señalización por canal común Nº 7 es aquel en el cual la señalización correspondiente a varios canales de información, se transporta por un canal común para muchas comunicaciones. La señalización consiste de paquetes cortos de mensajes que son enrutados a través de una red de señalización, superpuesta a la red de voz. Sus componentes fundamentales son los puntos de señalización y los enlaces que unen estos puntos. Los puntos de señalización son nodos capaces de manejar los mensajes del sistema de señalización Nº 7. A cada punto de señalización se le asigna una dirección que se llama código de punto de señalización. Estos códigos de puntos de señalización se asignan conforme a un plan de numeración.

En la actualidad las redes de comunicaciones utilizan sofisticados sistemas de señalización para establecer, terminar las llamadas, controlar y mantener en funcionamiento la propia red. En la medida en que las redes se vuelven más complejas crece el número de funciones que debe realizar el sistema de señalización. Algunas de estas funciones son:

Información audible para el usuario que llama (tono de invitación a discar, tono de repique y tono de ocupado) y para el llamado (señal de repique)

Transmisión del número marcado a las centrales de conmutación.

Información entre centrales

Información de tasación.

Información sobre el estado de los enlaces y equipos, para ser utilizada en el enrutamiento, gestión y mantenimiento de red.

En resumen, las funciones de señalización se pueden clasificar en supervisión, direccionamiento, información sobre la llamada y gestión, constituyendo el soporte básico para las funciones de mando y control de la red.

La supervisión se refiere a las señales de estado y de control como por ejemplo: solicitud de servicio, contestación, alerta, en espera.

Las señales de direccionamiento representan un mecanismo para identificar a los usuarios que intentan comunicarse, llevando información como números telefónicos, códigos de área.

La evolución de la tecnología en los sistemas de conmutación y la automatización del tráfico telefónico en las redes nacionales e internacionales han culminado en el desarrollo de diversos sistemas de señalización. Con la introducción de los sistemas de transmisión digital y los progresos realizados en las telecomunicaciones de datos, se ha logrado por último el sistema de señalización Nº 7. Una red de señalización Nº 7 puede ser considerada como una red de

comunicación de datos, optima para la transferencia de diversos tipos de información de señalización que debe transmitirse entre los procesadores de una red de telecomunicaciones.

La red de señalización N° 7 dispone de medios para asegurar la transferencia fiable de los mensajes de señalización, aún en el caso de averías en la red. Con enlaces y rutas de señalización redundantes pueden generarse funciones para la desviación automática de señalización a enlaces y rutas alternativas, en caso de fallas. De allí que el sistema puede dimensionarse para adaptarlo a los requisitos de calidad y fiabilidad de la administración y de los usuarios. La señalización Nº 7 tiene como objetivo proporcionar un sistema de señalización por canal común de aplicación general. Tiene muchas aplicaciones tanto de voz como de datos, permitiendo una amplia gama de conexiones incluyendo el modo circuito, el modo paquete, Frame Relay y ATM. Es requisito de la RSDI, pero puede utilizarse sólo para telefonía convencional, servicios móviles y bases de datos y su flexibilidad permite la introducción de nuevos servicios. Esta optimizado para funcionar en canales digitales de 64 kbit/s y puede utilizarse a través de canales por satélite, también funciona a través de canales analógicos.

El sistema de señalización Nº7 es considerado un protocolo superior que posee beneficios significativos caracterizados por: señalización estandarizada por canal común, flexibilidad, robustez y confiabilidad, posibilidad de evolución, capacidad de interconexión, soporte para nuevos y variados servicios.

2.1 Red de Señalización por Canal Común N° 7

En una red de señalización por canal común, los mensajes de señalización se transmiten en el canal común N°7 (CCS7) por enlaces de señalización separados, los cuales pueden transportar los mensajes de señalización necesarios para un gran número de canales útiles. Estos enlaces de señalización del CCS7 enlazan entre si los puntos de señalización en una red de comunicación, por tanto los puntos y enlaces de señalización conforman una red de señalización autónoma superpuesta la red de canales útiles, es decir, la red de señalización por canal común Nº 7 puede ser considerada como una red de paquetes superpuesta a la red de voz, en la cual sus componentes fundamentales son los puntos de señalización.

2.2 Puntos de señalización

Los puntos de señalización son los nodos de una red de señalización que pueden originar, recibir o transferir mensajes de señalización de un enlace de señalización a otro.

Los puntos de señalización pueden ser:

puntos terminales de señalización (SP) y

puntos de transferencia de señalización (STP).

Puntos de control de servicios (SCP).

Puntos terminales de señalización: son los puntos de orígenes y destinos del tráfico de señalización. En una red de comunicación estos son, en primer lugar, las centrales y constituyen los componentes básicos de una red de señalización Nº 7. Están compuestos por las siguientes partes: parte de control de conexión de señalización, gestión y mantenimiento del tráfico durante fallas o congestión de la red, gestión del estatus del sistema e interfaces para mensajes.

Puntos de transferencia de señalización: se encargan de retransmitir los mensajes de señalización recibidos, a otro punto de señalización o terminal de señalización, basándose en la dirección o destino. Puede estar integrado en un punto terminal de señalización, por ejemplo una central, o puede ser un nodo separado dentro de la red de señalización. En una red de señalización Nº 7 puede haber, según el dimensionamiento de la red, uno o varios niveles de puntos de transferencia de señalización, los cuales suelen establecerse por pares, en base al criterio de carga compartida, para mayor confiabilidad.

Puntos de control de servicios: permiten el acceso a las bases de datos, pueden ejecutar funciones de procesamientos de mensajes, operación, administración y mantenimiento del nodo.
Los puntos de señalización en una red de señalización están identificados por un código, el cual forma parte de un plan de numeración correspondiente a dicha red, pudiendo de esta manera, ser direccionados discrecionalmente en un mensaje de señalización.

2.3 Código de Punto de señalización

El código de punto de señalización es el código utilizado para identificar un punto de señalización.
A nivel internacional los códigos de punto de señalización tienen un formato de código binario de 14 bits (formato del código de punto de señalización internacional (en ingles ISPC)) y los campos de este formato sólo tienen una utilidad administrativa. El formato del código de punto de señalización internacional contempla dos partes, a saber: los códigos de área/red de señalización (en ingles SANC) y la identificación de puntos de señalización.
La Recomendación Q.708 también describe los principios y procedimientos de asignación de los códigos de área/ red de señalización y de los códigos de puntos de señalización de la red internacional del sistema de señalización Nº7.

Para fines administrativos de estructura de los códigos de puntos de señalización, se recomienda, por ejemplo, la división de un país en regiones y de una región en zonas, para adaptarse a las zonas administrativas existentes, esto para facilitar la gestión de administración de los puntos de señalización. El campo definido para zonas, dependiendo de la administración, podrá identificar un operador o red en una zona específica.

Ejemplos:

a): Formato de código de punto de señalización no estructurado

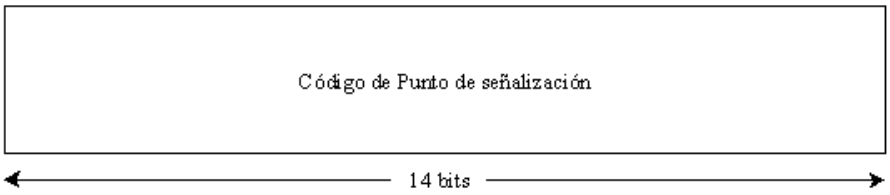


Fig.1

b): Formato de código de punto de señalización estructurado

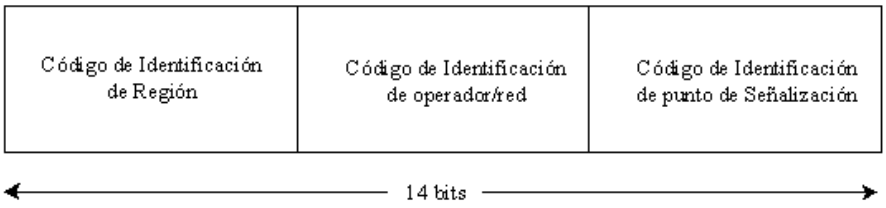


Fig. 2

La UIT también señala que el plan de numeración de señalización de un país dado puede ser:

a. "Uniforme": los valores m y l son fijos independientemente de la región.
b. "No uniforme": una región determinada puede incluir una zona codificada que tiene diferentes numero de bit y hasta x puntos de señalización, deferente de otra zona con diferente codificación y numero de puntos de señalización también diferentes, pero de igual longitud. (14 BIT).

Los códigos de puntos de señalización no tienen relación directa con el plan de numeración de la red telefónica, de datos o de RDSI. Dichos códigos están concebidos para ser procesados

dentro de la parte de transferencia de mensaje (PTM) de cada punto de transferencia de señalización.

2.4 Enlaces de Señalización

Un enlace de señalización consiste en un canal de señalización bidireccional que transporta la información entre dos SP. Para establecer el enlace se puede utilizar cualquier medio de transmisión digital. Por razones de redundancia suele haber entre dos puntos de señalización más de un enlace de señalización. Un grupo de enlaces entre dos SP específicos, constituye un grupo troncal de señalización (también llamado SET) que puede contener hasta un máximo de 16 enlaces. Una central puede cumplir funciones tanto de SP como de STP. Para el caso de falla de uno de los enlaces de señalización, se han implementado en el sistema CCS7 funciones que se encargan de desviar el tráfico de señalización hacia rutas alternativas libres de fallas.

2.5 Modos de operación

El modo de operación de la señalización Nº 7, se refiere a la relación o asociación existente entre el camino tomado por la señalización y el seguido por la conversación o información correspondiente. En la red de señalización por canal común Nº 7 se pueden emplear dos modos de operación:

Modo de operación asociado: El canal de señalización está asociado con los canales que llevan la información, en el sentido de que viajan por la misma ruta física, utilizando los mismos troncales. Esto quiere decir, que el enlace de señalización está conectado directamente con los puntos terminales, que son también los puntos de destino del troncal. Este modo se recomienda para una relación de tráfico bastante alta. En la siguiente figura se muestra un esquema de este modo de operación.

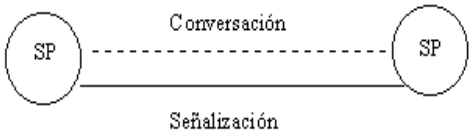


Fig.3

Modo de operación asociado

Modo de operación cuasi-asociado: Se instalan nodos adicionales de transferencia (STP), creando así una red de señalización prácticamente independiente de la red de voz. Los mensajes de señalización se envían sobre dos o más enlaces, haciendo transito sobre uno o más puntos de transferencia de señalización (STP). En la siguiente figura se esquematiza este modo de operación.

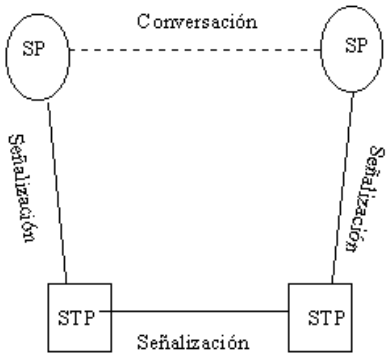


Fig. 4

Modo de operación Cuasi-Asociado.

En una red de señalización, a los puntos se señalización se les asigna una dirección que se llama código de punto de señalización, de manera que es fácil introducir señales necesarias para proveer servicios avanzados a través de nodos de control. Los Códigos de puntos de señalización pueden tener una estructura que permita fácilmente determinar la ruta hacia un determinado punto de señalización. Por ello, estos códigos se asignan conforme a un plan de numeración, el cual debe ser administrado por un organismo u organización designada. Es importante tomar en cuenta que la administración de los códigos debe ser realizada en forma eficaz de manera que se satisfagan las posibles demandas.

CAPITULO 3.- RED DIGITAL DE SERVICIOS INTEGRADOS (RDSI)

Se define la RDSI (Red Digital de Servicios Integrados, en ingles ISDN) como una evolución de las redes actuales, que presta conexiones extremo a extremo a nivel digital y capaz de ofertar diferentes servicios.

Decimos Servicios integrados porque utiliza la misma infraestructura para muchos servicios que tradicionalmente requerían interfaces distintas (télex, voz, conmutación de circuitos, conmutación de paquetes...); es digital porque se basa en la transmisión digital, integrando las señales analógicas mediante la transformación Analógico - Digital, ofreciendo una capacidad básica de comunicación de 64 Kbps.

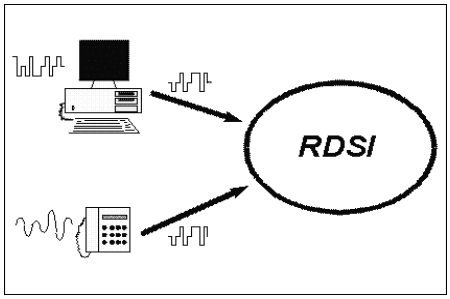


Figura 1. *Integración de señales en RDSI.*

Como podemos observar, en el caso del teléfono se efectúa la conversión Analógico Digital. En el caso de equipos digitales, computadora, se transforma el código original a otro más adecuado a la comunicación (Transformación de código).

3.1 Ventajas que aporta la RDSI.

La RDSI ofrece gran número de ventajas, entre las que se pueden destacar las siguientes:

Velocidad

Actualmente el límite de velocidad en las comunicaciones a través de una línea telefónica empleando señales analógicas entre central y usuario mediante el uso de MODEM está alrededor de los 56Kbps. La RDSI ofrece múltiples canales digitales que pueden operar simultáneamente a través de la misma conexión telefónica entre central y usuario; la tecnología digital está en la central del proveedor y en los equipos del usuario, que se comunican ahora con señales digitales.

Este esquema permite una transferencia de datos a velocidad mucho mayor. Así, con un servicio de acceso básico, y empleando un protocolo de agregación de canales, se puede alcanzar una velocidad de datos sin comprimir de unos 128 Kbps.

Señalización

La forma de realizar una llamada a través de una línea analógica es enviando una señal de tensión que hace sonar la “campana” en el teléfono destino. Esta señal se envía por el mismo canal que las señales analógicas de sonido. Establecer la llamada de esta manera requiere bastante tiempo, por ejemplo entre 30 y 60 segundos con la norma V.34 para modems.

En una conexión RDSI, la llamada se establece enviando un paquete de datos especial a través de un canal independiente de los canales para datos. Este método de llamada se engloba dentro de una serie de opciones de control de la RDSI conocidas como señalización, y permite establecer la llamada en un par de segundos. Además informa al destinatario del tipo de conexión (voz o datos) y desde que número se ha llamado, y puede ser gestionado fácilmente por equipos inteligentes como un ordenador.

Servicios

La RDSI no se limita a ofrecer comunicaciones de voz. Ofrece otros muchos servicios, como transmisión de datos informáticos télex, facsímil, videoconferencia, conexión a Internet, y opciones como llamada en espera, identidad del origen.

Los servicios portadores permiten enviar datos mediante conmutadores de circuitos (con un procedimiento de llamada se establece un camino fijo y exclusivo para transmitir los datos en la red, al estilo de las redes telefónicas clásicas) o mediante conmutadores de paquetes (la información a enviar se divide en paquetes de tamaño máximo que son enviados individualmente por la red.

3.2 Canales y Servicios

* Canales de transmisión

La RDSI dispone de distintos tipos de canales para el envío de datos de voz e información y datos de control: los canales tipo B, tipo D y Tipo H.

* Canal B

Los canales tipo B transmiten información a 64 Kbps y se emplean para transportar cualquier tipo de información de los usuarios, bien sean datos de voz o datos informáticos

Estos canales no transportan información de control de la RDSI.

Este tipo de canales sirve además como base para cualquier otro tipo de canales de datos de mayor capacidad, que se obtienen por combinación de canales tipo B.

* Canal D

Los canales tipo D se utilizan principalmente para enviar información de control de la RDSI, como es el caso de los datos necesarios para establecer una llamada o para colgar. Por ello también se conoce un canal D como "canal de señalización". Los canales D también pueden transportar datos cuando no se utilizan para control. Estos canales trabajan a 16Kbps o 64kbps según el tipo de servicio contratado.

* Canales H

Combinando varios canales B se obtienen canales tipo H, que también son canales para transportar solo datos de usuario, pero a velocidades mucho mayores. Por ello se emplean para información como audio de alta calidad o vídeo.

Hay varios tipos de canales H:

Canales H0, que trabajan a 384Kbps (6 canales B).
Canales H10, que trabajan a 1472Kbps (23 canales B).
Canales H11, que trabajan a 1536Kbps (24 canales B).
Canales H12, que trabajan a 1920Kbps (30 canales B).

3.3 Tipos de Servicio o Modos de Acceso.

Podemos dividir la RDSI en dos clases según el ancho de banda: RDSI de banda estrecha y RDSI de banda ancha.

RDSI de banda estrecha

Los Accesos de Usuario definidos para RDSI en Banda Estrecha permiten la comunicación a velocidades de 64 Kbps, o agrupaciones de está velocidad.

Debido a la estructura de transmisión y conmutación de la RDSI, técnicas digitales, la integridad de la información está asegurada. Por otra parte las técnicas digitales permiten un tratamiento de las señales de forma que la transmisión de la información no sufra degradaciones debido a la distancia o a perturbaciones externas, asegurando de esta forma una información más "limpia" de errores.

Es también una ventaja añadida la posibilidad de enviar pequeños mensajes en la "llamada" para indicar situaciones especiales, envío de textos como: "Llámame en 30 minutos", permiten al Usuario Llamado la posibilidad de devolver la llamada. La aparición de elementos como el

número de origen de la llamada, el número destino, etc., mejoran los servicios de la Red en beneficio del Usuario.

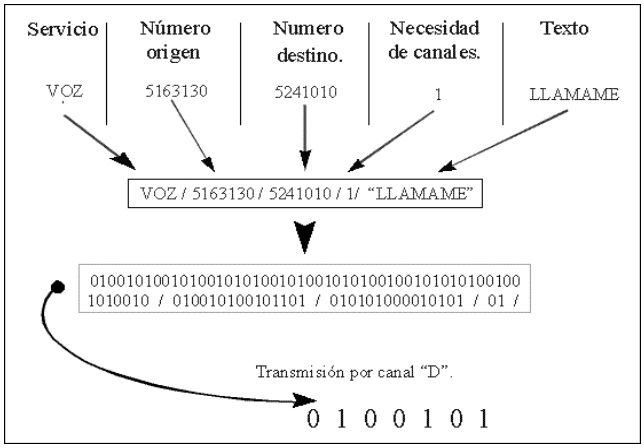


Figura 2. *Paquete de señalización, ejemplo.*

Un usuario puede contratar dos tipos de servicio diferentes con el proveedor telefónico según sus necesidades:

Acceso básico o BRI (Basic Rate Interface)

Proporciona dos canales B y un canal D de 16Kbps multiplexados a través de la línea telefónica. De esta forma se dispone de una velocidad total de 144Kbps.

Este es el tipo de servicio que encaja en las necesidades de usuarios individuales.

Acceso primario o PRI (Primary Rate Interface).

En EE.UU. suele tener 23 canales tipo B y un canal D de 64Kbps, alcanzando una velocidad global de 1536Kbps.

En Europa el PRI consiste de 30 canales B y un canal D de 64Kbps, alcanzando una velocidad global de 1984Kbps.

En el segundo caso, los canales B también pueden estar agrupados como 5 canales H0 o un canal H12.

Este es el tipo de servicio que contratan entidades con gran demanda.

RDSI de banda ancha

Esta nueva red es básicamente igual a la RDSI actual, con la diferencia de que la velocidad mínima a la que trabaje será de 2Mbps, pudiendo llegar a los 100Mbps. Estas velocidades permiten aumentar en gran medida el número de servicios que la red ofrecerá.

3.4 Agregación de Canales.

La RDSI ofrece la capacidad de agregar canales para realizar conexiones a mayor velocidad.

Así, con un acceso BRI se puede establecer dos conexiones a 64Kbps o una única conexión a 128Kbps, usando siempre una única línea RDSI.

En realidad, una llamada a 128Kbps son dos llamadas diferentes a 64Kbps cada una, existiendo un protocolo por encima que permite ver esa llamada como una sola. Lo que también quiere decir que una conexión a 128Kbps cuesta el doble que otra de igual duración a 64Kbps. Esto es así a pesar de que, en la práctica, doblar el ancho de banda no significa doblar la velocidad de transferencia máxima. La mejora del rendimiento depende de la utilización que el protocolo haga del ancho de mayor banda.

3.5 Interfaces y Configuraciones

La configuración de referencia, ver figura 3, está definida por Agrupaciones funcionales, equipos con una función concreta, y puntos de referencia o interfaces, puntos concretos en los que la RDSI presenta características de transmisión o conmutación determinadas.

Se comentan a continuación las características de cada elemento.

Agrupaciones funcionales

Las agrupaciones funcionales son elementos que desarrollan una función, en este caso corresponden a equipos o elementos de los mismos bien del Cliente o de Central.

TC.- Terminación de Central, situada en la Central de Conmutación se encarga del mantenimiento del Acceso de Usuario. Realiza la conexión de canales, soporta la señalización del usuario y el envío de información en modo paquete.

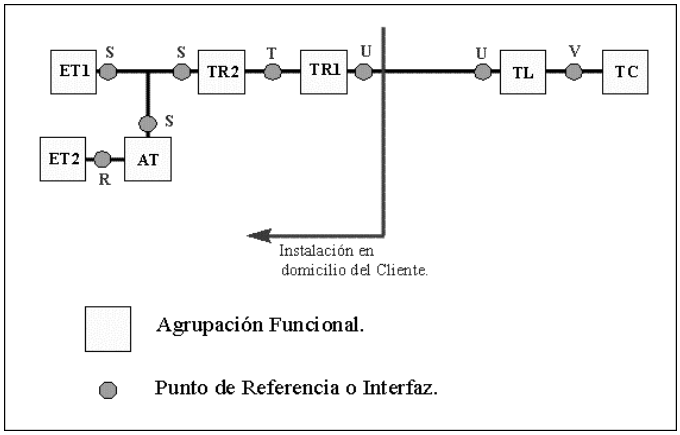


Figura 3. *Configuración de Referencia.*

TL.- Terminación de Línea, situada en la Central, se encarga de los aspectos de transmisión. Convierte el código binario al código de línea empleado. Controla la sincronización del Acceso. Ésta agrupación funcional está unida a la TC formando una agrupación.

TR1.- Terminación de Red nº 1, es el primer elemento en el domicilio del Cliente y obligación de la compañía explotadora del servicio, en España Telefónica. Permite la sincronización con los equipos conectados a continuación, controla la conexión con la Central, adecua las señales de la línea a códigos adecuados para la conexión de los equipo, permite la verificación a distancia, pudiéndose evaluar la calidad del enlace.

TR2.- Terminación de Red nº 2, realiza funciones de control en la instalación del Cliente: tratamiento de la señalización, multiplexación de canales de información, posible conmutación local (centralita), concentración de tráfico y mantenimiento de la instalación del usuario.

ET1.- Equipo Terminal nº 1, es el Equipo Terminal RDSI, preparado para señalización en modo paquete y gestión de canales de información. Algunos ejemplos pueden ser Teléfonos RDSI, equipos de Videotelefonía, Tarjetas de PC, etc.

AT.- Adaptador de Terminales, se trata de un equipo RDSI que tiene la capacidad de adaptar interfaces. Convierte las señales de otros equipos no RDSI a señales adecuadas al interfaz correspondiente (interfaz "S").

ET2.- Equipos Terminales nº 2, son equipos no RDSI que pueden conectarse mediante un interfaz no Normalizado por RDSI a la Red. Fax Grupos 2 y 3, Teléfonos analógicos, módem.

Puntos de referencia o interfaces

Los Puntos de Referencia son interfaces entre las agrupaciones funcionales y pueden ser Reales o Virtuales. Los puntos de referencia Virtuales no son accesibles, o en algunos casos coinciden con otro Interfaz.

V.- representa la separación entre las funciones de conmutación y transmisión en la Central. Se trata de una interfaz Virtual ya que TL y TC están unidas en la Placa de Línea de la Central Pública.

U.- representa las características de transmisión en la línea, de forma que especifica el formato de la trama en la misma, los códigos posibles, niveles de señal, las perturbaciones permitidas (atenuación, ruido). Brinda al TR1 la posibilidad sincronización, la activación, y sirve de transporte al Acceso.

T.- representa la separación entre la transmisión de línea y la transmisión en el domicilio del Cliente. Es un punto de Transmisión que puede coincidir con el Punto "S".

S.- representa el interfaz de conexión físico de los equipos terminales RDSI, y define la estructura de trama, la gestión del Canal D, la sincronización y las características de transmisión.

R.- representa un interfaz no normalizado en RDSI, y precisa de un AT para que el equipo correspondiente pueda conectarse al Acceso.

En el Acceso Básico los puntos S y T corresponden al mismo interfaz, denominándose interfaz S. Así pues la conexión de un equipo terminal se efectúa directamente al TR1, mediante una configuración de instalación determinada (Bus). Puede conectarse un TR2 pero éste deberá implementar un interfaz S en la conexión.

En el Acceso Primario se conectara un TR2 para transformar el interfaz T en interfaz S permitiendo la conexión de equipos terminales RDSI. En el caso de equipos que gestionen los 30 canales de comunicación, Videoconferencia de alta calidad, este se conecta al interfaz T, ya que el equipo hará las funciones de TR2.

En el lado de Central las agrupaciones TL y TC están siempre incluidas en la correspondiente tarjeta de línea, así pues el interfaz V no será accesible. El interfaz U puede adaptarse a otras señales mediante los equipos de transmisión adecuados, de esta forma se asegura una cobertura mayor (multiplexores).

3.6 Codificación de tramas

Una trama de nivel físico en una interface U de un acceso BRI se compone de un grupo de 8 tramas de menor tamaño, cada una de las cuales incluye los siguiente campos:

· Sincronización

Secuencia especial del código de línea que ayuda al receptor a identificar la señal de reloj de la trama.

· Datos

Doce grupos de 18 bits para los datos de los dos canales B y el canal D. En cada grupo se toman 8 bits para cada canal B y 2 para el canal D.

· Mantenimiento.

Contiene un valor de CRC para detección de errores en el receptor. También incluye bits dedicados a comandos especiales, como los de prueba o test de la línea.

En el caso de un acceso PRI, para el interface U se emplea la estructura de trama normalizada para TDM.

El sistema TDM (Multiplexión por división de tiempo) es un sistema digital que permite combinar o multiplexar hasta 30 canales de señales digitales de 8 bits a 64Kbps procedentes de diversas fuentes dentro de una trama de 32 bytes enviados a 2048 Kbps (la trama dura 125 mseg). La trama también incorpora 2 bytes para señalización y sincronización.

CAPITULO 4.- RED X.25

La norma X.25 es el estándar para redes de paquetes recomendado por CCITT, el cual emitió el primer borrador en 1974. Este original seria revisado en 1976,en 1978 y en 1980, y de nuevo en 1984, para dar lugar al texto definitivo publicado en 1985. En la actualidad, X.25 es la norma de interfaz orientada al usuario de mayor difusión en las redes de paquetes de gran cobertura.

Para que las redes de paquetes y las estaciones de usuario se puedan interconectar se necesitan unos mecanismos de control, siendo el mas importante desde el punto de vista de la red, el control de flujo, que sirve para evitar la congestión de la red. También el ETD ha de controlar el flujo que le llega desde la red. Además deben existir procedimientos de control de errores que garanticen la recepción correcta de todo el trafico. X.25 proporciona estas funciones de control de flujo y de errores.

La X.25 se define como la interfaz entre equipos terminales de datos y equipos de terminación del circuito de datos para terminales que trabajan en modo paquete sobre redes de datos publicas.

Las redes utilizan las redes X.25 para establecer los procedimientos mediante los cuales dos ETD que trabajan en modo paquete se comunican a través de la red. Este estándar pretende proporcionar procedimientos comunes de establecimiento de sesión e intercambio de datos entre un ETD y una red de paquetes(ETCD). Entre estos procedimientos se encuentran funciones como las siguientes: identificación de paquetes procedentes de ordenadores y terminales concretos, asentimiento de paquetes, rechazo de paquetes, recuperación de errores y control de flujo.

El estándar X.25 no incluye algoritmos de encaminamiento, pero conviene resaltar que, aunque los interfaces ETD/ETCD de ambos extremos de la red son independientes uno de otro, X.25 interviene desde un extremo hasta el otro, ya que el trafico seleccionado se encamina desde el principio hasta el final. A pesar de ello, el estándar recomendado es asimétrico ya que solo se define un lado de la interfaz con la red(ETD/ETCD).

4.1 Niveles de la X.25

El Nivel Físico

La recomendación X.25 para el nivel de paquetes coincide con una de las recomendaciones del tercer nivel ISO. X.25 abarca el tercer nivel y también los dos niveles más bajos. El interfaz de nivel físico recomendado entre el ETD y el ETCD es el X.21. X.25 asume que el nivel físico X.21 mantiene activados los circuitos T (transmisión) y R (recepción) durante el intercambio de paquetes. Asume también, que el X.21 se encuentra en estado 13S (enviar datos), 13R (recibir datos) o 13(transferencia de datos). Supone también que los canales C (control) e I(indicación)

de X.21 están activados. Por todo esto X.25 utiliza el interfaz X.21 que une el ETD y el ETCD como un "conducto de paquetes", en el cual los paquetes fluyen por las líneas de transmisión (T) y de recepción (R).

El nivel físico de X.25 no desempeña funciones de control significativas. Se trata más bien de un conducto pasivo, de cuyo control se encargan los niveles de enlace y de red.

El Nivel de Enlace

En X.25 se supone que el nivel de enlace es LAPB. Este protocolo de línea es un conjunto de HDLC. LAPB y X.25 interactúan de la siguiente forma: En la trama LAPB, el paquete X.25 se transporta dentro del campo I (información). Es LAPB el que se encarga de que lleguen correctamente los paquetes X.25 que se transmiten a través de un canal susceptible de errores, desde o hacia la interfaz ETD/ETCD. La diferencia entre paquete y trama es que los paquetes se crean en el nivel de red y se insertan dentro de una trama, la cual se crea en nivel de enlace.

Para funcionar bajo el entorno X.25, LAPB utiliza un subconjunto específico de HDLC. Los comandos que maneja son: Información (I), Receptor Preparado (RR), Rechazo (REJ), Receptor No Preparado (RNR), Desconexión (DSC), Activar Modo de Respuesta Asíncrono (SARM) y Activar Modo Asíncrono Equilibrado(SABM). Las respuestas utilizadas son las siguientes: Receptor Preparado(RR), Rechazo(REJ), Receptor No Preparado(RNR), Asentimiento No Numerado(UA), Rechazo de Trama(FRMR) y Desconectar Modo(DM).

Los datos de usuario del campo I no pueden enviarse como respuesta. De acuerdo con las reglas de direccionamiento HDLC, ello implica que las tramas I siempre contendrán la dirección de destino con lo cual se evita toda posible ambigüedad en la interpretación de la trama.

X.25 exige que LAPB utilice direcciones específicas dentro del nivel de enlace.

En X.25 pueden utilizarse comandos SARM y SABM con LAP y LAPB, respectivamente. No obstante se aconseja emplear SABM, mientras que la combinación SARM con LAP es poco frecuente.

Tanto X.25 como LAPB utilizan números de envió (S) y de recepción (R) para contabilizar el trafico que atraviesan sus respectivos niveles.

En LAPB los números se denotan como N(S) y N(R), mientras que en X.25 la notación de los números de secuencia es P(S) y P(R).

Caracteristicas

X.25 trabaja sobre servicios basados en circuitos virtuales. Un circuito virtual o canal lógico es aquel en el cual el usuario percibe la existencia de un circuito físico dedicado exclusivamente al ordenador que el maneja, cuando en realidad ese circuito físico "dedicado" lo comparten muchos usuarios. Mediante diversas técnicas de multiplexado estadístico, se entrelazan paquetes de distintos usuarios dentro de un mismo canal. Las prestaciones del canal son lo bastante buenas como para que el usuario no advierta ninguna degradación en la calidad del servicio como consecuencia del trafico que le acompaña en el mismo canal. Para identificar las conexiones en la red de los distintos ETD, en X.25 se emplean números de canal lógico (LCN). Pueden asignarse hasta 4095 canales lógicos y sesiones de usuario a un mismo canal físico.

4.2 Opciones del canal X.25

El estándar X.25 ofrece cuatro mecanismos para establecer y mantener las comunicaciones.

Circuito virtual permanente (Permanent Virtual Circuit-PVC) Un circuito virtual permanente es algo parecido a una línea alquilada en una red telefónica, es decir, el ETD que transmite tiene asegurada la conexión con el ETD que recibe a través de la red de paquetes.

En X.25, antes de empezar la sesión es preciso que se haya establecido un circuito virtual permanente. Por tanto, antes de reservarse un circuito virtual permanente, ambos usuarios han de llegar a un acuerdo con la compañía explotadora de la red. Una vez hecho esto, cada vez que un ETD emisor envía un paquete a la red la información identificativa de ese paquete (el numero del canal lógico) indicara a la red que el ETD solicitante posee un enlace virtual permanente con el ETD receptor. En consecuencia, la red establecerá una conexión con el ETD receptor, sin ningún otro arbitraje o negociación de la sesión. El PVC no necesita procedimiento de establecimiento ni de liberación. El canal lógico esta siempre en modo de transferencia de información.

Llamada virtual (VC).

Una llamada virtual recuerda en cierto modo a alguno de los procedimientos asociados con las líneas telefónicas habituales. El ETD de origen entrega a la red un paquete de solicitud de llamada con un 11 como numero de canal lógico (LCN). La red dirige ese paquete de solicitud de llamada al ETD de destino, el cual lo recibe como paquete de llamada entrante procedente de su nodo de red con un LCN de valor 16.

La numeración del canal lógico se lleva a cabo en cada extremo de la red. Lo mas importante es que la sesión entre los ETD este identificada en todo momento con los números LCN 11 y 16. Los números de canal lógico sirven para identificar de forma univoca las diversas sesiones

de usuarios que coexisten en el circuito físico en ambos extremos de la red. En el interior de la red, los nodos de conmutación de paquetes pueden mantener su propia numeración LCN.

Si el ETD receptor decide aceptar y contestar la llamada entregara a la red un paquete de llamada aceptada. La red transportara entonces este paquete al ETD que llama, en forma de paquete de llamada conectada. Después del establecimiento de la llamada el canal entrara en estado de transferencia de datos. Para concluir la sesión, cualquiera de los dos ETD puede enviar una señal de solicitud de liberación. Esta indicación es recibida y se confirma mediante un paquete de confirmación de liberación.

Las redes orientadas a conexión exigen que se haya establecido un enlace antes de empezar a intercambiar datos. Una vez que el ETD receptor ha aceptado la solicitud de llamada comienza el intercambio de datos según el estándar X.25.

Selección rápida.

La filosofía básica del datagrama que consiste en eliminar la sobrecarga que suponen los paquetes de establecimiento y liberación de la sesión tiene su utilidad en determinadas aplicaciones, por ejemplo en aquellas en las que las sesiones son muy cortas o las transacciones muy breves. Por eso se ha incorporado al estándar una posibilidad de selección rápida.

La selección rápida ofrece dos alternativas: La primera de ellas se denomina selección rápida y consiste en que en cada llamada, un ETD puede solicitar esta facilidad al nodo de la red (ETCD) mediante una indicación al efecto en la cabecera del paquete. La facilidad de llamada rápida admite paquetes de solicitud de llamada de hasta 128 octetos de usuario. El ETD llamado puede, si lo desea, contestar con un paquete de llamada aceptada que a su vez puede incluir datos de usuario. El paquete de solicitud de llamada/llamada entrante indica si el ETD remoto ha de contestar con un paquete de solicitud de liberación o con una llamada aceptada. Si lo que se transmite es una aceptación de la llamada la sesión X.25 sigue su curso, con los procedimientos de transferencia de datos y de liberación del enlace habituales en las llamadas virtuales conmutadas.

La selección rápida ofrece una cuarta función de establecimiento de llamada propia del interfaz X.25: la selección rápida con liberación inmediata. Al igual que en la otra opción de selección rápida, una solicitud de llamada en esta modalidad puede incluir también datos de usuario. Este paquete se transmite a través de la red al ETD receptor, el cual, una vez aceptados los datos, envía un paquete de liberación de la llamada (que a su vez incluye datos de usuario). Este paquete es recibido por el nodo de origen el cual lo interpreta como una señal de liberación del enlace, ante la cual devuelve una confirmación de la desconexión que no puede incluir datos de

usuario. En resumen, el paquete enviado establece la conexión a través de la red, mientras que el paquete de retorno libera el enlace.

La selección rápida esta pensada para aplicaciones basadas en transacciones. Sin embargo, puede prestar también un valioso servicio en aplicaciones como la entrada rechazada de trabajos (RJE) o en la transferencia masiva de trabajos. Una selección rápida puede tener por ejemplo 128 octetos que serán examinados por el ETD receptor para determinar si puede aceptar una sesión intensiva y prolongada. La respuesta de aceptación incluirá la autorización para ello- tal vez incluya también las reglas que gobiernan la transferencia de datos entre ambas aplicaciones de usuario.

4.3 Principios de control de flujos

X.25 permite al dispositivo de usuario (ETD) o al distribuidor de paquetes (ETCD) limitar la velocidad de aceptación de paquetes. Esta característica es muy útil cuando se desea controlar si una estación recibe demasiado tráfico.

El control de flujo puede establecerse de manera independiente para cada dirección y se basa en las autorizaciones de cada una de las estaciones. El control de flujo se lleva a cabo mediante diversos paquetes de control X.25, además de los números de secuencia del nivel de paquete.

4.4 Otros tipos de paquetes

La recomendación X.25 maneja otros tipos de paquetes:

El procedimiento de interrupción permite que un ETD envié a otro un paquete de datos sin numero de secuencia, sin necesidad de seguir los procedimientos normales de control de flujo establecidos por la norma X.25. El procedimiento de interrupción es útil en aquellas situaciones en las que una aplicación necesite transmitir datos en condiciones poco habituales. Así por ejemplo, un mensaje de alta prioridad puede enviarse como paquete de interrupción, para garantizar que el ETD receptor acepta los datos. Un paquete de interrupción puede contener datos de usuario (un máximo de 32 octetos). El empleo de estas interrupciones afecta a los paquetes normales que circulan por el circuito virtual, ya sea conmutado o permanente. Una vez enviado un paquete de interrupción es preciso esperar la llegada de una confirmación de la interrupción antes de enviar a través del canal lógico un nuevo paquete de interrupción.

Los paquetes de Receptor Preparado (RR) y de Receptor no Preparado(RNR) se usan de forma parecida a sus comandos homónimos del protocolo HDLC y del subconjunto LAPB. Desempeñan una importante tarea de controlar el flujo iniciado por los dispositivos de usuario.

Ambos paquetes incluyen un número de secuencia de recepción en el campo correspondiente, para indicar cual es el siguiente numero de secuencia que espera el ETD receptor. El paquete RR sirve para indicar al ETD/ETCD emisor que puede empezar a enviar paquetes de datos, y también utiliza el número de secuencia de recepción para acusar recibo de todos los paquetes transmitidos con anterioridad. Al igual que el comando de respuesta RR de HDLC, el paquete RR puede servir simplemente para acusar recibo de los paquetes que han llegado cuando el receptor no tiene ningún paquete específico que enviar al emisor.

El paquete RNR sirve para pedir al emisor que deje de enviar paquetes. También existe un campo de secuencia de recepción con el cual se asientan todos los paquetes recibidos con anterioridad. El RNR suele usarse cuando durante un cierto periodo de tiempo la estación es incapaz de recibir tráfico. Conviene señalar que si un ETD concreto genera un RNR, lo más probable es que la red genere otro RNR para el ETD asociado, con el fin de evitar que se genere en la red un tráfico excesivo. La capacidad de almacenamiento y espera en cola en los nodos de conmutación de paquetes de la red no es ilimitada. Por eso un RNR a veces conduce al estrangulamiento de ambos extremos de la sesión ETD/ETCD.

Estos dos paquetes proporcionan a X.25 un sistema de control de flujo que va más allá que el que ofrece el nivel de enlace LAPB. Así pues, se dispone de control de flujo y control de ventanas a dos niveles: en el nivel de enlace para LAPB y en el nivel de red para X.25.

Sin embargo, el nivel de enlace no ofrece un control de flujo eficaz para los desposito de usuario (ETD) individuales; por el contrario, en el nivel de red, X.25 emplea los RR y RNR con números específicos del canal lógico, para llevar a cabo las operaciones de control de flujo.

Cualquier nodo que tenga asignado un número de canal lógico puede efectuar este control de flujo. En algunas redes, se asigna un bloque de números de canal lógico al ordenador central y este se encarga de gestionar los LCN de sus terminales y programas de aplicación.

El paquete de rechazo (REJ) sirve para rechazar de forma específica un paquete recibido. Cuando se utiliza, la estación pide que se retransmitan los paquetes, a partir del número incluido en el campo de recepción de paquetes.

Los paquetes de reinicialización (reset) sirven para reinicializar un circuito virtual permanente o conmutado. El procedimiento de reinicialización elimina en ambas direcciones, todos los paquetes de datos y de interrupción que pudieran estar en la red. Estos paquetes pueden ser necesarios también cuando aparecen determinados problemas, como es la perdida de paquetes, su duplicación, o la perdida de secuencia de los mismos. La reinicialización solo se utiliza en modo de transferencia de información y puede ser ordenada por el ETD (solicitud de reinicialización) o por la propia red (indicación de reinicialización).

El procedimiento de reiniciación (restart) sirve para inicializar o reinicializar el interfaz del nivel de paquetes entre el ETD y el ETCD. Puede afectar hasta 4095 canales lógicos de un puerto físico. Este procedimiento libera todas las llamadas virtuales y reinicializa todos los circuitos virtuales permanentes del interfaz. La reiniciación puede presentarse como consecuencia de algún problema serio, como es la caída de la red. Todos los paquetes pendientes se pierden, y deberán ser recuperados por algún protocolo de nivel superior.

En ocasiones, la red generara una reiniciación al arrancar o reinicializar el sistema para garantizar que todas las sesiones empiecen desde 0.

Cuando un ETD haya enviado una señal de reiniciación, la red habrá de enviar una reiniciación a cada uno de los ETD que tengan establecida una sesión de circuito virtual con el ETD que genero la reiniciación. Los paquetes de reiniciación pueden incluir también códigos que indiquen el motivo de tal evento.

Dentro de la red de paquetes pueden perderse algunos paquetes de usuario. Ello puede suceder también en una red X.25. Los paquetes de liberación, reiniciación y reinicialización pueden provocar que la red ignore los paquetes aun no cursados. Una situación así no es demasiado infrecuente ya que en muchos casos estos paquetes de control llegan a su destino antes de que lo hayan hecho todos los paquetes de usuario. Los paquetes de control no están sometidos al retardo inherente a los procedimientos de control de flujo que afectan a los paquetes de usuario. Por tanto, los protocolos de nivel superior están obligados a tener en cuenta estos paquetes perdidos.

Dentro de la red pueden perderse algunos paquetes de usuario. Esto puede suceder también en una red X.25. Los paquetes de liberación, reiniciación y reinicialización pueden provocar que la red ignore los paquetes aun no cursados. Una situación así no es demasiado infrecuente, ya que en muchos casos estos paquetes de control llegan a su destino antes de que lo hayan hecho todos los paquetes de usuario. Los paquetes de control no están sometidos al retardo inherente a los procedimientos de control de flujo que afectan a los paquetes de usuario. Por lo tanto, los protocolos de nivel superior están obligados a tener en cuenta estos paquetes perdidos.

Dentro de la red X.25, el paquete de liberación (clear) desempeña diversas funciones, aunque la principal es el cierre de una sesión entre dos ETD. Otra de sus misiones consiste en indicar que no puede llevarse a buen término una solicitud de llamada. Si el ETD remoto rechaza la llamada enviara a su nodo de red una solicitud de liberación. Este paquete será transportado a través de la red al nodo de red de origen, el cual entregara a su ETD una indicación de liberación. El cuarto octeto del paquete contiene un código que indica el motivo de la liberación.

4.5 Temporizador para los ETD y ETCD

Los temporizadores se emplean para establecer límites en el tiempo de establecimiento de las conexiones, en la liberación de canales, en la reinicialización de una sesión, etc. Si no existiesen estos relojes, un usuario podría quedar a la espera de un acontecimiento indefinidamente, si este no se verifica. Los temporizadores obligan simplemente a X.25 a tomar una decisión en caso de que suceda algún problema; por tanto, ayudan a resolver los errores.

4.6 Formatos de paquetes

En un paquete de datos, la longitud por omisión del campo de datos de usuario es de 128 octetos, aunque X.25 ofrece opciones para distintas longitudes. Otros tamaños autorizados son: 16, 32, 64, 256, 512, 1024, 2048 y 4096 octetos. Si el campo de datos de un paquete supera la longitud máxima permitida el ETD receptor liberará la llamada virtual generando un paquete de reinicialización.

Todo paquete que atraviesa el interfaz ETD/ETCD con la red debe incluir al menos tres octetos, los de la cabecera del paquete, aunque esta puede incluir también otros octetos adicionales.

Los 4 primeros bits del primer octeto contienen el número de grupo del canal lógico. Los 4 últimos bits del primer octeto contienen el identificador general de formato. Los bits 5 y 6 del identificador general de formato(SS) sirven para indicar el tipo de secuenciamiento empleado en las sesiones de paquetes . X.25 admite dos modalidades de secuenciamiento: módulo 8(con números entre 0 y 7) y módulo

128(con números entre 0 y 127). El BIT D, séptimo BIT del identificador general de formato solo se utiliza en determinados paquetes. El octavo BIT es el BIT O, y solo se emplea para paquetes de datos destinado al usuario final. Sirve para establecer dos niveles de datos de usuario dentro de la red.

El segundo octeto de la cabecera del paquete contienen el número de canal lógico (LCN). Este campo de 8 bits, en combinación con el número de grupo del canal lógico, proporciona los doce bits que constituyen la identificación completa del canal lógico; por tanto, son 4095 los canales lógicos posibles. El LCN 0 está reservado para las funciones de control (paquetes de diagnóstico y de reinicialización).

Las redes utilizan estos dos campos de diversas formas. En algunas se emplean combinados, mientras que en otras se consideran de forma independiente.

Los números de canal lógico sirven para identificar el ETD frente al nodo de paquetes (ETCD), y viceversa. Estos números pueden asignarse a circuitos virtuales permanentes, llamadas entrantes y salientes, llamadas entrantes, y por último llamadas salientes.

Durante el comienzo del proceso de comunicación, es posible que el ETD y el ETCD utilicen el mismo LCN. Así por ejemplo, una solicitud de llamada generada por un ETD podría emplear el mismo número de canal lógico que una llamada conectada correspondiente a un ETCD. Para reducir al mínimo esta posibilidad, la red comienza a buscar un número a partir del extremo inferior, mientras que el ETD busca su número empezando por arriba. Si la llamada saliente (solicitud de llamada) de un ETD tiene el mismo LCN que una llamada entrante(llamada conectada) procedente del ETCD de la red, X.25 liberará la llamada entrante y procesará la solicitud de llamada.

Cuando el paquete no es de datos, el tercer octeto de la cabecera de paquete X.25 es el de identificador de tipo de paquete, mientras que cuando es de datos ese octeto es el de secuenciamiento.

En los paquetes de establecimiento de llamada se incluyen también las direcciones de los ETD y las longitudes de estas direcciones. El convenio de direccionamiento utilizado podría ser por ejemplo, el estándar X.121. Los campos de direccionamiento pueden estar contenidos entre el cuarto y el decimonoveno octeto del paquete de solicitud de llamada. En los paquetes de establecimiento de llamadas, estos campos de direccionamiento sirven para identificar las estaciones interlocutoras: la que llama y la que contesta. A partir de este momento, la red utilizará los números de canal lógico asociados para identificar la sesión entre los dos ETD. Existen también otros campos de facilidad que pueden emplearse cuando los ETD deseen aprovechar algunas de las opciones del estándar X.25. Por último el paquete puede transportar datos de llamada del propio usuario. El espacio máximo para datos de usuario que admiten los paquetes de solicitud de llamada es de 16 octetos. Este campo es útil para transportar ciertas informaciones dirigidas al ETD receptor, como por ejemplo palabras de acceso, información de tarificación, También utiliza estos datos el protocolo X.29. Para determinadas opciones como la llamada rápida, está permitido incluir hasta 128 octetos de usuario.

La cabecera del paquete se modifica con el fin de facilitar el movimiento de datos de usuario por la red. El tercer octeto de la cabecera, normalmente reservado para el identificador de tipo de paquete, se descompone en dos campos independientes:

Bits.....Descripción o valor

1.....0

2 - 4.....Secuencia de envío del paquete [P(S)]

5.....BIT de mas datos(el BIT M)

6 - 8.....Secuencia de recepción de paquetes [P(R)]

Las misiones de estos campos son las siguientes: si el primer BIT vale 0, indica que se trata de un paquete de datos. El número de secuencia de envió [P(S)] tiene asignados tres bits. Otro BIT lleva a cabo la función de bit M. Por último los tres bits restantes se asignan al número de secuencia de recepción [P(R)].

Los números de secuencia de envío y de recepción sirven para coordinar y asentir las transmisiones que tienen lugar entre ETD y ETCD. A medida que un paquete atraviesa la red de un nodo a otro, es posible que los números de secuencia cambien durante el recorrido por los centros de conmutación. Pese a ello, el ETD o ETCD receptor tiene que saber que numero de recepción ha de enviar al dispositivo emisor.

El empleo de P(R) y P(S) en el nivel de red exige que el P(R) sea una unidad mayor que el P(S) del paquete de datos.

4.6.1 El Bit D

La facilidad "BIT D" se añadió en la versión de 1980 de la norma X.25. Sirve para especificar una de las siguientes funciones: cuando este BIT vale 0, el valor de P(R) indica que es la red la que asiente los paquetes; cuando el BIT D vale 1, la confirmación de los paquetes se realiza de extremo a extremo, es decir, es el otro ETD el que asiente los datos enviados por el ETD emisor. Cuando se utiliza el BIT D con valor 1, X.25 asume una de las funciones del nivel de transporte: la contabilización de extremo a extremo.

4.6.2 El Bit M

El BIT M (Más datos) indica que existe una cadena de paquetes relacionados atravesando la red. Ello permite que tanto la red como los ETD identifiquen los bloques de datos originales cuando la red los ha subdividido en paquetes más pequeños. Así por ejemplo, un bloque de información relativo a una base de datos debe presentarse al ETD receptor en un determinado orden.

4.7 Paquetes A y B

La combinación de los BIT M y D establece dos categorías dentro del estándar X.25 que se designan como paquetes A y paquetes B.

Gracias a ello los ETD o ETCD pueden combinar el secuenciamiento de dos o más paquetes y la red puede también combinar paquetes.

En X.25, una secuencia de paquetes completa se define como un único paquete B y todos los paquetes contiguos tipo A que lo precedan (si es que hay alguno).

Un paquete de categoría B sirve para cerrar una secuencia de paquetes relacionados con el tipo A. Por contra los paquetes A representan la transmisión en curso, han de contener datos, y deben llevar el BIT M a 1 y el BIT D a 0. Sólo los paquetes tipo B pueden tener el BIT D a 1 para realizar confirmaciones de extremo a extremo. La red puede agrupar una serie de paquetes A y el paquete B subsiguiente dentro de un solo paquete, pero los paquetes B han de mantener las entidades independientes en paquetes independientes.

La combinación de paquetes puede resultar útil cuando se empleen paquetes de distintas longitudes a través de una ruta de la red, o cuando las subredes de un sistema de redes interconectadas empleen distintos tamaños de paquete. De este modo es posible manejar los paquetes a nivel lógico como un todo. En este caso, puede usarse el BIT M para señalar al ETD receptor que los paquetes que llegan están relacionados y siguen una determinada secuencia.

Uno de los objetivos de los bits M y D es la combinación de paquetes. Por ejemplo, si el campo de datos del ETD receptor es más largo que el del ETD emisor, la red puede combinar los paquetes dentro de una secuencia completa.

4.8 El Bit Q

Este BIT es opcional, y puede usarse para distinguir entre datos de usuario y informaciones de control.

Control de flujo y ventanas

X.25 emplea técnicas de control de flujo y ventanas muy similares a las de HDLC, LAPB y otros protocolos de línea. En un paquete de datos se combinan dos números de secuencia (el de envío y el de recepción) para coordinar el intercambio de paquetes entre el ETD y el ETCD. El esquema de numeración extendida permite que el número de secuencia tome valores hasta 127(módulo 128). En el interfaz ETD/ETCD, los paquetes de datos se controlan separadamente para cada dirección basándose en las autorizaciones que los usuarios envían en forma de números de secuencia de recepción o de paquetes de control "receptor preparado"(RR) y "receptor no preparado".

La razón de que exista control de flujo tanto en el nivel de red como en el de paquetes es que se multiplexan muchos usuarios en un mismo enlace físico y si se emplease un RNR en el nivel

físico podrían estrangularse todos los canales lógicos incluidos en ese enlace. El control de flujo que incorpora X.25 permite aplicar este estrangulamiento de forma más selectiva. Además, la incorporación del secuenciamiento en el nivel de interfaz con la red proporciona un grado adicional de contabilidad y seguridad para los datos de usuario.

La numeración de los paquetes en este tercer nivel se lleva a cabo de forma muy similar a la del segundo nivel del estándar HDLC/LAPB.

El ciclo de los números de secuencia de los paquetes va de 0 a 7, y regresa a 0 de nuevo. Si se emplea el sistema módulo 128, el ciclo de secuenciamiento va de 0 a 127 y vuelve a 0.

En X.25 las ventanas que establece el esquema de módulo sirven para prevenir la saturación de paquetes. No obstante, en X.25 se recomienda un tamaño normalizado de ventana de dos posiciones, aunque pueden incorporarse también otros tamaños en las redes. Este valor dos limita el flujo de paquetes que pueden estar pendientes de servicio en un momento dado. Tal limitación obliga a procesar más deprisa los asentimientos de los paquetes que llegan al ETD receptor. También reduce el número de paquetes que puede tener pendientes la propia red en un determinado instante.

4.9 Facilidades X.25

Las facilidades se invocan mediante instrucciones concretas dentro del paquete de solicitud de llamada. Su clasificación es:

1. Facilidades internacionales.

2. Facilidades de ETD especificadas por CCITT.

3. Facilidades ofrecidas por la red pública de datos de origen.

4. Facilidades ofrecidas por la red pública de datos de destino.

Notificación de la facilidad en línea. Esta facilidad permite al ETD, en cualquier momento, solicitar facilidades u obtener los parámetros de las facilidades tal y como los entiende el ETCD. Para el dialogo entre el ETD y el ETCD se emplean los paquetes de notificación que aparecen en la tabla "Tipos de paquetes". Estos mismos paquetes indican si puede gestionarse el valor de la facilidad.

Numeración de paquetes extendida. Esta facilidad proporciona el esquema de numeración de secuencias módulo 128. En su ausencia lo que se emplea es el módulo 7.

Modificación del BIT D. Esta facilidad está pensada para usarse con equipos ETD desarrollados con anterioridad a la introducción del procedimiento del BIT D. Permite trabajar con asentimiento de extremo a extremo.

Retransmisión de paquetes. Un ETD puede solicitar al ETCD la retransmisión de uno o varios paquetes de datos. Para ello el ETD especifica, dentro de un paquete de rechazo, el número de canal lógico y un valor de P(R). El ETCD deberá retransmitir todos los paquetes comprendidos entre el número P(R) y el siguiente que tuviera que enviar por primera vez. Esta facilidad es similar a la técnica de rechazo no selectivo que utilizan los protocolos de línea en el segundo nivel del modelo ISA.

Obstrucción de las llamadas entrantes. Obstrucción de las llamadas salientes. Estas facilidades impiden que el ETCD presente llamadas entrantes al ETD, o que el ETCD presente llamadas salientes del ETD.

Canal lógico unidireccional entrante. Canal lógico unidireccional saliente. Estas facilidades solo permiten al canal lógico aceptar en el primer caso o enviar llamadas en el segundo pero no ambas cosas. Su función es similar a las facilidades de obstrucción salvo en que ahora la restricción afecta solo a canales individuales.

Tamaño de paquetes por omisión no estándar. Permite seleccionar el tamaño de paquetes que la red admitirá por omisión. Para gestionar el tamaño de los paquetes pueden emplearse paquetes de notificación.

Tamaño de ventana por omisión estándar. Permite ampliar el tamaño de las ventanas por encima del valor por defecto dos para todas las llamadas.

Asignación de clases de velocidad de transmisión por defecto. Esta facilidad permite seleccionar una de las siguientes velocidades de transmisión (en bits por segundo): 75, 150, 300, 600, 1200, 2400, 4800, 9600, 19200 y 48000. Pueden gestionarse también otros valores.

Negociación de los parámetros de control de flujo. Esta facilidad permite variar el tamaño de una ventana de una llamada a otra. A veces un ETD sugiere el tamaño de la ventana durante el establecimiento de la llamada. En algunas redes estos parámetros deben ser los mismos para ambos ETD.

Negociación de la clase de velocidad de transmisión. Permite modificar la velocidad de transmisión de una llamada a otra.

Grupo cerrado de usuarios (CUG). Conjunto de funciones que permite a los usuarios formar grupos de ETD de acceso restringido. Esta facilidad proporciona a la red pública un nuevo

grado de seguridad y privacidad. Incluye diversas opciones como el acceso en un solo sentido entrante o saliente. Por lo general, la estación que llama especifica el grupo cerrado de usuarios que desea mediante los campos de facilidad incluidos en el paquete de solicitud de llamada. Si la estación solicitada no es miembro de ese grupo la red rechaza la llamada.

Grupo cerrado de usuarios bilateral. Esta facilidad es similar a la anterior, pero permite establecer restricciones de acceso entre pares de ETD.

Selección rápida. Aceptación rápida de la selección. Cobro revertido. Aceptación del cobro revertido. Estas facilidades permiten cargar el coste de la llamada al ETD receptor. Pueden usarse con llamadas virtuales y con selecciones rápidas.

Prevención de cobros locales. Esta facilidad autoriza al ETCD a rechazar las llamadas que tenga que pagar su ETD. Por ejemplo, un ETD puede no estar autorizado a aceptar los cobros revertidos de ningún ETD que llame.

Identificación del usuario de la red. Esta facilidad permite que el ETD que llama entregue a su ETCD la información de tarificación, seguridad o gestión, llamada por llamada. Si no es válida esta información la llamada no se cursa.

Información de tarificación. Esta facilidad permite que el ETCD informe a su ETD sobre las condiciones de tarificación de la sesión de paquetes en curso.

Selección de compañía. Permite que el ETD que llama escoja una o varias compañías telefónicas para gestionar su sesión de paquetes.

Grupo local. Esta facilidad se encarga de distribuir las llamadas que lleguen entre un grupo preestablecido de interfaces ETD/ETCD. Esta mejora de la versión 1984 permite a los usuarios seleccionar múltiples puertos de un ordenador o procesador frontal, o escoger entre varios de estos sistemas dentro de un mismo nodo de usuario. Se trata de una posibilidad muy útil en aquellas organizaciones equipadas con grandes sistemas informáticos que necesiten flexibilidad para asignar tareas a los distintos recursos. La idea es similar al selector de puertos que puede verse en muchas instalaciones.

Redireccionamiento de la llamada. Esta facilidad, también fruto de la revisión de 1984, redirige la llamada cuando el ETD de destino está averiado, comunica, o cuando ha solicitado expresamente que se reoriente la llamada. Permite orientar las comunicaciones entrantes hacia algún ETD de apoyo, que se encargará de solucionar los posibles problemas y de mantener al usuario final aislado de los fallos. El Redireccionamiento de llamadas permite también redirigir la llamada a distintas zonas de un país o continente por cuestiones relacionadas con los usos horarios.

Notificación del cambio en la dirección de la llamada. En caso de que se haya producido la redirección de una llamada, esta facilidad explica al ETD que llama por qué la dirección de destino de la llamada conectada o del paquete indicador de liberación es distinta de la dirección del paquete de petición de llamada del ETD.

Notificación de redireccionamiento de llamada. Cuando se produce un redireccionamiento de llamada, esta facilidad informa del hecho al ETD alternativo, indicándole además por qué ha cambiado la dirección del ETD original.

Indicación y selección del retardo de tránsito. Esta última facilidad permite al ETD seleccionar un determinado tiempo de tránsito por la red de paquetes. Esta función puede ser de gran utilidad para el usuario final, pues le confiere un cierto control sobre la velocidad de respuesta de la red.

4.10 El PAD (ensamblado /desensabladode paquetes)

Durante el desarrollo de la recomendación X.25, en los años sesenta, los organismos de normalización advirtieron que la mayoría de los terminales en funcionamiento eran dispositivos asíncronos no inteligentes. Se hacía necesario un interfaz que conectase a estos equipos con las redes de paquetes. Con el fin de hacer frente a esto, se desarrollaron estándares para dotar a los terminales asíncronos de capacidades de conversión de protocolos y de ensamblado/desensamblado de paquetes (PAD). PAD es un servicio que se ofrece al usuario para permitirle conectarse con una red de paquetes. Tras el primer borrador de la norma X.25, aparecido en 1976, los comités de normalización editaron en 1977 una nueva recomendación en la que aparecían tres especificaciones relativas a los interfaces para terminales asíncronos: X.3, X.28 y X.29.

La idea del PAD es ofrecer una conversión de protocolos entre un dispositivo de usuario (ETD) y una red pública o privada, junto con otra conversión complementaria en un extremo receptor de la red. Se trata de conseguir un servicio transparente para los ETD de usuario. La norma X.3 y sus normas accesorias X.28 y X.29 sólo están pensadas para dispositivos asíncronos, pero muchos fabricantes ofrecen otros servicios tipo PAD capaces de aceptar protocolos como BSC o SDLC. Estas opciones no asíncronas del esquema PAD se encuentran dentro de la filosofía de X.3, X.28 y X.29.

Los estándares PAD permiten diversas configuraciones. En la figura 8 se ve la conexión entre un ETD de usuario no generador de paquetes y otro ETD capaz de operar en modo paquete. Obsérvese que el PAD (X.3) y el X.28 sólo es necesario en los ETD asíncronos.

X.3. La versión X.3 de 1984 proporciona una serie de 22 parámetros, que son utilizados por el PAD para identificar y atender a cada una de las terminales con las que se comunica. Cuando se establece una conexión con el PAD desde un ETD de usuario. El usuario puede también alterar estos parámetros una vez iniciada su sesión con el PAD. Cada uno de estos 22 parámetros consta de un número de referencia y de una serie de valores. Ejemplos de parámetros:

Parámetro 3 = 0 Ordena al PAD que envíe sólo paquetes llenos

Parámetro 3 = 2 Ordena al PAD que envíe el paquete una vez que el terminal entregue un carácter de retorno de carro.

Parámetro 6 = 1 Un terminal de usuario desea recibir las señales de servicio del PAD. Es útil para localizar averías.

Parámetro 7 = 1 Cuando reciba del terminal un carácter de interrupción (break), el PAD enviará un paquete de interrupción al ETD receptor.

X.28. En este estándar se definen los procedimientos de control de flujo entre el terminal de usuario y el PAD. Una vez recibida una conexión inicial desde el ETD de usuario, el PAD establece el enlace y proporciona los servicios propios de la norma X.28. El ETD de usuario entrega al PAD diversos comandos X.28, y el PAD solicita de X.25 una llamada virtual con el ETD remoto. A partir de entonces, el PAD será responsable de transmitir los paquetes adecuados de solicitud de llamada X.25. Existen los siguientes procedimientos:

Establecimiento de trayectoria.

Inicialización del servicio.

Intercambio de datos.

Intercambio de información de control.

Con X.28, cuando un PAD recibe un comando procedente de un terminal, está obligado a devolver una respuesta. También pueden definirse dos perfiles para atender al ETD de usuario. Con el perfil transparente, el PAD que atiende el servicio es transparente para ambos ETD, es decir, que los dos ETD "piensan" que existe una conexión virtual entre ellos. En esta situación, el ETD remoto debe encargarse de algunas funciones PAD, como es la comprobación de errores. El perfil simple, por el contrario, atiende las solicitudes del usuario mediante las opciones que proporciona la norma X.3 y las funciones de parámetros.

Un ejemplo de comandos y señales de servicio X.28 sería el siguiente: SET 3:0,6:1. Esto significa que asignar el valor 0 al parámetro 3 y el valor 1 al parámetro 6.

X.29. Este estándar indica al PAD y a la estación remota cómo deben intercambiar funciones de control dentro de una llamada X.25. X.29 permite que el intercambio de información tenga lugar en cualquier momento, ya sea en la fase de transporte de datos o en cualquier otra etapa de la llamada virtual.

La secuencia del BIT Q gobierna algunas de las funciones de X.29. El BIT Q(BIT cualificador de datos) lo utiliza el ETD remoto para distinguir los paquetes de información de usuario(Q=0) y paquetes que contienen información esencial del PAD(Q=1). X.29 resulta especialmente útil cuando un ordenador central necesita modificar los parámetros de funcionamiento X.3 de los terminales conectados a él.

Para reconfigurar sus estaciones de trabajo, el ordenador central puede enviar un paquete de control X.29 a un PAD, con el BIT Q puesto a 1.

En X.29 están definidos siete mensajes de control, llamados mensajes del PAD. En concreto:

Establecer (set): modifica un valor X.3

Leer (read): lee un valor X.3

Establecer y leer: modifica un valor X.3 y pide confirmación del hecho al PAD.

Indicación de parámetros: se devuelve en respuesta a los comandos anteriores.

Invitación a liberar la llamada: permite al ETD remoto liberar la llamada X.25; el PAD por su parte, libera el terminal local.

Indicación de interrupción (break): el PAD indica que el terminal ha transmitido una señal de interrupción (break).

Error: respuesta a un mensaje inválido del PAD.

4.11 PAD: Formato de paquetes y flujo de paquetes

El paquete PAD tiene un formato similar al del paquete X.25 convencional. Necesita una cabecera de tres octetos, seguida de un campo de control de un octeto y por último los números y valores correspondientes al PAD.

1. Activo: el ETD y el ETCD intercambian un 1 por la interfaz.

2. Solicitud de servicio: se autoriza al PAD para detectar la velocidad de transmisión de los datos y el codigo que utiliza el ETD, y para seleccionar el perfil inicial.

3. ETD en espera: el interfaz queda en estado de espera.

4. Preparado para dar servicio: se entra en este estado una vez que el PAD ha transmitido su señal de identificación.

5. PAD en espera: el PAD queda a la espera de señales de control o de datos.

6. Comando del PAD: a este estado se llega desde diferentes estados de espera. Permite transmitir comandos al PAD.

7. Conexión en curso: en este estado se entra cuando el PAD inicia una conexión con la red.

8. Señales de servicio: autoriza todas las señales de servicio de este estado.

9. Transferencia de datos: permite la transferencia de datos a través de la interfaz.

10. En espera de un comando: en este estado se entra cuando el ETD debe recibir a un comando o dato del PAD.

4.12 El nivel de transporte .

El nivel de transporte exige que el usuario especifique a la red una determinada calidad de servicio. Ha de conocer los distintos tipos de servicio que le ofrecen los niveles inferiores de la red. Una vez recibida la solicitud de calidad de servicio del usuario, el nivel de transporte selecciona una clase de protocolo para hacer frente a tales exigencias. El nivel de transporte asegura al usuario un nivel de servicio consistente incluso aunque sean varias las redes disponibles.

La calidad de los servicios de red depende del tipo de red del que dispongan el usuario final y el nivel de transporte. CCITT, ISO, y ECMA han definido tres clases de redes:

Tipo A. Redes que ofrecen tasas aceptables de error y de señalización de fallos (calidad aceptable).

Tipo B. Redes que proporcionan tasas de error aceptables, pero tasas de señalización de fallos inaceptables (señalización de fallos inaceptables).

Tipo C. Redes cuyas tasas de errores son inaceptables para el usuario (no fiables).

Esta definición de tipos de redes intenta expresar que pueden existir distintas clases de redes, y que el usuario ha de obtener un servicio consistente sea cual sea la clase de red empleada. El nivel de transporte ofrece además al usuario diversas opciones que le permiten obtener de la red con un coste mínimo, servicios orientados a cada conexión.

Considerando las distintas clases de redes que pueden existir, el nivel de transporte permite al usuario establecer los siguientes parámetros de calidad de servicio: caudal efectivo, precisión, fiabilidad, retardo de tránsito, prioridades, protección, multiplexado, control de flujo, detección de errores y segmentación. En la definición de un servicio del nivel de transporte se emplean primitivas para especificar cuales son los servicios a los que hay que acceder a través de los niveles de transporte y de red. Los parámetros asociados a cada una de las primitivas indican las etapas y acciones que deben emprender los distintos niveles. Durante la fase de establecimiento del enlace en la red, los usuarios finales negociarán con el nivel de transporte las características de la conexión. Esta negociación se lleva a cabo mediante las primitivas y sus correspondientes parámetros. Si la red o un usuario final no son capaces de ofrecer las condiciones exigidas, o no consiguen ponerse de acuerdo al respecto, es posible que la conexión no tenga lugar.

Una vez aceptados los parámetros por ambas partes, una de ellas emprende la transferencia de datos desde el nivel de transporte atravesando los tres niveles inferiores y el canal físico. En el nodo de destino, los datos atravesarán en orden inverso esos tres niveles y llegarán al correspondiente nivel de transporte. El nivel de transporte es el que se encarga de seleccionar el protocolo capaz de proporcionar la calidad de servicio especificada por el usuario a través de los correspondientes parámetros. Puesto que el nivel de transporte conoce las características de la red, puede escoger entre cinco clases de procedimientos de protocolo para atender las necesidades de calidad de servicio especificadas por el usuario:

Clase 0: simple.

Clase 1: con recuperación de errores básicos.

Clase 2: con multiplexación.

Clase 3: con recuperación de errores.

Clase 4: con detección de errores y recuperación.

Los protocolos de clase 0 proporcionan un mecanismo muy sencillo de transporte para el establecimiento de la conexión, adecuado para las redes de tipo A. Ofrecen un servicio orientado a la conexión, tanto en la fase de enlace con la red como en la fase de liberación. No ofrecen ningún apoyo a la transferencia de datos del usuario durante el establecimiento de la

conexión. Este protocolo es capaz de detectar y señalizar errores de protocolo. Si el nivel de red informa de algún error al nivel de transporte este libera la conexión con su nivel de red, y el usuario final es informado de tal desconexión.

Los protocolos de clase 1 están asociados con redes como la red de paquetes X.25. Esta clase de protocolo se encarga de segmentar los datos si es necesario; también se ocupa de retener datos y acusar recibo de los mismos; por último, si aparece algún paquete X.25 de reinicialización (reset), lleva a cabo la resincronización de la red. Este protocolo es también necesario para efectuar la transferencia acelerada de datos. Es capaz de responder a solicitudes de desconexión y a errores de protocolo. También es responsable de las operaciones de resincronización y reasignación cuando tiene lugar un fallo en la red.

Dentro de una solicitud de conexión de clase 1 pueden transmitirse datos de usuario. Además, a cada Unidad de Datos del Protocolo (PDU) se le asocia una secuencia para facilitar el asentimiento(ACK) y el rechazo de tramas(NACK), y como ayuda la recuperación de errores. Cada ACK libera la copia que se guarda en el nodo emisor. Los protocolos de clase 1 permiten escoger entre asentimiento por parte del usuario y por parte de la red. Conviene tener presente que los protocolos de clase 1 solo son capaces de recuperar aquellos errores que hayan sido señalizados por la red. No emplean temporizadores que permitan retardos o paquetes desaparecidos.

Los protocolos de clase 2 permiten multiplexar varias conexiones de transporte a través de una misma sesión de red X.25. También se encargan de controlar el flujo y de evitar congestiones en los nodos ETD. No ofrecen detección ni recuperación de errores. Si se detecta un paquete X.25 de reinicialización (reset) o de liberación, el protocolo desconecta la sesión e informa de ello al usuario. Los protocolos de clase 2 están pensado para las redes tipo A de alta fiabilidad. El control de flujo que ofrecen se basa en la conocida idea de ventanas.

Permiten enviar datos de usuario dentro del paquete de solicitud de conexión.

Los protocolos de clase 3 proporcionan todos los servicios de la clase 2 y además son capaces de resolver errores de la red sin necesidad de informar de ello al usuario. Los datos de usuario se retienen hasta que el nivel de transporte receptor asienta los datos. En esta clase de protocolo existe un mecanismo de retransmisión de datos muy útil. Cada paquete en tránsito por la red tiene asignado un tiempo de vida máximo gestionado mediante temporizadores. Todos los datos que exigen una respuesta están sometidos a este cronometraje. Si el plazo del temporizador expira antes de que haya llegado el asentimiento, puede ordenarse una retransmisión o invocarse otros procedimientos de recuperación. En este protocolo de clase 3 se supone que la red es de tipo B.

Los protocolos de la clase 4 se emplean cuando la red puede perder o deteriorar los datos. Incluyen varios mecanismos sofisticados de comprobación de errores, de resolución de pérdidas de secuencia y de recuperación de paquetes perdidos. Es la única clase de transporte que retransmite los datos una vez expirado el plazo del temporizador y se ocupa de reordenar los datos en el receptor. Es capaz de hacer frente a un fallo de la red, ya que conserva una copia de los datos hasta que llegue al asentimiento.

4.13 Comunicaciones entre niveles

El nivel de transporte envía una solicitud de conexión al nivel de red. Este responde enviando una solicitud de conexión al nivel de enlace el cual entrega al nivel físico una solicitud de activación. Todas las primitivas solicitan el establecimiento de un enlace para el diálogo entre los usuarios y a medida que esta solicitud atraviesa los niveles de red y de enlace, entran del estado de conexión al estado pendiente.

La señal atraviesa la red, llega al nodo receptor B, y el nivel físico activa el circuito I de X.21. El nivel físico crea una indicación de activación física, y el nivel de enlace la convierte en una respuesta de activación física. A continuación, la X.21 del nodo B activa su circuito C y envía la señal a la red. El nodo A recibe esta señal y activa su circuito I del nivel físico mediante una confirmación de la activación física.

Es posible establecer un enlace físico sin el concurso de las señales procedentes de los niveles superiores.

Lo primero que se activa es el nivel físico, después el nivel de enlace, a continuación el nivel de red y por último el nivel de transporte. La lógica de LAPB situada en el nivel de enlace inicia un proceso enviando a la red un comando SABM (establecer modo asíncrono equilibrado). El nivel físico acepta este comando y lo transporta a través del canal T del nivel físico. Los dos viajan por la red y llegan al nodo receptor B; atraviesan el nivel físico por el circuito R. El comando SABM se entrega al nivel de enlace del nodo B, el cual asiente este comando mediante un Asentimiento No Numerado (UA). Esta respuesta recorre en sentido inverso los niveles sucesivos de la red hasta ser recibida por el LAPB del nivel de enlace en el nodo A, el cual por su parte, iniciará una señal de confirmación del establecimiento de enlace.

Una vez activados los niveles de enlace entre los dos nodos, la confirmación del establecimiento de enlace enviada al nivel de paquetes permite al nivel de paquetes iniciar un paquete de petición de llamada desde la lógica X.25. La petición de llamada se envía con un número de canal lógico (LCN) de valor 75 en la cabecera del paquete. El paquete se transmite al nivel de enlace LAPB, etapa en la cual el paquete se coloca en el campo I de la trama LAPB. Los números de secuencia de envió y recepción LAPB se establecen de la siguiente forma: el

número de secuencia de envío toma valor 0 cuando se trata de la primera trama que se envía por el enlace. La trama es transportada a través de los niveles del nodo A, y recorre la red hasta llegar al nodo receptor B. A continuación, se entrega al nivel de enlace, en el cual tiene lugar una comprobación de errores.

El paquete se entrega al nivel de red, el cual lo recibe como un paquete de llamada entrante, con un 106 como número de canal lógico. El nivel de red envía al nivel de transporte una señal de indicación de conexión con la red, y responde con un paquete de aceptación de llamada generado desde X.25. Este paquete se entrega al nivel de enlace el cual lo coloca dentro de una trama de información. El nivel de enlace pone a uno el campo de secuencia de recepción para sentir la trama que le ha sido enviada desde A. La trama atraviesa los niveles físicos de la red y es recibida por el nivel de enlace del nodo A, en el cual se efectúa una comprobación de errores. La verificación indica que la transmisión ha transcurrido sin problemas. Acto seguido, el paquete se entrega al nivel de red, el cual lo recibe como un paquete de conexión de llamada según la lógica de X.25.

Ahora todos los niveles se encuentran en estado activo y preparado para aceptar datos. El paquete transmitido desde la red al nodo A contiene números de secuencia. Estos números se denotan como P(S) y P(R), para distinguirlos de los números de secuencia del nivel de enlace, denotados como N(S) y N(R). Ambos niveles tienen la capacidad de establecer secuenciamientos, ya que estos son necesarios para llevar la cuenta de los paquetes intercambiados entre dos niveles gemelos.

El paquete se entrega al LAPB del nivel de enlace. Los números de secuencia LAPB del nodo A están coordinados con los del nodo B.

La trama se envía al nodo B; LAPB comprueba si hay errores y transmite el paquete de datos al nivel de red. De modo similar, el nivel de red añade los números de secuencia adecuados y transporta los datos hacia el nivel de red del nodo B.

Los números de secuencia del nivel de red solo son significativos para el propio nivel de red, al igual que los números de secuencia del nivel de enlace solo conciernen al nivel de enlace. Puesto que se puede multiplexar varias sesiones X.25 en un mismo enlace físico, es totalmente posible que un enlace de datos pueda transportar los canales lógicos (usuarios distintos).

Lo único que hace el enlace de datos LAPB es "depositar" dentro del campo I cada paquete de la sesión lógica que le ha sido asignada, y solicitar al nodo receptor que compruebe si hay errores y envíe un asentimiento

.

4.14 Conmutación de Paquetes

En el mundo de las comunicaciones se dan diferentes topologías o diseños de las redes. Dos de las más conocidas son la configuración de conmutación con circuitos dedicados y la configuración de conmutación por paquetes con medios con acceso compartido. La conmutación de paquetes se emplea, por ejemplo, en la telefonía de voz, módems de transferencia de datos por teléfono, ISDN y las telecomunicaciones de datos transferidos vía satélite de la actualidad. En todos estos ámbitos los usuarios establecen una conexión dedicada con una computadora anfitriona en el otro extremo. Esta conexión se mantiene o reserva hasta que el usuario decide finalizar. Estas conexiones se caracterizan por una capacidad relativamente restringida de ancho de banda y ofrecen un caudal de procesamiento máximo de alrededor de 64 a 128 Kbps usando ISDN, o 28.8 Kbps o menos con un módem estándar que usa el teléfono.

La otra configuración, la conmutación por paquetes, semejante a la que se emplea en muchas redes de área local ("LAN"), XDSL, y entorno de transferencia de datos a través de cable, es muy diferente. En el universo de la conmutación por paquetes, hay un sólo "conducto" con ancho de banda amplio, compartido por muchos usuarios. Este canal proporciona capacidad de caudal de procesamiento de entrada y salida desde varias decenas de Mega bits por segundo hasta varios cientos de Mega bits por segundo, dependiendo de la red. Puesto que varios usuarios comparten un conducto o canal común, existe la necesidad de contar con un conjunto de reglas que todos los usuarios deben observar para compartir ese recurso de manera justa y eficiente(en estos sistemas, el nivel de enlace de datos está dividido en la capa MAC y en la LLC generalmente). Con un conjunto de reglas o "protocolo" bien diseñado, la red de acceso compartido es capaz de proporcionar un servicio eficiente y eficaz al usuario.

4.14.1 Ventajas de una Red de Conmutación por Paquetes

En primer lugar una red de conmutación por paquetes con acceso compartido proporciona una capacidad superior de transmisión de datos a alta velocidad. Cuando un usuario hace clic en un hipervínculo, quiere que la página se descargue de inmediato. La capacidad para transmitir esa página de manera oportuna se conoce como la capacidad de "estallido" de la red. Con una red de conmutación por paquetes con acceso compartido, el usuario tiene la capacidad de tomar un fragmento grande (por ejemplo, varios Mbps) del conducto compartido para descargar la página Web solicitada y luego liberar dicho recurso para que sea asignado a los demás usuarios. Esta capacidad de usar los recursos sólo cuando es necesario proporciona un gran beneficio de desempeño (conocido como transmisión múltiplex estadística), así como una ventaja económica inherente tanto para el proveedor del servicio como para el cliente. De este modo, una arquitectura de conmutación por paquetes proporciona no sólo una velocidad promedio mayor y

una velocidad máxima más grande, sino también permite al proveedor del servicio proporcionarlo a un costo mucho más bajo.

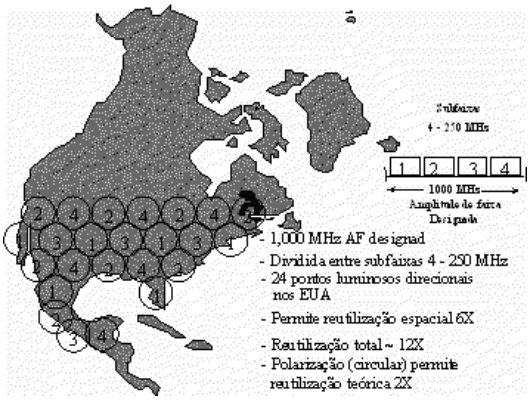
En segundo lugar, una red de conmutación por paquetes con acceso compartido otorga al abonado la capacidad de contar con una conexión activa todo el tiempo, sin la molestia de establecer una conexión por la red cada vez que necesite enviar un mensaje de correo electrónico o buscar información. Tercero, todos los usuarios de una red con acceso compartido se conectan al mismo conducto de información. Esto da al proveedor de contenidos la capacidad única de transmitir corrientes de datos (por ejemplo, enviar una corriente de datos por el conducto y hacer que cientos de usuarios la vean simultáneamente; esto se conoce como multivaciado).

4.15 Servicios Multimedia vía Satelite de Banda KA

La conmutación de paquetes no se tiene por que utilizar únicamente en la tradicional red cableada terrestre, sino que se puede extrapolar dicho concepto en el ámbito espacial, adquiriendo así, todas las ventajas comentadas anteriormente para el cable.. Aquí, también se podrá aplicar una tecnología semejante de conmutación por paquetes a través de satélites, con los mismos beneficios de desempeño para el usuario final y los mismos beneficios económicos tanto para el usuario como para el proveedor del servicio.

De manera específica, el procesamiento a bordo de la banda de frecuencias permite la conmutación y la transmisión múltiplex del tráfico de usuarios, de acuerdo con los puntos luminosos de destino, para generar portadores de enlace a tierra de alta velocidad.

Otro elemento atractivo de la banda Ka es la utilización de puntos luminosos direccionales, que proporcionan un alto nivel de reutilización de frecuencias. El diseño del sistema permite volver a utilizar la frecuencia de diez a doce veces. La reutilización de frecuencias aumenta la capacidad de comunicaciones por satélite, produciendo un costo menor por usuario.



CAPITULO 5.- FRAME RELAY

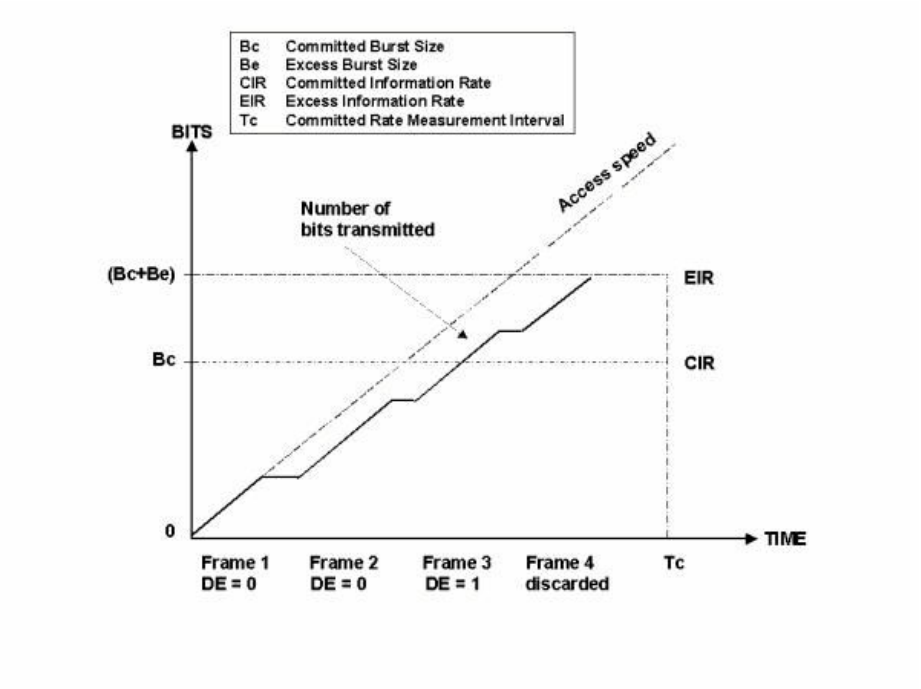
Frame Relay o (Frame-mode Bearer Service) es una técnica de comunicación mediante retranmisión de tramas, introducida por la ITU-T a partir de la recomendación I.122 de 1988. Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos("frames") para datos, perfecto para la transmisión de grandes cantidades de datos.
Ofrece mayores velocidades y rendimiento, a la vez que provee la eficiencia de ancho de banda que viene como resultado de los múltiples circuitos virtuales que comparten un puerto de una sola línea. Los servicios de Frame Relay son confiables y de alto rendimiento. Son un método económico de enviar datos, convirtiéndolo en una alternativa a las líneas dedicadas.

Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada punto a punto, esto quiere decir que es orientado a la conexión.
Las conexiones pueden ser del tipo permanente, (PVC), *Permanent Virtual Circuit*) o conmutadas (SVC, *Switched Virtual Circuit*). Por ahora solo se utiliza la permanente. De hecho, su gran ventaja es la de reemplazar las líneas privadas por un sólo enlace a la red.

El uso de conexiones implica que los nodos de la red son conmutadores, y las tramas deben llegar ordenadas al destinatario, ya que todas siguen el mismo camino a través de la red, puede manejar tanto tráfico de datos como de voz.

Al contratar un servicio Frame Relay, contratamos un ancho de banda determinado en un tiempo determinado. A este ancho de banda se le conoce como CIR (*Commited Information Rate*). Esta velocidad, surge de la división de Bc (*Committed Burst*), entre Tc (el intervalo de tiempo). No obstante, una de las características de Frame Relay es su capacidad para adaptarse a las necesidades de las aplicaciones, pudiendo usar una mayor velocidad de la contratada en momentos puntuales, adaptándose muy bien al tráfico en ráfagas, pero en media en el intervalo Tc no deberá superarse la cantidad estipulada Bc.
Estos Bc bits, serán enviados de forma transparente.

No obstante, cabe la posibilidad de transmitir por encima del CIR contratado, mediante los Be (*Excess Burst*). Estos datos que superan lo contratado, serán enviados en modo *best-effort*, activándose el bit DE de estas tramas, con lo que serán las primeras en ser descartadas en caso de congestión en algún nodo.



Como se observa en la imagen, los bits que superen la cantidad de Bc+Be en el intervalo, serán descartados directamente sin llegar a entrar en la red.

Para realizar control de congestión de la red, Frame Relay activa unos bits, que se llaman FECN (*forward explicit congestion notification*), BECN (*backward explicit congestion notification*) y DE (*Discard Eligibility*).
FECN se activa, o lo que es lo mismo, se pone en 1, cuando hay congestión en el mismo sentido que va la trama. BECN se activa cuando hay congestión en el sentido opuesto a la transmisión. DE igual a 1 indica que la trama será descartable en cuanto haya congestión. En cada nodo hay un gestor de tramas, que decide, en caso de congestión, a quien notificar, si es leve avisa a las estaciones que generan más tráfico, si es severa le avisa a todos.

Por otro lado, no lleva a cabo ningún tipo de control de errores o flujo, ya que delega ese tipo de responsabilidades en capas superiores, obteniendo como resultado una notable reducción del tráfico en la red, aumentando significativamente su rendimiento. Esta delegación de responsabilidades también conlleva otra consecuencia, y es la reducción del tamaño de su cabecera, necesitando de menor tiempo de proceso en los nodos de la red y consiguiendo de nuevo una mayor eficiencia. Esta delegación de control de errores en capas superiores es debido a que Frame Relay trabaja bajo redes digitales en las cuales la probabilidad de error es muy baja.

5.1 Aplicaciones y Beneficios

Reducción de complejidad en la red. Conexiones virtuales múltiples son capaces de compartir la misma línea de acceso.

Equipo a costo reducido. Se reduce las necesidades del “hardware” y el procesamiento simplificado ofrece un mayor rendimiento.

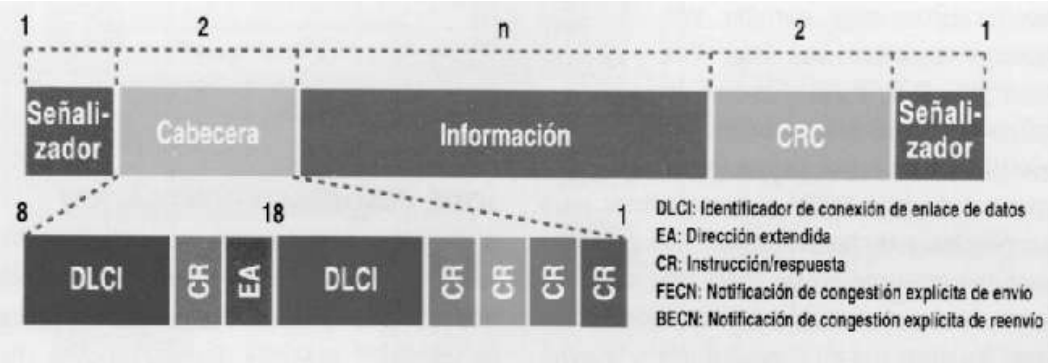
Mejoramiento del desempeño y del tiempo de respuesta. Conectividad directa entre localidades con pocos atrasos en la red. Mayor disponibilidad en la red. Las conexiones a la red pueden redirigirse automáticamente a diversos cursos cuando ocurre un error.

Mayor flexibilidad. Las conexiones son definidas por los programas. Los cambios hechos a la red son más rápidos.

Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada con circuitos punto a punto. De hecho, su gran ventaja es la de reemplazar las líneas privadas por un sólo enlace a la red. El uso de conexiones implica que los nodos de la red son conmutadores, y las tramas deben de llegar ordenadas al destinatario, ya que todas siguen el mismo camino a través de la red.

5.2 Tecnologías

Las redes Frame Relay se construyen partiendo de un equipamiento de usuario que se encarga de empaquetar todas las tramas de los protocolos existentes en una única trama Frame Relay. También incorporan los nodos que conmutan las tramas Frame Relay en función del identificador de conexión, a través de la ruta establecida para la conexión en la red.



En Frame Relay, los dispositivos del usuario se interrelacionan con la red de comunicaciones, haciendo que sean aquellos mismos los responsables del control de flujo y de errores. La red sólo se encarga de la transmisión y conmutación de los datos, así como de indicar cual es el estado de sus recursos. En el caso de errores o de saturación de los nodos de la red, los

equipos del usuario solicitarán el reenvío (al otro extremo) de las tramas incorrectas y si es preciso reducirán la velocidad de transmisión, para evitar la congestión.

Las redes Frame Relay son orientadas a conexión, como X.25, SNA e incluso ATM. El identificador de conexión es la concatenación de dos campos HDLC (High-level Data Link Control), en cuyas especificaciones originales de unidad de datos (protocolo de la capa 2), se basa Frame Relay. Entre los dos campos HDLC que forman el "identificador de conexión de enlace de datos" o DLCI (Data Link Connection Identifier) se insertan algunos bits de control (CR y EA).

A continuación se añaden otros campos que tienen funciones muy especiales en las redes Frame Relay. Ello se debe a que los nodos conmutadores Frame Relay carecen de una estructura de paquetes en la capa 3, que por lo general es empleada para implementar funciones como el control de flujo y de la congestión de la red, y que estas funciones son imprescindibles para el adecuado funcionamiento de cualquier red.

Los tres más esenciales son DE o "elegible para ser rechazada" (Discard Eligibility), FECN o "notificación de congestión explícita de envío" (Forward Explicit Congestion Notification), y BECN o "notificación de congestión explícita de reenvío" (Backward Explicit Congestion Notification). El bit DE es usado para identificar tramas que pueden ser rechazadas en la red en caso de congestión. FECN es usado con protocolos de sistema final que controlan el flujo de datos entre en emisor y el receptor, como el mecanismo "windowing" de TCP/IP; en teoría, el receptor puede ajustar su tamaño de "ventana" en respuesta a las tramas que llegan con el bit FECN activado. BECN, como es lógico, puede ser usado con protocolos que controlan el flujo de los datos extremo a extremo en el propio emisor.

Según esto, la red es capaz de detectar errores, pero no de corregirlos (en algunos casos podría llegar tan solo a eliminar tramas).

No se ha normalizado la implementación de las acciones de los nodos de la red ni del emisor/receptor, para generar y/o interpretar estos tres bits. Por ejemplo, TCP/IP no tiene ningún mecanismo que le permita ser alertado de que la red Frame Relay esta generando bits FECN ni de como actuar para responder a dicha situación. Las acciones y funcionamiento de las redes empleando estos bits son temas de altísimo interés y actividad en el "Frame Relay Forum" (equivalente en su misión y composición al "ATM Forum").

El protocolo X.25 opera en la capa 3 e inferiores del modelo OSI, y mediante la conmutación de paquetes, a través de una red de conmutadores, entre identificadores de conexión. En cada salto de la red X.25 se verifica la integridad de los paquetes y cada conmutador proporciona una función de control de flujo. La función de control de flujo impide que un conmutador X.25 no

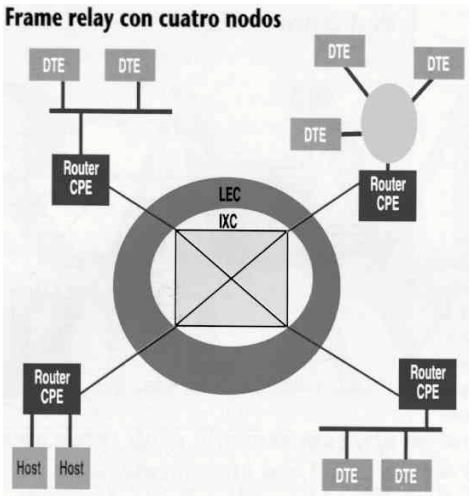
envíe paquetes a mayor velocidad de la que el receptor de los mismos sea capaz de procesarlos. Para ello, el conmutador X.25 receptor no envía inmediatamente la señal de reconocimiento de los datos remitidos, con lo que el emisor de los mismos no envía más que un determinado número de paquetes a la red en un momento dado.

Frame Relay realiza la misma función, pero partiendo de la capa 2 e inferiores. Para ello, descarta todas las funciones de la capa 3 que realizaría un conmutador de paquetes X.25, y las combina con las funciones de trama. La trama contiene así al identificador de conexión, y es transmitida a través de los nodos de la red en lugar de realizar una "conmutación de paquetes".

Lógicamente, todo el control de errores en el contenido de la trama, y el control de flujo, debe de ser realizado en los extremos de la comunicación (nodo origen y nodo destino). La conmutación de paquetes en X.25, un proceso de 10 pasos, se convierte en uno de 2 pasos, a través de la transmisión de tramas.

Un caso práctico:

Si el usuario "A" desea una comunicación con el usuario "B", primero establecerá un Circuito Virtual (VC o Virtual Circuit), que los una. La información a ser enviada se segmenta en tramas a las que se añade el DLCI. En destino, las tramas son reensambladas.



5.3 Tecnologías FRAME – RELAY

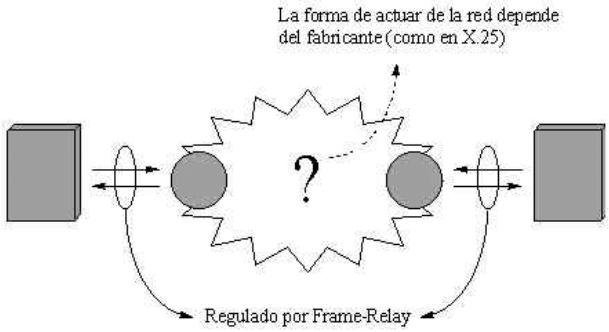
Las principales características de Frame-Relay son:

- Es un protocolo de *Acceso a Subred* (regula interfaz usuario-red)

- El funcionamiento interno no está normalizado (igual que en X.25), por lo que sólo lo está el interfaz usuario-red.

- Frame-Relay posibilita tráfico impulsivo, así como múltiples terminales de usuario.

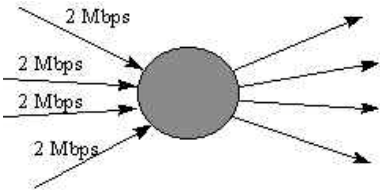
- Frame-Relay ofrece una simplificación de los servicios que ofrece. Para comprender mejor el por qué de las simplificaciones que ofrece Frame-Relay, pasemos al siguiente ejemplo:



Línea de 2 Mbps.

Paquetes de aproximadamente 131 octetos (~ 1000 bits).

El nodo asociado a esta línea debería procesar paquetes cada $\frac{1000bits}{2Mbps} = 500\mu s$ *, y el hecho de tener varias líneas accediendo a cada nodo, así como saliendo de el, encarecería demasiado los equipos:*



En Frame-Relay, para reducir este coste, se realizan las siguientes simplificaciones de protocolo:

• Separación (funcional) del Plano de Usuario y Plano de Control:

- En X.25, estos planos no estaban separados, lo que complicaba el diseño de los equipos. La separación en Frame-Relay se debe a que se tiende a diseñar en el equipo una parte distinta para procesar cada plano, ya que la característica deseada para el usuario es conseguir MAS

CAUDAL, y para el de control, tener FLEXIBILIDAD (se tiende a la implementación software de los equipos en el plano de control y hardware en el plano de usuario).

5.4 Servicio FRAME-RELAY

Orientación a conexión (CO).

- Es no fiable, con garantías de caudal mínimo, por lo que se acepta que proveedor pierda datos (PDUs). Con fiable nos referimos a que tramas errores pueden ser detectadas y descartadas en los nodos de la red (comprobando el CRC) sin avisar a los sistemas finales.
- Las perdidas de datos en Frame-Relay no son preocupantes si disponemos de un protocolo de Nivel Superior que resuelva el problema para las aplicaciones que no toleren perdidas de datos. A pesar de esto, la no fiabilidad es muy baja, ya que los medios de transmisión tienen una probabilidad de error (P_e) bajísima.
- QoS: El cliente tiene garantizadas (por contrato) las prestaciones que obtendrá de la red.

Frame-Relay ofrece dos tipos de conexiones:

  - Circuitos Virtuales Permanentes(PVC): están definidos en todos los estándares.
  - Circuitos Virtuales Conmutados (CVC): Éstos solo han sido definidos en el estandar propuesto por la ITU-T y no por el estandar de facto.

5.5 Arquitectura de Protocolos

En cada sistema final y sistema intermedio, tenemos dos arquitecturas distintas y separadas: la correspondiente al plano de usuario y la correspondiente al plano de control.

- Plano de Usuario:

(a) Nivel Físico (dos opciones):

  - Línea de Serie (interfaces físicas: V.35, G.703)
  - RDSI (BRI, PRI)

(b) Nivel de Enlace: en la recomendación de ITU-T, el protocolo utilizado es LAP-F.

- Plano de Control (en la práctica no se utilizan):

- Se instala sobre el mismo plano de usuario, utilizando el mismo nivel físico, excepto en RDSI, que se utiliza el Canal D para el plano de Control.
- Nivel 2: el mismo que RDSI, es decir, LAP-D.
- Nivel 3: Se usa el protocolo Q.933 (similar al Q.931 usado en establecimiento y liberación de llamadas en RDSI).

NOTA: a nivel físico, existirá una separación de los flujos de información de usuario y de control.

- Plano de Gestión: Se identifican dos protocolos: ILMI (Interin Local Management Interface) y CLLM (Consolidated Link Layer Management).

5.6 Formato de Trama

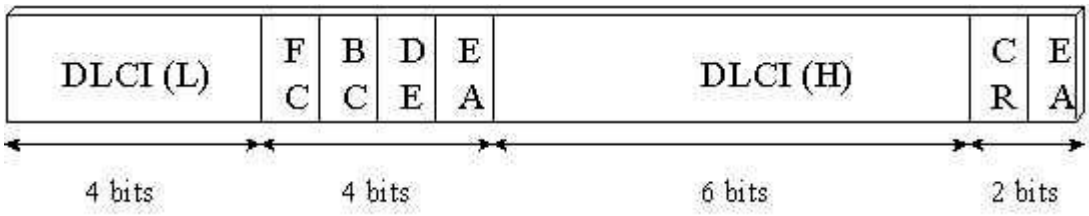
En este formato no se establece una longitud máxima de trama, pero debe ser un múltiplo entero de octetos, lo cual se puede observar en la figura. Conviene destacar que el protocolo define también el orden de transmisión de los bits de la trama por línea. Este orden es, según se ha querido dar a entender con la figura, de derecha a izquierda. La transmisión es en serie por la línea y un bit va detrás de otro. Un sistema final o intermedio que reciba una trama debe saber el significado de cada bit que le llega, y este significado depende del orden de ese bit dentro de su trama.

- CRC (también llamado FCS): Código de detección de errores. Es un código *cíclico*. Es necesario, ya que cuando se detecta una trama con error, se descarta.
- DATOS: En este campo es donde van los datos del Nivel superior, es decir, esta información se mete en la trama y, en recepción, se pasa directamente al nivel superior. Su longitud máxima no está definida en el estándar de facto (no está normalizada), pues no se pudo llegar a un acuerdo. Normalmente los operadores de redes FR la sitúan alrededor de 1600 bytes. Esta gran diferencia con X.25 (128 octetos) es debida a la escasa P_e. El Nivel superior entrega los datos, y estos son encapsulados en una trama. Por último, añadir que

este campo está alineado a octeto, es decir se exige al usuario del servicio que entregue un número entero de octetos.

- FLAG: Tiene el mismo formato que en LAB-B (01111110), y también se utiliza para separar tramas consecutivas. Cuando no hay tramas que transmitir, se generan guiones continuamente.

- CAMPO DE CONTROL: Llamamos campo de control a los bytes que siguen al Flag y que están por delante de los Datos de usuario. Puede tener varios formatos (como en X.25), pero normalmente suele tener 16 bits de longitud (2 octetos):



  - DLCI: Data Link Circuit Identifier. Estos diez bits son el identificador de conexión de enlace de datos. Permite definir hasta 1024 circuitos virtuales. Ya habíamos avanzado que la función de multiplexión se realiza en el nivel 2, y con el DLCI se identifica al canal lógico al que pertenece cada trama. Los números de canal lógico se asignan por contratación. Equivale al NCL de X.25.

  - E A: Extended Address. Campo de extensión de dirección. Puesto que se permiten más de dos octetos en el campo de control, este primer bit de cada octeto indica (cuando está marcado con un '0') si detrás siguen más octetos o bien (cuando está marcado con un '1') si se trata del último del campo de control. Emplear más de dos bytes resulta bastante infrecuente y se utiliza en el caso de que la dirección de multiplexión (en el campo DLCI) supere los 10 bits.

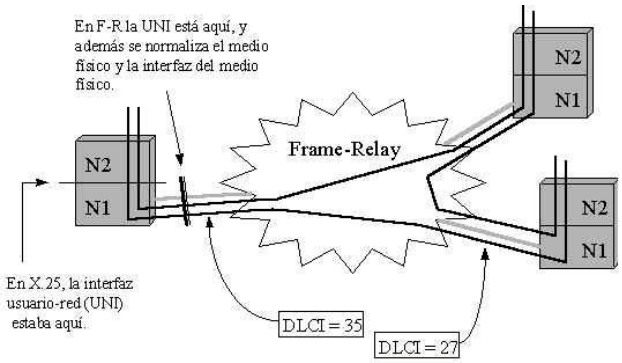
  - C R: Bit de Comando / Respuesta. Es parecido al bit "Q" de X.25, y al igual que ocurría con éste, no es un bit utilizado por la red. Se introduce por compatibilidad con protocolos anteriores, como los del tipo HDLC. Cuando el protocolo de enlace es fiable, utilizan este bit.

  - F C, B C y F C: Bits para control de congestión y se verán más adelante en este tema.

Los sistemas pueden almacenar las tramas de formas diferentes. No olvidemos que la representación interna de la información dentro de un sistema puede tener diferentes significados, según el convenio que haya adoptado la implementación de esa máquina. Existen

los convenios extremista mayor y extremista menor (Big-Endian y Little- Endian en inglés), y éstos, a su vez pueden estar referidos a bits, bytes o palabras. El sistema debe tener esto en cuenta para operar adecuadamente con los bits que tiene almacenados, y al transmitir o recibir bits de tramas, hacerlo en el orden que establece el protocolo.

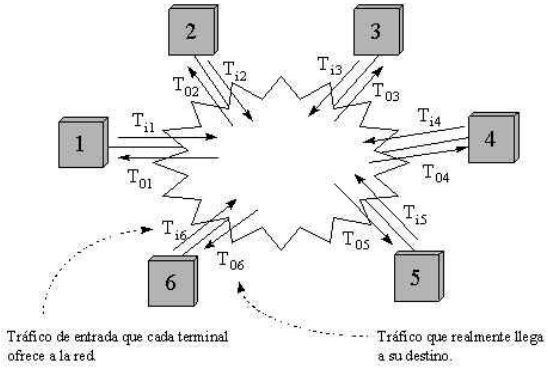
(NOTA: La velocidad de llegada de tramas al nodo depende de la longitud de las tramas y del caudal. El nodo a de ser capaz de procesar las tramas según llegan. Luego, el que se queden en el nodo y tarden en salir es otra cosa, y depende del tráfico).



Vemos como, a diferencia de X.25, en Frame-Relay tendremos DLCIs diferentes en el UNI para datos entrantes y salientes de la red. Además, cada circuito se trata de un **CVP**, y no de un **CVC**.

5.7 Control de Congestión

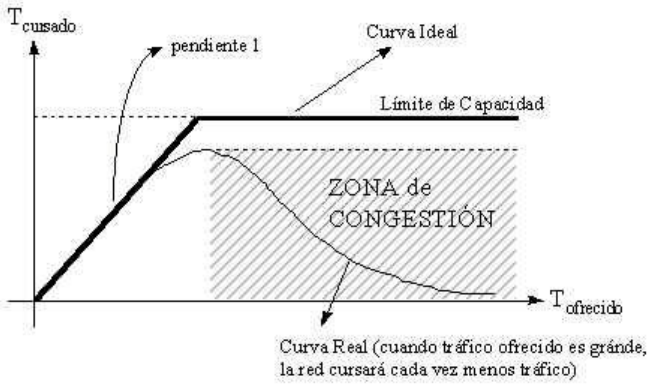
El control de congestión no es una función local, sino global (participan todos los sistemas). Veamos algunos conceptos:



Tráfico ofrecido: $\sum_j T_{ij}$

Tráfico cursado: $\sum_j T_{0j}$

Por la gráfica siguiente, queda claro que el objetivo de la tecnología de redes será evitar entrar en la zona de congestión.



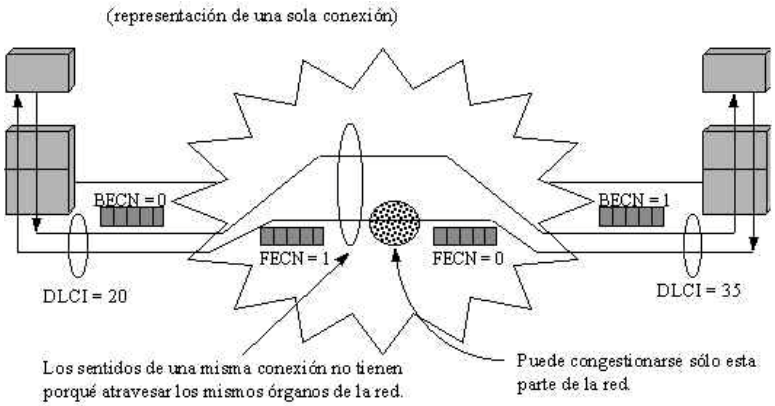
- En redes de *medio compartido*, la red pierde tiempo en solucionar las colisiones.
- En redes *sin medio compartido*, esta gráfica se debe a la limitación de la capacidad de conmutación de los nodos. Cuando a un nodo le llegan datos que no puede cursar, los descarta, quedándose sin llegar a su destino (*curva cae*)

"Cuando se detecta una zona congestionada, se notifica al usuario que envía los datos que pasan por esa parte de la red, el cual disminuye la tasa de tráfico inyectado. Si el usuario no lo hace, la red descartará los datos que considere oportuno (aceptable, ya que F-R es un servicio no fiable). Esta pérdida, si es de porcentaje elevado, provoca el cese del funcionamiento a las entidades de nivel superior, por lo que el usuario intentará evitar este tipo de situaciones".

La implementación de la técnica de NOTIFICACIÓN Y DESCARTE se realiza mediante los campos FECN, BECN y DE en el campo de control de la trama que ya fueron introducidos anteriormente:

- FECN (*Forward Explicit Congestion Notification*): Notificación de congestión en el sentido de la transmisión.
- BECN (*Backward Explicit Congestion Notification*): Notificación de congestión en el sentido contrario a la transmisión.
- DE (*Discard Eligibility*): Las tramas que tienen este bit a "1" son susceptibles de descarte en situaciones de congestión.

El bit BECN y el FECN se usan para avisar que hay congestión (la red los cambia de 0 a 1 y viceversa):



Hay que señalar que la congestión es unidireccional, pues puede haber caminos distintos para los dos sentidos de la transmisión y mientras uno puede estar sufriendo problemas de tráfico (congestión), el otro puede no tenerlos. Los bits FECN y BECN notifican congestión a los dos extremos de una conexión de la siguiente forma: A una trama que atraviesa una zona congestionada se le pone su bit FECN a '1'. La red identifica las tramas de esa conexión que circulan en sentido contrario y en ellas marca el bit BECN también a '1'.

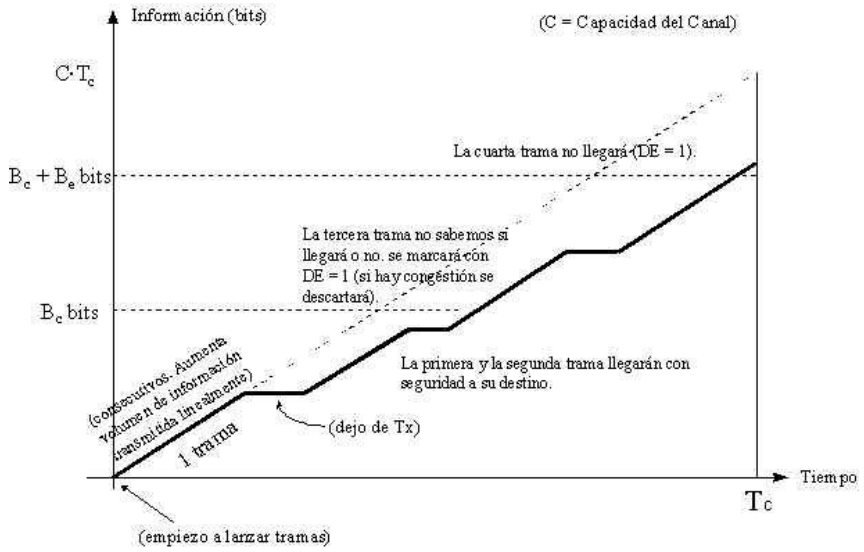
Es decir, la red F-R sólo notifica la congestión al origen y al destino, y del N. Superior dependerá seguir estas indicaciones (indicando al N. Superior del origen que reduzca la tasa, etc.) o no hacerlo, en cuyo caso, F-R procederá a descartar tramas.

QoS

Es posible contratar para cada conexión una calidad de servicio distinta. Dicha calidad está definida mediante ciertos parámetros:

- CIR (*Committed Information Rate*) (bits/s): Es la tasa de información comprometida, es decir, el caudal medio garantizado que la red se compremete a dar en una conexión durante un intervalo de tiempo definido (Tc). Es un parámetro asociado a cada sentido de la transmisión de cada circuito virtual.

Se define una relación entre el tiempo real y el volumen de información transferida:



- T_c (*Commited rate measurement interval*): Intervalo de observación *(es el tiempo hasta el cual ha sido representado la gráfica anterior)*. Parámetro del algoritmo para calcular el CIR).

- $C \cdot T_c$: Máximo volumen de información que se podría cursar en T_c (es lo que posibilita el canal).

El caudal físico (C) de la línea de acceso también se contrata. Así el operador dimensiona la red en función de los parámetros contratados por sus abonados.

En el interfaz usuario-red se controla, para cada circuito virtual, que los usuarios se ajusten a los parámetros Bc, y Be que han negociado. Si la red está bien diseñada no debe perder datos que no superen el tráfico comprometido.

Definimos dos zonas en el diagrama:

- B_c (*Committed burst size*): Es el volumen de información comprometida: durante el intervalo T_c la compañía se compromete a transmitir un volumen B_c.

- B_e : Volumen de información en exceso: la información cursada durante el intervalo T_c que exceda de $B_c + B_e$ no se sabe si llegará o no a su destino (la compañía no lo garantiza). El volumen de información que exceda de $B_c + B_e$ seguro que no llegará.

Existe un bit en la trama (bit DE) que es activado por la red en tramas que superen Bc (es decir aquellas que pertenezcan a Be) para indicar que esas tramas deberían ser descartadas en preferencia a otras, si es necesario. El servicio permite que el propio usuario también pueda marcar este bit para indicar la importancia relativa de una trama respecto a otras (en este caso,

estas tramas no se contabilizan como pertenecientes a la zona bajo B_c, sino como perteneciente a la zona sobre B_c y bajo $B_c + B_e$, no contando para el CIR).

Si el T_c se toma grande, existe la posibilidad de transmitir grandes picos de información en algunos momentos y nada de información en otros. Por tanto, un T_c pequeño nos garantiza el que la transmisión sea más homogénea.

5.8 Plano de Control y Señalización

- Protocolos ILMI y CLLM
- CLLM - Trama XID (*eXchange IDentification*) sobre Canal D (ISDN)

XID se utiliza en F-R para llevar la información de CLLM. Si no se utiliza F-R sobre RDSI se utiliza un DLCI determinado.

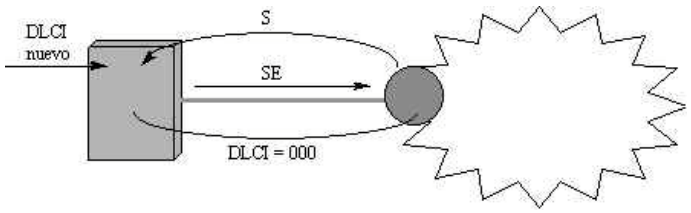
Independientemente de cual sea la longitud de DLCI, CLLM utiliza el DLCI que tenga el campo todo a 1.

El protocolo CLLM se utiliza para enviar información de control de congestión, en aquellos casos en que no hay tramas en sentido contrario al congestionado .

El ILMI se puede enviar de dos maneras dependiendo de como esté integrado:

- Trama UI (*Unnumbered Information*) sobre Canal D (RDSI)
- DLCI = 0?0 (forma más habitual, pues casi no se usa F-R sobre RDSI)

Se encarga de comprobar el estado del acceso físico. F-R no tiene temporizador, por lo que supervisa el estado del acceso físico para, mediante protocolo de señalización, informar de que se ha dañado o hay errores. También se encarga de comprobar el estado de cada DLCI (dado de alta o baja).



CAPITULO 6 .- MODO DE TRANSFERENCIA ASINCRONA ATM

6.1 Introducción

La tecnología llamada *Asynchronous Transfer Mode* (ATM) Modo de Transferencia Asíncrona es el corazón de los servicios digitales integrados que ofrecerán las nuevas redes digitales de servicios integrados de Banda Ancha (B-ISDN).

La primera referencia del ATM (Asynchronous Transfer Mode) tiene lugar en los años 60 cuando un norteamericano de origen oriental perteneciente a los laboratorios Bell describió y patentó un modo de transferencia no síncrono. Sin embargo el ATM no se hizo popular hasta 1988 cuando el CCITT decidió que sería la tecnología de conmutación de las futuras red ISDN en banda ancha.

6.2 Arquitectura de un Nodo ATM

El ATM puede ser considerado como una tecnología de conmutación de paquetes en alta velocidad con unas características particulares:

Los paquetes son de pequeño y constante tamaño (53 Bytes).

Es una tecnología de naturaleza conmutada y orientada a la conexión.

Los nodos que componen la red no tiene mecanismos para el control de errores de control de flujo.

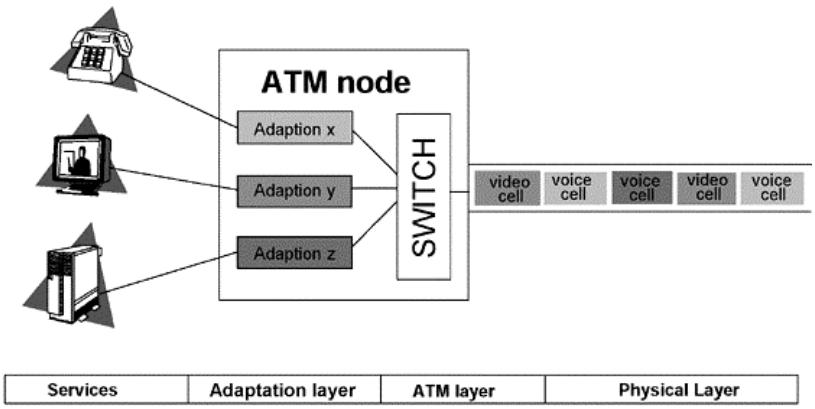
Simplificando al máximo podemos ver que una red ATM esta compuesta por nodos de comunicación, elementos de transmisión y equipos terminales de usuarios. Los nodos son capaces de encaminar la información empaquetada en células a través de unos caminos conocidos como conexiones de Canal Virtual. El routing en los nodos conmutadores de células, es un proceso de hardware mientras que el establecimiento de conexiones y el empaquetamiento / desempaquetamiento de las células son procesos de software.

La capa de Adaptación de ATM adapta y segmenta el flujo de tráfico en celdas de 48 bytes. La capa ATM añade los 5 bytes de cabecera, y los pasa a la capa física, que convierte las celdas en señales eléctricas u ópticas.

6.3 Multiplexación en ATM:

Un examen más cercano del protocolo ATM y cómo opera ayudará a explicar cómo los circuitos virtuales, las rutas virtuales, los conmutadores y los servicios que ellos acarrean se afectan entre sí.

La figura muestra un formato básico y la jerarquía de ATM. Una conexión ATM, consiste de "celdas" de información contenidos en un circuito virtual (VC). Estas celdas provienen de diferentes fuentes representadas como generadores de bits a tasas de transferencia constantes como la voz y a tasas variables tipo ráfagas (bursty traffic) como los datos.



Cada celda compuesta por 53 bytes, de los cuales 48 (opcionalmente 44) son para trasiego de información y los restantes para uso de campos de control (cabecera) con información de "quién soy" y "donde voy"; es identificada por un "virtual circuit identifier" VCI y un "virtual path identifier" VPI dentro de esos campos de control, que incluyen tanto el enrutamiento de celdas como el tipo de conexión. La organización de la cabecera (header) variará levemente dependiendo de sí la información relacionada es para interfaces de red a red o de usuario a red. Las celdas son enrutadas individualmente a través de los conmutadores basados en estos identificadores, los cuales tienen significado local - ya que pueden ser cambiados de interfase a interfase.

La técnica ATM multiplexa muchas celdas de circuitos virtuales en una ruta (path) virtual colocándolas en particiones (slots), similar a la técnica TDM. Sin embargo, ATM llena cada slot con celdas de un circuito virtual a la primera oportunidad, similar a la operación de una red conmutada de paquetes. La figura No.2 describe los procesos de conmutación implícitos los VC switches y los VP switches.

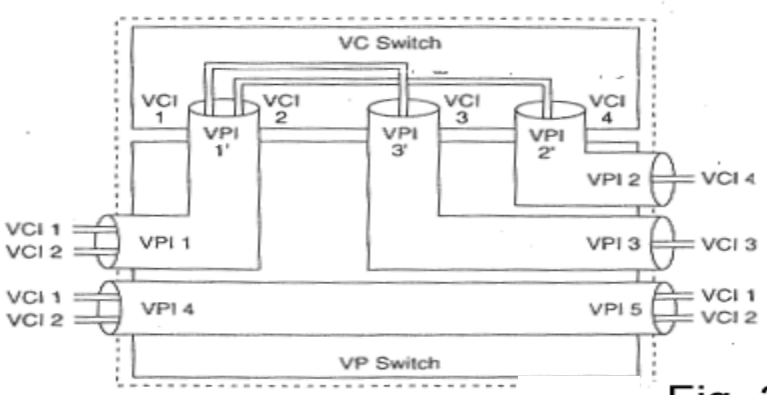


Fig. 2

Los slots de celda no usados son llenados con celdas "idle", identificadas por un patrón específico en la cabecera de la celda. Este sistema no es igual al llamado "bit stuffing"en la multiplexación Asíncrona, ya que aplica a celdas enteras.

Diferentes categorías de tráfico son convertidas en celdas ATM vía la capa de adaptación de ATM (AAL - ATM Adaptation Layer), de acuerdo con el protocolo usado.

La tecnología ATM ha sido definida tanto por el ANSI como por el CCITT a través de sus respectivos comités ANSI T1, UIT SG XVIII, como la tecnología de transporte para la B-ISDN (Broad Band Integrated Services Digital Network), la RDSI de banda ancha. En este contexto "transporte" se refiere al uso de técnicas de conmutación y multiplexación en la capa de enlace (Capa 2 del modelo OSI) para el trasiego del tráfico del usuario final de la fuente al destino, dentro de una red. El ATM Forum, grupo de fabricantes y usuarios dedicado al análisis y avances de ATM, ha aprobado cuatro velocidades UNI (User Network Interfases) para ATM: DS3 (44.736 Mbit/s), SONET STS3c (155.52 Mbit/s) y 100 Mbit/s para UNI privados y 155 Mbit/s para UNI privadas. UNI privadas se refieren a la interconexión de usuarios ATM con un switch ATM privado que es manejado como parte de la misma red corporativa. Aunque la tasa de datos original para ATM fue de 45 Mbit/s especificado para redes de operadores (carriers) con redes T3 existentes, velocidades UNI adicionales se han venido evaluando y están ofreciéndose. También hay un alto interés en interfases, para velocidades EI (2Mbps) y T1 (1,544 Mbps) para accesos ATM de baja velocidad.

6.4 Protocolos ATM:

El protocolo ATM consiste de tres niveles o capas básicas. La primera capa llamada capa física (Physical Layer), define los interfases físicos con los medios de transmisión y el protocolo de trama para la red ATM es responsable de la correcta transmisión y recepción de los bits en el medio físico apropiado. A diferencia de muchas tecnologías LAN como Ethernet, que especifica ciertos medios de transmisión, (10 base T, 10 base 5, etc.) ATM es independiente

del transporte físico. Las celdas ATM pueden ser transportadas en redes SONET (Synchronous Optical Network), SDH (Synchronous Digital Hierarchy), T3/E3, TI/EI o aún en modems de 9600 bps. Hay dos subcapas en la capa física que separan el medio físico de transmisión y la extracción de los datos:

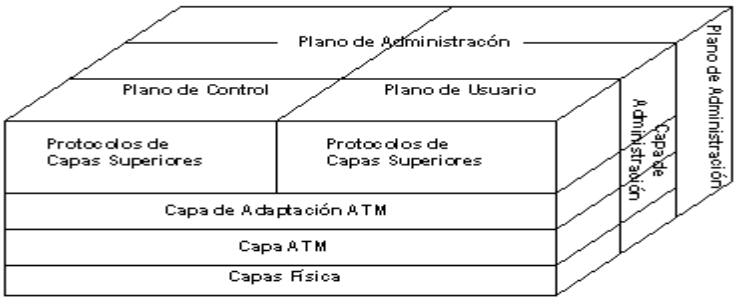


Fig. 3 Protocolo de Modelo de Referencia para ATM Banda Ancha

La subcapa PMD (Physical Medium Depedent) tiene que ver con los detalles que se especifican para velocidades de transmisión, tipos de conectores físicos, extracción de reloj, etc., Por ejemplo, la tasa de datos SONET que se usa, es parte del PMD. La subcapa TC (Transmission Convergence) tiene que ver con la extracción de información contenida desde la misma capa física. Esto incluye la generación y el chequeo del Header Error Corrección (HEC), extrayendo celdas desde el flujo de bits de entrada y el procesamiento de celdas "idles" y el reconocimiento del límite de la celda. Otra función importante es intercambiar información de operación y mantenimiento (OAM) con el plano de.Administración.

La segunda capa es la capa ATM. Ello define la estructura de la celda y cómo las celdas fluyen sobre las conexiones lógicas en una red ATM, esta capa es independiente del servicio. El formato de una celda ATM es muy simple. Consiste de 5 bytes de cabecera y 48 bytes para información.

Las celdas son transmitidas serialmente y se propagan en estricta secuencia numérica a través de la red. El tamaño de la celda ha sido escogido como un compromiso entre una larga celda, que es muy eficiente para transmitir largas tramas de datos y longitudes de celdas cortas que minimizan el retardo de procesamiento de extremo a extremo, que son buenas para voz, vídeo y protocolos sensibles al retardo. A pesar de que no se diseñó específicamente para eso, la longitud de la celda ATM acomoda convenientemente dos Fast Packets IPX de 24 bytes cada uno.

Los comités de estándares han definido dos tipos de cabeceras ATM: los User-to-Network interfase (UNI) y la Network to Network interfase (UNI). La UNI es un modo nativo de interfaz ATM que define la interfaz entre el equipo del cliente (Customer Premises Equipment), tal

como hubs o routerss ATM y la red de área ancha ATM (ATM WAN). La NNI define la interfase entre los nodos de la redes (los switches o conmutadores) o entre redes. La NNI puede usarse como una interfase entre una red ATM de un usuario privado y la red ATM de un proveedor público (carrier). Específicamente, la función principal de ambos tipos de cabeceras de UNI y la NNI, es identificar las "Virtual paths identifiers" (VPIS) y los "virtual circuits" o virtual channels"(VCIS) como identificadores para el ruteo y la conmutación de las celdas ATM.

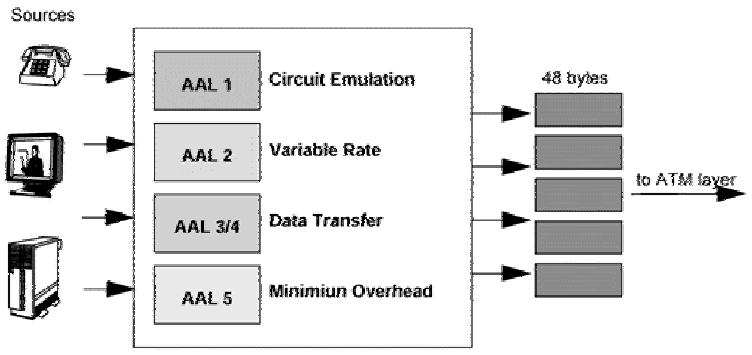
6.5 La Capa de Adaptación de ATM:

La tercer capa es la ATM Adaptation Layer (AAL). La AAL juega un rol clave en el manejo de múltiples tipos de tráfico para usar la red ATM, y es dependiente del servicio. Específicamente, su trabajo es adaptar los servicios dados por la capa ATM a aquellos servicios que son requeridos por las capas más altas, tales como emulación de circuitos, vídeo, audio, frame relay, etc. La AAL recibe los datos de varias fuentes o aplicaciones y las convierte en los segmentos de 48 bytes. Cinco tipos de servico AAL están definidos actualmente:

La capa de Adaptación de ATM yace entre el ATM layer y las capas más altas que usan el servicio ATM. Su propósito principal es resolver cualquier disparidad entre un servicio requerido por el usuario y atender los servicios disponibles del ATM layer. La información transportada por la capa de adaptación se divide en cuatro clases según las propiedades siguientes:

1. Que la información que esta siendo transportada dependa o no del tiempo.
2. Tasa de bit constante/variable.
3. Modo de conexión.

Estas propiedades definen ocho clases posibles, cuatro se definen como B-ISDN Clases de servicios. La capa de adaptación de ATM define 4 servicios para equiparar las 4 clases definidas por B-ISDN:



- AAL-1
- AAL-2
- AAL-3
- AAL-4

La capa de adaptación se divide en dos subcapas:

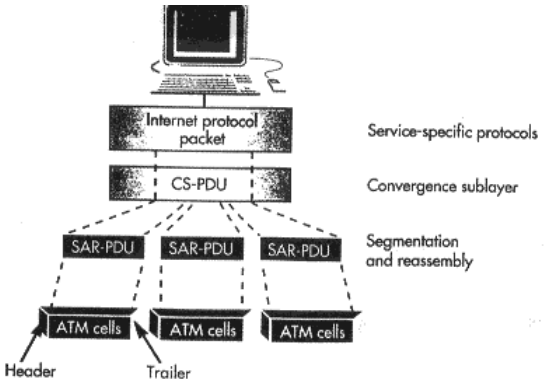
1) Capa de convergencia (convergence sublayer (CS)):

En esta capa se calculan los valores que deben llevar la cabecera y los payloads del mensaje. La información en la cabecera y en el payload depende de la clase de información que va a ser transportada.

2) Capa de Segmentación y reensamblaje (segmentation and reassembly (SAR))

Esta capa recibe los datos de la capa de convergencia y los divide en trozos formando los paquetes de ATM. Agrega la cabecera que llevara la información necesaria para el reensamblaje en el destino.

La figura siguiente aporta una mejor comprensión de ellas. La subcapa CS es dependiente del servicio y se encarga de recibir y paquetizar los datos provenientes de varias aplicaciones en tramas o paquete de datos longitud variable.



Estos paquetes son conocidos como (CS - PDU) CONVERGENCE SUBLAYER PROTOCOL DATA UNITS.

Luego, la sub capa recibe los SAR CS - PDU, los reparte en porciones del tamaño de la celda ATM para su transmisión. También realiza la función inversa (reensamblado) para las unidades

de información de orden superior. Cada porción es ubicada en su propia unidad de protocolo de segmentación y reemsable conocida como (SAR - PDU) SEGMENTATION AND REASSEMBLER PROTOCOL DATA UNIT, de 48 bytes.

Finalmente cada SAR - PDU se ubica en el caudal de celdas ATM con su header y trailer respectivos.

AAL1:

AAL-1 se usa para transferir tasas de bits constantes que dependen del tiempo. Debe enviar por lo tanto información que regule el tiempo con los datos. AAL-1 provee recuperación de errores e indica la información con errores que no podrá ser recuperada.

Capa de convergencia:

Las funciones provistas a esta capa difieren dependiendo del servicio que se proveyó. Provee la corrección de errores.

Capa de segmentación y reensamblaje:

En esta capa los datos son segmentados y se les añade una cabecera. La cabecera contiene 3 campos (ver diagrama)

- Número de secuencia usado para detectar una inserción o pérdida de un paquete.
- Número de secuencia para la protección usado para corregir errores que ocurren en el número de secuencia.
- Indicador de capa de convergencia usado para indicar la presencia de la función de la capa de convergencia.

ALL 2:

AAL-2 se usa para transferir datos con tasa de bits variable que dependen del tiempo. Envía la información del tiempo conjuntamente con los datos para que esta pueda recuperarse en el destino. AAL-2 provee recuperación de errores e indica la información que no puede recuperarse.

Capa de convergencia:

Esta capa provee para la corrección de errores y transporta la información del tiempo desde el origen al destino.

Capa de segmentación y recuperación:

El mensaje es segmentado y se le añade una cabecera a cada paquete. La cabecera contiene dos campos.

- Numero de secuencia que se usa para detectar paquetes introducidas o perdidas.
- El tipo de información es:
    - BOM, comenzando de mensaje
    - COM, continuación de mensaje
    - EOM, fin de mensaje o indica que el paquete contiene información de tiempo u otra.

El payload también contiene dos campos:

- Indicador de longitud que indica el número de bytes validos en un paquete parcialmente lleno.
- CRC que es para hacer el control de errores.

AAL 3:

AAL-3 se diseña para transferir los datos con tasa de bits variable que son independientes del tiempo. AAL-3 puede ser dividido en dos modos de operación:

1. Fiable: En caso de perdida o mala recepción de datos estos vuelven a ser enviados. El control de flujo es soportado.
2. No fiable: La recuperación del error es dejado para capas mas altas y el control de flujo es opcional.

Capa de convergencia:

La capa de convergencia en AAL 3 es parecida al ALL 2. Esta subdividida en dos secciones:

1. Parte común de la capa de convergencia. Esto es provisto también por el AAL-2 CS. Añade una cabecera y un payload a la parte común.

La cabecera contiene 3 campos:

Indicador de la parte común que dice que el payload forma parte de la parte común.

Etiqueta de comienzo que indica el comienzo de la parte común de la capa de convergencia.

Tamaño del buffer que dice al receptor el espacio necesario para acomodar el mensaje.

El payload también contiene 3 campos:

Alineación es un byte de relleno usado para hacer que la cabecera y el payload tengan la misma longitud.

Fin de etiqueta que indica el fin de la parte común de la CS(capa de convergencia).

El campo de longitud tiene la longitud de la parte común de la CS.

2. Parte especifica del servicio. Las funciones proveídas en esta que capa dependen de los servicios pedidos. Generalmente se incluyen funciones para la recuperación y detección de errores y puede incluir también funciones especiales.

Capa de segmentación y reensamblaje

En esta capa los datos son partidos en paquetes de ATM. Una cabecera y el payload que contiene la información necesaria para la recuperación de errores y reensamblaje se añaden al paquete. La cabecera contiene 3 campos:

1) Tipo de segmento que indica que parte de un mensaje contiene en payload. Tiene uno de los siguientes valores:

BOM: Comenzando de mensaje

COM: Continuación de mensaje

EOM: Fin de mensaje

SSM: Mensaje único en el segmento

2) Numero de secuencia usado para detectar una inserción o una perdida de un paquete.

3) Identificador de multiplexación. Este campo se usa para distinguir datos de diferentes comunicaciones que ha sido multiplexadas en una única conexión de ATM.

El payload contiene dos de campos:

1) Indicado de longitud que indica el número de bytes útiles en un paquete parcialmente lleno.

2) CRC es para el control de errores.

ALL 4:

AAL-4 se diseña para transportar datos con tasa de bits variable independientes del tiempo. Es similar al AAL3 y también puede operar en transmisión fiable y o fiable. AAL-4 provee la capacidad de transferir datos fuera de una conexión explícita.

AAL 2, AAL 3/4 y AAL 5 manejan varios tipos de servicios de datos sobre la base de tasas de bits variables tales como Switched Multimegabit Data Service (SMDS), Frame Relay o tráfico de redes de área local (LAN). AAL 2 y AAL 3 soportan paquetes orientados a conexión. (Ver figura No.5)

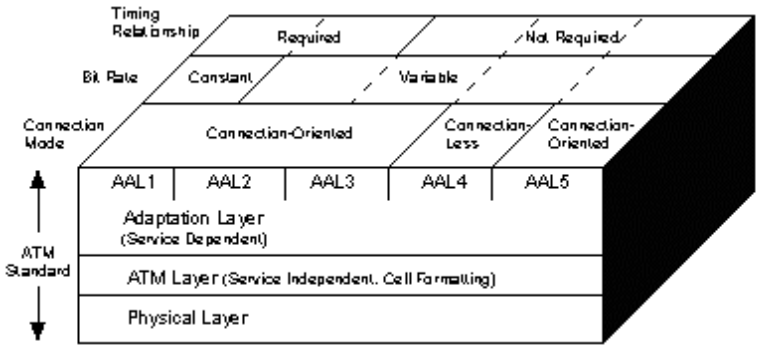


Fig 5 ATM and the AAL

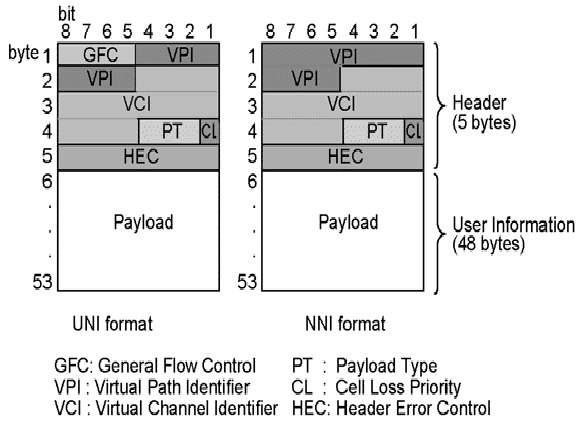
(El término orientado a conexión describe la transferencia de datos después del establecimiento de un circuito virtual).

6.6 Formato de las Celulas ATM

Son estructuras de datos de 53 bytes compuestas por dos campos principales.

1.- Header, sus 5 bytes tienen tres funciones principales: identificación del canal, información para la detección de errores y si la célula es o no utilizada.

2.- Payload, tiene 48 bytes fundamentalmente con datos del usuario y protocolos AAL que también son considerados como datos del usuario.



6.7 El Nivel Fisico

El nivel físico realiza dos funciones fundamentales: el transporte de células validas y la entrega de la información de sincronismo.

6.7.1 Estructura del Nivel Fisico

Se divide en dos capas:

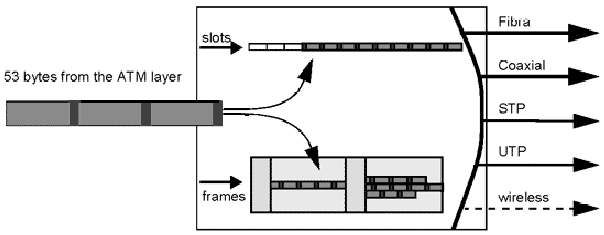
1. El subnivel Convergencia de la transmisión (TC).

Encargado de adaptar la velocidad y de crear el datastream para su posterior transmisión al medio físico. El proceso inverso se realiza en el otro extremo de la red donde el TC destino debe extraer las células del satastream recibido, comprobar su corrección y entregarlas finalmente al Nivel superior ATM. Las células interconectadas o vacías se desechan.

2. El subnivel Medio físico (PM)

Es el encargado de la transmisión de bits y de la sincronización de señales.

Dos velocidades estandarizadas por el ITU son 155,52 Mbits/s y 622,08 Mbits/s; mientras que el ATM Forum ha estandarizado interfases con velocidades a 25 Mbits/s, 44,736 Mbits/s, 100 Mbits/s y 155,52 Mbits/s.



El Nivel físico debe adaptar la secuencia de celdas a la estructura y a la velocidad del canal de transmisión utilizado.

6.8 Datastream del Medio de Transmisión

El servicio portador de la red encargado de transportar la información hasta los usuarios puede ser de dos modelos:

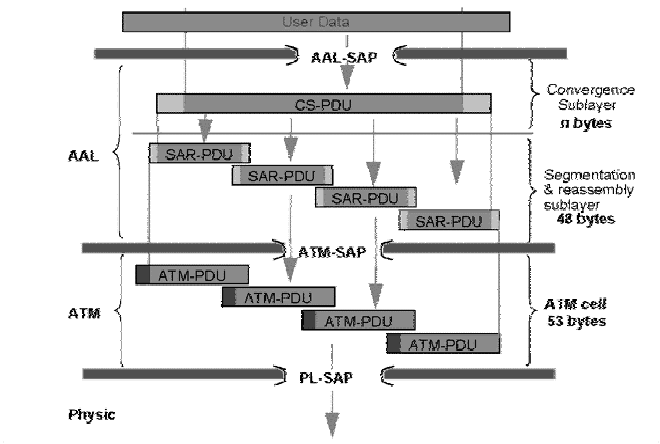
Basado en células.

Es la forma nativa utilizado en redes locales. Consiste en la transmisión directa de la secuencia de células ATM sobre el medio de transmisión que puede ser fibra y cable de diversas

categorías. Dependiendo del estándar utilizado deben ser insertadas señales de delineación, sincronismo de las células.

Basado en tramas plesiócronas o PDH.

Las células se agrupan en una forma plesiócrana que incluye funciones de mantenimiento. El estándar utilizado se deriva del IEEE 802.6 utilizado en redes metropolitanas.



Estructura e interacción de las PDUs (Protocol Data Units).

CAPITULO 7.- TCP/IP

7.1 Historia

El Protocolo de Internet (IP) y el Protocolo de Transmisión (TCP), fueron desarrollados inicialmente en 1973 por el informático estadounidense Vinton Cerf como parte de un proyecto dirigido por el ingeniero norteamericano Robert Kahn y patrocinado por la Agencia de Programas Avanzados de Investigación (ARPA, siglas en inglés) del Departamento Estadounidense de Defensa. Internet comenzó siendo una red informática de ARPA (llamada ARPAnet) que conectaba redes de ordenadores de varias universidades y laboratorios en investigación en Estados Unidos. World Wibe Web se desarrolló en 1989 por el informático británico Timothy Berners-Lee para el Consejo Europeo de Investigación Nuclear (CERN, siglas en francés).

7.2 Introducción

Internet no es un nuevo tipo de red física, sino un conjunto de tecnologías que permiten interconectar redes muy distintas entre sí. Internet no es dependiente de la máquina ni del sistema operativo utilizado. De esta manera, podemos transmitir información entre un servidor Unix y un ordenador que utilice Windows . O entre plataformas completamente distintas como Macintosh, Alpha o Intel. Es más: entre una máquina y otra generalmente existirán redes distintas: redes Ethernet, redes Token Ring e incluso enlaces vía satélite.

El protocolo TCP/IP tiene que estar a un nivel superior del tipo de red empleado y funcionar de forma transparente en cualquier tipo de red. Y a un nivel inferior de los programas de aplicación (páginas WEB, correo electrónico…) particulares de cada sistema operativo. Todo esto nos sugiere el siguiente modelo de referencia:

Capa de aplicación (HTTP, SMTP, FTP, TELNET...)
Capa de transporte (UDP, TCP)
Capa de red (IP)
Capa de acceso a la red (Ethernet, Token Ring...)
Capa física (cable coaxial, par trenzado...)

El nivel más bajo es la capa física. Aquí nos referimos al medio físico por el cual se transmite la información. Generalmente será un cable aunque no se descarta cualquier otro medio de transmisión como ondas o enlaces vía satélite.

La capa de acceso a la red determina la manera en que las estaciones (ordenadores) envían y reciben la información a través del soporte físico proporcionado por la capa anterior. Es decir, una vez que tenemos un cable, ¿cómo se transmite la información por ese cable? ¿Cuándo puede una estación transmitir? ¿Tiene que esperar algún turno o transmite sin más? ¿Cómo sabe una estación que un mensaje es para ella? Pues bien, son todas estas cuestiones las que resuelve esta capa.

Las dos capas anteriores quedan a un nivel inferior del protocolo TCP/IP, es decir, no forman parte de este protocolo. La capa de red define la forma en que un mensaje se transmite a través de distintos tipos de redes hasta llegar a su destino. El principal protocolo de esta capa es el IP aunque también se encuentran a este nivel los protocolos ARP, ICMP e IGMP. Esta capa proporciona el direccionamiento IP y determina la ruta óptima a través de los encaminadores (*routers*) que debe seguir un paquete desde el origen al destino.

La capa de transporte (protocolos TCP y UDP) ya no se preocupa de la ruta que siguen los mensajes hasta llegar a su destino. Sencillamente, considera que la comunicación extremo a extremo está establecida y la utiliza. Además añade la noción de puertos, como veremos más adelante.

Una vez que tenemos establecida la comunicación desde el origen al destino nos queda lo más importante, ¿qué podemos transmitir? La capa de aplicación nos proporciona los distintos servicios de Internet: correo electrónico, páginas Web, FTP, TELNET…

7.3 Arquitectura de TCP/IP

TCP/IP no es un único protocolo, sino que es en realidad lo que se conoce con este nombre es un conjunto de protocolos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (Transmission Control Protocol) y el IP (Internet Protocol), que son los que dan nombre al conjunto. La arquitectura del TCP/IP consta de cinco niveles o capas en las que se agrupan los protocolos, y que se relacionan con los niveles OSI de la siguiente manera:

1. Aplicación: Se corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota

(TELNET) y otros más recientes como el protocolo HTTP (*Hypertext Transfer Protocol*).

2. Transporte: Coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.

3. Internet: Es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes. Es utilizado con esta finalidad por los protocolos del nivel de transporte.

   - Físico : Análogo al nivel físico del OSI.
   - Red : Es la interfaz de la red real. TCP/IP no especifíca ningún protocolo concreto, así es que corre por las interfaces conocidas, como por ejemplo: 802.2, CSMA/CD, X.25, etc.

Fig: Arquitectura TCP/IP

El TCP/IP necesita funcionar sobre algún tipo de red o de medio físico que proporcione sus propios protocolos para el nivel de enlace de Internet. Por este motivo hay que tener en cuenta que los protocolos utilizados en este nivel pueden ser muy diversos y no forman parte del conjunto TCP/IP. Sin embargo, esto no debe ser problemático puesto que una de las funciones y ventajas principales del TCP/IP es proporcionar una abstracción del medio de forma que sea posible el intercambio de información entre medios diferentes y tecnologías que inicialmente son incompatibles.

Para transmitir información a través de TCP/IP, ésta debe ser dividida en unidades de menor tamaño. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren y, por otro lado, esto es algo común en cualquier protocolo de comunicaciones. En TCP/IP cada una de estas unidades de información recibe el nombre de "datagrama" (*datagram*), y son conjuntos de datos que se envían como mensajes independientes.

7.4 Protocolos TCP/IP

FTP, SMTP, TELNET	SNMP, X-WINDOWS, RPC, NFS
TCP	UDP
IP, ICMP, 802.2, X.25	
ETHERNET, IEEE 802.2, X.25	

- FTP (File Transfer Protocol). Se utiliza para transferencia de archivos.
- SMTP (Simple Mail Transfer Protocol). Es una aplicación para el correo electrónico.
- TELNET: Permite la conexión a una aplicación remota desde un proceso o Terminal.
- RPC (Remote Procedure Call). Permite llamadas a procedimientos situados remotamente. Se utilizan las llamadas a RPC como si fuesen procedimientos locales.
- SNMP (Simple Network Management Protocol). Se trata de una aplicación para el control de la red.
- NFS (Network File System). Permite la utilización de archivos distribuidos por los programas de la red.
- X-Windows. Es un protocolo para el manejo de ventanas e interfaces de usuario.

7.5 Características de TCP/IP

Ya que dentro de un sistema TCP/IP los datos transmitidos se dividen en pequeños paquetes, éstos resaltan una serie de características.

- La tarea de IP es llevar los datos a granel (los paquetes) de un sitio a otro. Las computadoras que encuentran las vías para llevar los datos de una red a otra (denominadas enrutadores) utilizan IP para trasladar los datos. En resumen *IP mueve*

los paquetes de datos a granel, mientras TCP se encarga del flujo y asegura que los datos estén correctos.

- Las líneas de comunicación se pueden compartir entre varios usuarios. Cualquier tipo de paquete puede transmitirse al mismo tiempo, y se ordenará y combinará cuando llegue a su destino. Compare esto con la manera en que se transmite una conversación telefónica.

- Los datos no tienen que enviarse directamente entre dos computadoras. Cada paquete pasa de computadora en computadora hasta llegar a su destino.

- Los paquetes no necesitan seguir la misma trayectoria. La red puede llevar cada paquete de un lugar a otro y usar la conexión más idónea que esté disponible en ese instante. No todos los paquetes de los mensajes tienen que viajar, necesariamente, por la misma ruta, ni necesariamente tienen que llegar todos al mismo tiempo.

- La flexibilidad del sistema lo hace muy confiable. Si un enlace se pierde, el sistema usa otro. Cuando usted envía un mensaje, el TCP divide los datos en paquetes, ordena éstos en secuencia, agrega cierta información para control de errores y después los lanza hacia fuera, y los distribuye. En el otro extremo, el TCP recibe los paquetes, verifica si hay errores y los vuelve a combinar para convertirlos en los datos originales. De haber error en algún punto, el programa TCP destino envía un mensaje solicitando que se vuelvan a enviar determinados paquetes.

7.6 Como Funciona TCP/IP

7.6.1 IP

IP a diferencia del protocolo X.25, que está orientado a conexión, es sin conexión. Está basado en la idea de los datagramas interred, los cuales son transportados transparentemente, pero no siempre con seguridad, desde el host fuente hasta el host destinatario, quizás recorriendo varias redes mientras viaja.

El protocolo IP trabaja de la siguiente manera; la capa de transporte toma los mensajes y los divide en datagramas, de hasta 64K octetos cada uno. Cada datagrama se transmite a través de la red interred, posiblemente fragmentándose en unidades más pequeñas, durante su recorrido normal. Al final, cuando todas las piezas llegan a la máquina destinataria, la capa de transporte los reensambla para así reconstruir el mensaje original.

Un datagrama IP consta de una parte de cabecera y una parte de texto. La cabecera tiene una parte fija de 20 octetos y una parte opcional de longitud variable. En la figura 1 se muestra el formato de la cabecera. El campo *Versión* indica a qué versión del protocolo

pertenece cada uno de los datagramas. Mediante la inclusión de la versión en cada datagrama, no se excluye la posibilidad de modificar los protocolos mientras la red se encuentre en operación.

El campo *Opciones* se utiliza para fines de seguridad, encaminamiento fuente, informe de errores, depuración, sellado de tiempo, así como otro tipo de información. Esto, básicamente, proporciona un escape para permitir que las versiones subsiguientes de los protocolos incluyan información que actualmente no está presente en el diseño original. También, para permitir que los experimentadores trabajen con nuevas ideas y para evitar, la asignación de bits de cabecera a información que muy rara vez se necesita.

Debido a que la *longitud de la cabecera* no es constante, un campo de la cabecera, *IHL*, permite que se indique la longitud que tiene la cabecera en palabras de 32 bits. El valor mínimo es de 5. Tamaño 4 bit.

El campo *Tipo de servicio* le permite al hostal indicarle a la subred el tipo de servicio que desea. Es posible tener varias combinaciones con respecto a la seguridad y la velocidad. Para voz digitalizada, por ejemplo, es más importante la entrega rápida que corregir errores de transmisión. En tanto que, para la transferencia de archivos, resulta más importante tener la transmisión fiable que entrega rápida. También, es posible tener algunas otras combinaciones, desde un tráfico rutinario, hasta una anulación instantánea. Tamaño 8 bit.

La *Longitud total* incluye todo lo que se encuentra en el datagrama -tanto la cabecera como los datos. La máxima longitud es de 65 536 octetos(bytes). Tamaño 16 bit.

El campo *Identificación* se necesita para permitir que el hostal destinatario determine a qué datagrama pertenece el fragmento recién llegado. Todos los fragmentos de un datagrama contienen el mismo valor de identificación. Tamaño 16 bits.

Enseguida viene un bit que no se utiliza, y después dos campos de 1 bit. Las letras *DF* quieren decir no fragmentar. Esta es una orden para que las pasarelas no fragmenten el datagrama, porque el extremo destinatario es incapaz de poner las partes juntas nuevamente. Por ejemplo, supóngase que se tiene un datagrama que se carga en un micro pequeño para su ejecución; podría marcarse con DF porque la ROM de micro espera el programa completo en un datagrama. Si el datagrama no puede pasarse a través de una red, se deberá encaminar sobre otra red, o bien, desecharse.

Las letras *MF* significan más fragmentos. Todos los fragmentos, con excepción del último, deberán tener ese bit puesto. Se utiliza como una verificación doble contra el campo de

Longitud total, con objeto de tener seguridad de que no faltan fragmentos y que el datagrama entero se reensamble por completo.

El *desplazamiento de fragmento* indica el lugar del datagrama actual al cual pertenece este fragmento. En un datagrama, todos los fragmentos, con excepción del último, deberán ser un múltiplo de 8 octetos, que es la unidad elemental de fragmentación. Dado que se proporcionan 13 bits, hay un máximo de 8192 fragmentos por datagrama, dando así una longitud máxima de datagrama de 65 536 octetos, que coinciden con el campo *Longitud total*. Tamaño 16 bits.

El campo *Tiempo de vida* es un contador que se utiliza para limitar el tiempo de vida de los paquetes. Cuando se llega a cero, el paquete se destruye. La unidad de tiempo es el segundo, permitiéndose un tiempo de vida máximo de 255 segundos. Tamaño 8 bits.

Cuando la capa de red ha terminado de ensamblar un datagrama completo, necesitará saber qué hacer con él. El campo *Protocolo* indica, a qué proceso de transporte pertenece el datagrama. El TCP es efectivamente una posibilidad, pero en realidad hay muchas más.

Protocolo: El número utilizado en este campo sirve para indicar a qué protocolo pertenece el datagrama que se encuentra a continuación de la cabecera IP, de manera que pueda ser tratado correctamente cuando llegue a su destino. *Tamaño: 8 bit.*

El *código de redundancia de la cabecera* es necesario para verificar que los datos contenidos en la cabecera IP son correctos. Por razones de eficiencia este campo no puede utilizarse para comprobar los datos incluidos a continuación, sino que estos datos de usuario se comprobarán posteriormente a partir del *código de redundancia* de la cabecera siguiente, y que corresponde al nivel de transporte. Este campo debe calcularse de nuevo cuando cambia alguna opción de la cabecera, como puede ser el tiempo de vida. *Tamaño: 16 bit*

La Dirección de origen contiene la dirección del *host* que envía el paquete. *Tamaño: 32 bit.*

La Dirección de destino: Esta dirección es la del *host* que recibirá la información. Los *routers* o *gateways* intermedios deben conocerla para dirigir correctamente el paquete. *Tamaño: 32 bit.*

7.6.1.1 La Dirección de Internet

La dirección IP es el identificador de cada host dentro de su red de redes. Cada host conectado a una red tiene una dirección IP asignada, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host. En el caso de Internet, no puede haber dos ordenadores con 2 direcciones IP (públicas) iguales. Pero sí podríamos tener dos ordenadores con la misma dirección IP

siempre y cuando pertenezcan a redes independientes entre sí (sin ningún camino posible que las comunique).

Las direcciones IP se clasifican en:

- Direcciones IP públicas. Son visibles en todo Internet. Un ordenador con una IP pública es accesible (visible) desde cualquier otro ordenador conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.

- Direcciones IP privadas (reservadas). Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por routers. Se utilizan en las empresas para los puestos de trabajo. Los ordenadores con direcciones IP privadas pueden salir a Internet por medio de un router (o *proxy*) que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a ordenadores con direcciones IP privadas.

A su vez, las direcciones IP pueden ser:

- Direcciones IP estáticas (fijas). Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas.

- Direcciones IP dinámicas. Un host que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un módem. Los proveedores de Internet utilizan direcciones IP dinámicas debido a que tienen más clientes que direcciones IP (es muy improbable que todos se conecten a la vez).

Las direcciones IP están formadas por 4 bytes (32 bits). Se suelen representar de la forma a.b.c.d donde cada una de estas letras es un número comprendido entre el 0 y el 255. Por ejemplo la dirección IP del servidor de IBM (www.ibm.com) es 129.42.18.99.
Las direcciones IP también se pueden representar en hexadecimal, desde la 00.00.00.00 hasta la FF.FF.FF.FF o en binario, desde la 00000000.00000000.00000000.00000000 hasta la 11111111.11111111.11111111.11111111.
Las tres direcciones siguientes representan a la misma máquina (podemos utilizar la calculadora científica de Windows para realizar las conversiones).

(decimal)	128.10.2.30
(hexadecimal)	80.0A.02.1E
(binario)	10000000.00001010.00000010.00011110

¿Cuántas direcciones IP existen? Si calculamos 2 elevado a 32 obtenemos más de 4000 millones de direcciones distintas. Sin embargo, no todas las direcciones son válidas para asignarlas a hosts. Las direcciones IP no se encuentran aisladas en Internet, sino que pertenecen siempre a alguna red. Todas las máquinas conectadas a una misma red se caracterizan en que los primeros bits de sus direcciones son iguales. De esta forma, las direcciones se dividen conceptualmente en dos partes: el *identificador de red* y el *identificador de host*.

Dependiendo del número de hosts que se necesiten para cada red, las direcciones de Internet se han dividido en las clases primarias A, B y C. La clase D está formada por direcciones que identifican no a un host, sino a un grupo de ellos. Las direcciones de clase E no se pueden utilizar (están reservadas).

- Clase A: Son las que en su primer byte tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer byte para identificar la red, quedando los otros tres bytes disponibles para cada uno de los *hosts* que pertenezcan a esta misma red. Esto significa que podrán existir más de dieciséis millones de ordenadores en cada una de las redes de esta clase. Este tipo de direcciones es usado por redes muy extensas, pero hay que tener en cuenta que sólo puede haber 126 redes de este tamaño. ARPAnet es una de ellas, existiendo además algunas grandes redes comerciales, aunque son pocas las organizaciones que obtienen una dirección de "clase A". Lo normal para las grandes organizaciones es que utilicen una o varias redes de "clase B".

- Clase B: Estas direcciones utilizan en su primer byte un valor comprendido entre 128 y 191, incluyendo ambos. En este caso el identificador de la red se obtiene de los dos primeros bytes de la dirección, teniendo que ser un valor entre 128.1 y 191.254 (no es posible utilizar los valores 0 y 255 por tener un significado especial). Los dos últimos bytes de la dirección constituyen el identificador del *host* permitiendo, por consiguiente, un número máximo de 64516 ordenadores en la misma red. Este tipo de direcciones tendría que ser suficiente para la gran mayoría de las organizaciones grandes. En caso de que el número de ordenadores que se necesita conectar fuese mayor, sería posible obtener más de una dirección de "clase B", evitando de esta forma el uso de una de "clase A".

- Clase C: En este caso el valor del primer byte tendrá que estar comprendido entre 192 y 223, incluyendo ambos valores. Este tercer tipo de direcciones utiliza los tres primeros bytes para el número de la red, con un rango desde 192.1.1 hasta 223.254.254. De esta manera queda libre un byte para el *host*, lo que permite que se conecten un máximo de 254 ordenadores en cada red. Estas direcciones permiten un

menor número de *host* que las anteriores, aunque son las más numerosas pudiendo existir un gran número redes de este tipo (más de dos millones).

- Clase D: Los primeros cuatro bits de una dirección son 1110. estas direcciones se utilizan para un proceso denominados multicast, pero han tenido un uso limitado, Una dirección multicast es una dirección de redunica que dirige paquetes con esa dirección destino a grupos predefinidos de direcciones IP. Las direcciones de red de esta clase D van de 224.0.0.0 a 239.255.255.254

- Clase E: Se ha definido una dirección de clase E, pero esta reservada por el IETF para su propia investigación. Este intervalo va por deducción, de 240.0.0.0 a 255.255.255.0.

Tabla de direcciones IP de Internet

CLASE	PRIMER BYTE	IDENTIFICACION DE RED	IDENTIFICACION DE HOST	NUMERO DE REDES	NUMERO DE HOST
A	1 ... 126	1 BYTE	3 BYTE	126	16.387.064
B	128 ... 191	2 BYTE	2 BYTE	16.256	64.516
C	192 ... 223	3 BYTE	1 BYTE	2.064.512	254
D	224 ... 239	.....	.....	.....	.....
E	240 ... 255	.....	.....	.....	.....

7.6.1.2 Direcciones IP Especiales y Reservadas

No todas las direcciones comprendidas entre la 0.0.0.0 y la 223.255.255.255 son válidas para un host: algunas de ellas tienen significados especiales. Las principales direcciones especiales se resumen en la siguiente tabla. Su interpretación depende del host desde el que se utilicen.

Bits de red	Bits de host	Significado	Ejemplo
todos 0		Mi propio host	0.0.0.0
todos 0	host	Host indicado dentro de mi red	0.0.0.10
red	todos 0	Red indicada	192.168.1.0
todos 1		Difusión a mi red	255.255.255.255
red	todos 1	Difusión a la red indicada	192.168.1.255
127	cualquier valor válido de host	Loopback (mi propio host)	127.0.0.1

Difusión o *broadcasting* es el envío de un mensaje a todos los ordenadores que se encuentran en una red. La dirección de *loopback* (normalmente 127.0.0.1) se utiliza para comprobar que los protocolos TCP/IP están correctamente instalados en nuestro propio ordenador. Lo veremos más adelante, al estudiar el comando PING.

Las direcciones de redes siguientes se encuentran reservadas para su uso en redes privadas (*intranets*). Una dirección IP que pertenezca a una de estas redes se dice que es una dirección IP privada.

CLASE	RANGO DE DIRECCIONES RESERVADAS DE REDES
A	10.0.0.0
B	172.16.0.0 – 172.31.0.0
C	192.168.0.0 – 192.168.255.0

Intranet.-- Red privada que utiliza los protocolos TCP/IP. Puede tener salida a Internet o no. En el caso de tener salida a Internet, el direccionamiento IP permite que los hosts con direcciones IP privadas puedan salir a Internet pero impide el acceso a los hosts internos desde Internet. Dentro de una intranet se pueden configurar todos los servicios típicos de Internet (web, correo, mensajería instantánea, etc.) mediante la instalación de los correspondientes servidores. La idea es que las intranets son como "internets" en miniatura o lo que es lo mismo, Internet es una intranet pública gigantesca.

Extranet.-- Unión de dos o más intranets. Esta unión puede realizarse mediante líneas dedicadas (RDSI, X.25, frame relay, punto a punto, etc.) o a través de Internet.

Internet.-- La mayor red pública de redes TCP/IP.

Por ejemplo, si estamos construyendo una red privada con un número de ordenadores no superior a 254 podemos utilizar una red reservada de clase C. Al primer ordenador le podemos asignar la dirección 192.168.23.1, al segundo 192.168.23.2 y así sucesivamente hasta la 192.168.23.254. Como estamos utilizando direcciones reservadas, tenemos la garantía de que no habrá ninguna máquina conectada directamente a Internet con alguna de nuestras direcciones. De esta manera, no se producirán conflictos y desde cualquiera de nuestros ordenadores podremos acceder a la totalidad de los servidores de Internet .

7.6.1.3 Mascara de Subred

Una máscara de subred es aquella dirección que enmascarando nuestra dirección IP, nos indica si otra dirección IP pertenece a nuestra subred o no.

La siguiente tabla muestra las máscaras de subred correspondientes a cada clase:

Clase	Máscara de subred

A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Si expresamos la máscara de subred de clase A en notación binaria, tenemos:
11111111.00000000.00000000.00000000
Los unos indican los bits de la dirección correspondientes a la red y los ceros, los correspondientes al host. Según la máscara anterior, el primer byte (8 bits) es la red y los tres siguientes (24 bits), el host. Por ejemplo, la dirección de clase A 35.120.73.5 pertenece a la red 35.0.0.0.
Supongamos una subred con máscara 255.255.0.0, en la que tenemos un ordenador con dirección 148.120.33.110. Si expresamos esta dirección y la de la máscara de subred en binario, tenemos:

```
148.120.33.1      10 10010100.01111000.00100001.01101110
      (dirección de una máquina)
255.255.0.0       11111111.11111111.00000000.00000000 (dirección  de
su máscara de red).
148.120.0.0       10010100.01111000.00000000.00000000
      (dirección de su subred)
                                          <------RED------> <------
HOST----->
```

Al hacer el producto binario de las dos primeras direcciones (donde hay dos 1 en las mismas posiciones ponemos un 1 y en caso contrario, un 0) obtenemos la tercera.
Si hacemos lo mismo con otro ordenador, por ejemplo el 148.120.33.89, obtenemos la misma dirección de subred. Esto significa que ambas máquinas se encuentran en la misma subred (la subred 148.120.0.0).

```
148.120.33.89  10010100.01111000.00100001.01011001  (dirección  de  una
máquina)
255.255.0.0      11111111.11111111.00000000.00000000  (dirección  de  su
máscara                              de                              red)
148.120.0.0              10010100.01111000.00000000.00000000 (dirección
de su subred)
```

En cambio, si tomamos la 148.115.89.3, observamos que no pertenece a la misma subred que las anteriores.

148.115.89.3 10010100.01110011.01011001.00000011 (dirección de una máquina)
255.255.0.0 11111111.11111111.00000000.00000000 (dirección de su máscara de red)
148.115.0.0 10010100.01110011.00000000.00000000 (dirección de su subred).

Cálculo de la dirección de difusión.-- Ya hemos visto que el producto lógico binario (AND) de una IP y su máscara devuelve su dirección de red. Para calcular su dirección de difusión, hay que hacer la suma lógica en binario (OR) de la IP con el inverso (NOT) de su máscara.
En una red de redes TCP/IP no puede haber hosts aislados: todos pertenecen a alguna red y todos tienen una dirección IP y una máscara de subred (si no se especifica se toma la máscara que corresponda a su clase). Mediante esta máscara un ordenador sabe si otro ordenador se encuentra en su misma subred o en otra distinta. Si pertenece a su misma subred, el mensaje se entregará directamente. En cambio, si los hosts están configurados en redes distintas, el mensaje se enviará a la puerta de salida o router de la red del host origen. Este router pasará el mensaje al siguiente de la cadena y así sucesivamente hasta que se alcance la red del host destino y se complete la entrega del mensaje.

7.6.1.4 Protocolos IP

IP es el principal protocolo de la capa de red. Este protocolo define la unidad básica de transferencia de datos entre el origen y el destino, atravesando toda la red de redes. Además, el software IP es el encargado de elegir la ruta más adecuada por la que los datos serán enviados. Se trata de un sistema de entrega de paquetes (llamados *datagramas IP*) que tiene las siguientes características:

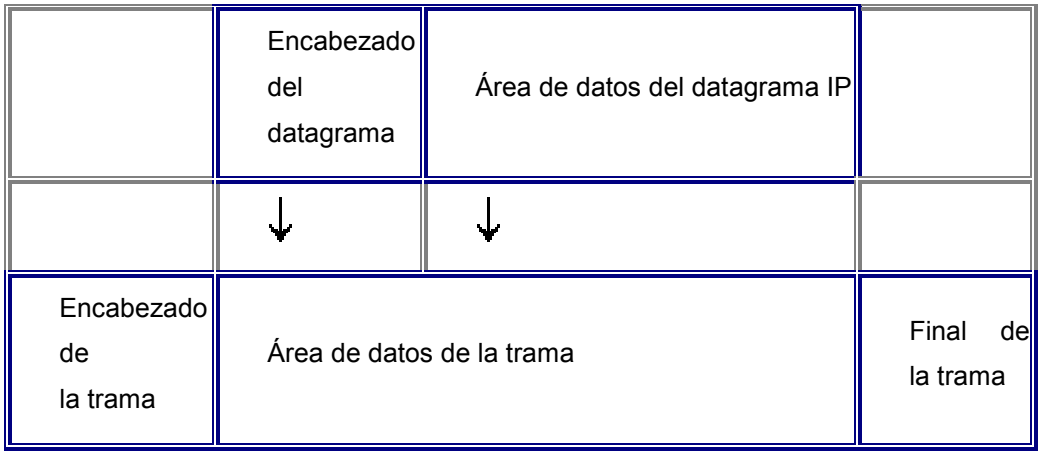
- Es no orientado a conexión debido a que cada uno de los paquetes puede seguir rutas distintas entre el origen y el destino. Entonces pueden llegar duplicados o desordenados.

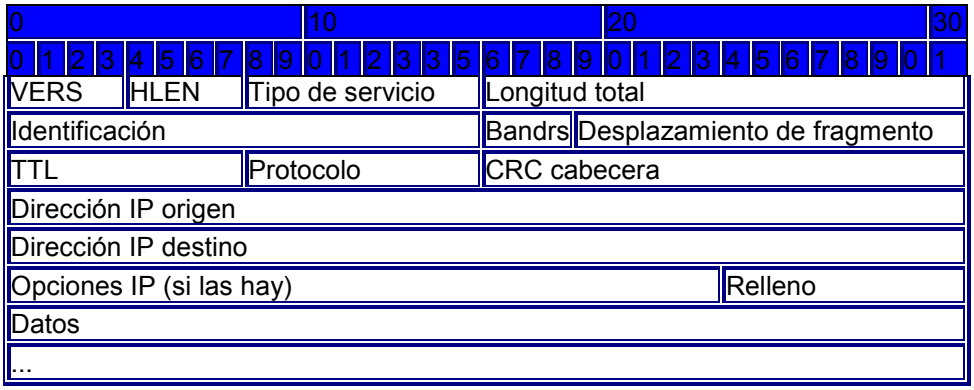
- Es no fiable porque los paquetes pueden perderse, dañarse o llegar retrasados.

7.6.1.5 Formato del Datagrama IP

El datagrama IP es la unidad básica de transferencia de datos entre el origen y el destino. Viaja en el campo de datos de las tramas físicas de las distintas redes que va atravesando. Cada vez que un datagrama tiene que atravesar un router, el datagrama *saldrá* de la trama física de la red que abandona y se *acomodará* en el campo de datos de una trama física de la siguiente red. Este mecanismo permite que un mismo datagrama IP pueda atravesar redes distintas: enlaces

punto a punto, redes ATM, redes Ethernet, redes Token Ring, etc. El propio datagrama IP tiene también un campo de datos: será aquí donde viajen los paquetes de las capas superiores.





Campos del datagrama IP:

VERS (4 bits). Indica la versión del protocolo IP que se utilizó para crear el datagrama. Actualmente se utiliza la versión 4 (IPv4) aunque ya se están preparando las especificaciones de la siguiente versión, la 6 (IPv6).

HLEN (4 bits). Longitud de la cabecera expresada en múltiplos de 32 bits. El valor mínimo es 5, correspondiente a 160 bits = 20 bytes.

Tipo de servicio *(Type Of Service)*. Los 8 bits de este campo se dividen a su vez en:

Prioridad (3 bits). Un valor de 0 indica baja prioridad y un valor de 7, prioridad máxima.

Los siguientes tres bits indican cómo se prefiere que se transmita el mensaje, es decir, son sugerencias a los encaminadores que se encuentren a su paso los cuales pueden tenerlas en cuenta o no.

Bit D *(Delay)*. Solicita retardos cortos (enviar rápido).

Bit T *(Throughput)*. Solicita un alto rendimiento (enviar mucho en el menor tiempo posible).
Bit R *(Reliability)*. Solicita que se minimice la probabilidad de que el datagrama se pierda o resulte dañado (enviar bien).
Los siguientes dos bits no tienen uso.
Longitud total (16 bits). Indica la longitud total del datagrama expresada en bytes. Como el campo tiene 16 bits, la máxima longitud posible de un datagrama será de 65535 bytes.
Identificación (16 bits). Número de secuencia que junto a la dirección origen, dirección destino y el protocolo utilizado identifica de manera única un datagrama en toda la red. Si se trata de un datagrama fragmentado, llevará la misma identificación que el resto de fragmentos.
Banderas o indicadores (3 bits). Sólo 2 bits de los 3 bits disponibles están actualmente utilizados. El bit de *Más fragmentos* (MF) indica que no es el último datagrama. Y el bit de *No fragmentar* (NF) prohíbe la fragmentación del datagrama. Si este bit está activado y en una determinada red se requiere fragmentar el datagrama, éste no se podrá transmitir y se descartará.
Desplazamiento de fragmentación (13 bits). Indica el lugar en el cual se insertará el fragmento actual dentro del datagrama completo, medido en unidades de 64 bits. Por esta razón los campos de datos de todos los fragmentos menos el último tienen una longitud múltiplo de 64 bits. Si el paquete no está fragmentado, este campo tiene el valor de cero.
Tiempo de vida o TTL (8 bits). Número máximo de segundos que puede estar un datagrama en la red de redes. Cada vez que el datagrama atraviesa un router se resta 1 a este número. Cuando llegue a cero, el datagrama se descarta y se devuelve un mensaje ICMP de tipo "tiempo excedido" para informar al origen de la incidencia.
Protocolo (8 bits). Indica el protocolo utilizado en el campo de datos: 1 para ICMP, 2 para IGMP, 6 para TCP y 17 para UDP.
CRC cabecera (16 bits). Contiene la suma de comprobación de errores sólo para la cabecera del datagrama. La verificación de errores de los datos corresponde a las capas superiores.
Dirección origen (32 bits). Contiene la dirección IP del origen.
Dirección destino (32 bits). Contiene la dirección IP del destino.

7.6.2 TCP

Una entidad de transporte TCP acepta mensajes de longitud arbitrariamente grande procedentes de los procesos de usuario, los separa en pedazos que no excedan de 64K octetos y, transmite cada pedazo como si fuera un datagrama separado. La capa de red, no garantiza que los datagramas se entreguen apropiadamente, por lo que TCP deberá utilizar temporizadores y retransmitir los datagramas si es necesario. Los datagramas que consiguen llegar, pueden hacerlo en desorden; y dependerá de TCP el hecho de reensamblarlos en mensajes, con la secuencia correcta.

Cada octeto de datos transmitido por TCP tiene su propio número de secuencia privado. El espacio de números de secuencia tiene una extensión de 32 bits, para asegurar que los duplicados antiguos hayan desaparecidos, desde hace tiempo, en el momento en que los números de secuencia den la vuelta. TCP, sin embargo, sí se ocupa en forma explícita del problema de los duplicados retardados cuando intenta establecer una conexión, utilizando el protocolo de ida-vuelta-ida para este propósito.

En la figura 2 se muestra la cabecera que se utiliza en TCP. La primera cosa que llama la atención es que la cabecera mínima de TCP sea de 20 octetos. A diferencia de la clase 4 del modelo OSI, con la cual se puede comparar a grandes rasgos, TCP sólo tiene un formato de cabecera de TPDU(llamadas mensajes). Enseguida se analizará minuciosamente campo por campo, esta gran cabecera. Los campos *Puerto fuente y Puerto destino* identifican los puntos terminales de la conexión(las direcciones TSAP de acuerdo con la terminología del modelo OSI). Cada hostal deberá decidir por sí mismo cómo asignar sus puertos.

Los campos *Número de secuencia y Asentimiento en superposición* efectúan sus funciones usuales. Estos tienen una longitud de 32 bits, debido a que cada octeto de datos está numerado en TCP.

La *Longitud de la cabecera TCP* indica el número de palabra de 32 bits que están contenidas en la cabecera de TCP. Esta información es necesaria porque el campo *Opciones* tiene una longitud variable, y por lo tanto la cabecera también.

Después aparecen seis banderas de 1 bit. Si el *Puntero acelerado* se está utilizando, entonces URG se coloca a 1. *El puntero acelerado* se emplea para indicar un desplazamiento en octetos a partir del número de secuencia actual en el que se encuentran datos acelerados. Esta facilidad se brinda en lugar de los mensajes de interrupción. El bit SYN se utiliza para el establecimiento de conexiones. La solicitud de conexión tiene SYN=1 y ACK=0, para indicar que el campo de asentimiento en superposición no se está utilizando. La respuesta a la solicitud de conexión si lleva un asentimiento, por lo que tiene SYN=1 y ACK=1. En esencia, el bit SYN se utiliza para denotar las TPDU CONNECTION REQUEST Y CONNECTION CONFIRM, con el bit ACK utilizado para distinguir entre estas dos posibilidades. El bit FIN se utiliza para liberar la conexión; especifica que el emisor ya no tiene más datos. Después de cerrar una conexión, un proceso puede seguir recibiendo datos indefinidamente. El bit RST se utiliza para reiniciar una conexión que se ha vuelto confusa debido a SYN duplicados y retardados, o a caída de los hostales. El bit EOM indica el Fin del Mensaje.

El control de flujo en TCP se trata mediante el uso de una *ventana* deslizante de tamaño variable. Es necesario tener un campo de 16 bits, porque la ventana indica el número de octetos

que se pueden transmitir más allá del octeto asentido por el campo ventana y no cuántas TPDU.

El *código de redundancia* también se brinda como un factor de seguridad extrema. El algoritmo de código de redundancia consiste en sumar simplemente todos los datos, considerados como palabras de 16 bits, y después tomar el complemento a 1 de la suma.

El campo de *Opciones* se utiliza para diferentes cosas, por ejemplo para comunicar tamaño de tampones durante el procedimiento de establecimiento.

7.7 Similitud y diferencias entre la Clase 4 del Modelo OSI y TCP

El protocolo de transporte de clase 4 del modelo OSI (al que con frecuencia se le llama TP4), y TCP tienen numerosas similitudes, pero también algunas diferencias. Los dos protocolos están diseñados para proporcionar un servicio de transporte seguro, orientado a conexión y de extremo a extremo, sobre una red insegura, que puede perder, dañar, almacenar y duplicar paquetes. Los dos deben enfrentarse a los peores problemas como sería el caso de una subred que pudiera almacenar una secuencia válida de paquetes y más tarde volviera a entregarlos.

Los dos protocolos también son semejantes por el hecho de que los dos tienen una fase de establecimiento de conexión, una fase de transferencia de datos y después una fase de liberación de la conexión. Los conceptos generales del establecimiento, uso y liberación de conexiones también son similares, aunque difieren en algunos detalles. En particular, tanto TP4 como TCP utilizan la comunicación ida-vuelta-ida para eliminar las dificultades potenciales ocasionadas por paquetes antiguos que aparecieran súbitamente y pudiesen causar problemas.

Sin embargo, los dos protocolos también presentan diferencias muy notables, las cuales se pueden observar en la lista que se muestra en la figura 3. Primero, TP4 utiliza nueve tipos diferentes de TPDU, en tanto que TCP sólo tiene uno. Esta diferencia trae como resultado que TCP sea más sencillo, pero al mismo tiempo también necesita una cabecera más grande, porque todos los campos deben estar presentes en todas las TPDU. El mínimo tamaño de la cabecera TCP es de 20 octetos; el mínimo tamaño de la cabecera TP4 es de 5 octetos. Los dos protocolos permiten campos opcionales, que pueden incrementar el tamaño de las cabeceras por encima del mínimo permitido.

CARACTERÍSTICA	OSI TP4	TCP

Numero de tipos de TPDU	9	1
Fallo de Conexión	2 conexiones	1 conexión
Formato de direcciones	No está definido	32 bits
Calidad de servicio	Extremo abierto	Opciones específicas
Datos del usuario en CR	Permitido	No permitido
Flujo	Mensajes	Octetos
Datos importantes	Acelerados	Acelerados
Superposición	No	Sí
Control de flujo explícito	Algunas veces	Siempre
Número de subsecuencia	Permitidos	No Permitido
Liberación	Abrupta	Ordenada

Figura 3: Diferencias entre el protocolo TP4 del modelo OSI y TCP

Una segunda diferencia es con respecto a lo que sucede cuando los dos procesos, en forma simultánea, intentan establecer conexiones entre los mismos dos TSAP (es decir, una colisión de conexiones). Con TP4 se establecen dos conexiones duplex independientes; en tanto que con TCP, una conexión se identifica mediante un par de TSAP, por lo que solamente se establece una conexión.

Una tercera diferencia es con respecto al formato de direcciones que se utiliza. TP4 no especifica el formato exacto de una dirección TSAP; mientras que TCP utiliza números de 32 bits.

El concepto de calidad de servicio también se trata en forma diferente en los dos protocolos, constituyendo la cuarta diferencia. TP4 tiene un mecanismo de extremo abierto, bastante elaborado, para una negociación a tres bandas sobre la calidad de servicio. Esta negociación incluye al proceso que hace la llamada, al proceso que es llamado y al mismo servicio de

transporte. Se pueden especificar muchos parámetros, y pueden proporcionarse los valores: deseado y mínimo aceptable. A diferencia de esto, TCP no tiene ningún campo de calidad de servicio, sino que el servicio subyacente IP tiene un campo de 8 bits, el cual permite que se haga una relación a partir de un número limitado de combinaciones de velocidad y seguridad.

Una quinta diferencia es que TP4 permite que los datos del usuario sean transportados en la TPDU CR, pero TCP no permite que los datos del usuario aparezcan en la TPDU inicial. El dato inicial (como por ejemplo, una contraseña), podría ser necesario para decidir si se debe, o no, establecer una conexión. Con TCP no es posible hacer que el establecimiento dependa de los datos del usuario.

Las cuatro diferencias anteriores se relacionan con la fase de establecimiento de la conexión. Las cinco siguientes se relacionan con la fase de transferencia de datos. Una diferencia básica es el modelo del transporte de datos. El modelo TP4 es el de una serie de mensajes ordenados (correspondientes a las TSDU en la terminología OSI). El modelo TCP es el de un flujo continuo de octetos, sin que haya ningún límite explícito entre mensajes. En la práctica, sin embargo, el modelo TCP no es realmente un flujo puro de octetos, porque el procedimiento de biblioteca denominado push puede llamarse para sacar todos los datos que estén almacenados, pero que todavía no se hayan transmitido. Cuando el usuario remoto lleva a cabo una operación de lectura, los datos anteriores y posteriores al push no se combinarán, por lo que, en cierta forma un push podría penarse como si definiesen una frontera entre mensajes.

La séptima diferencia se ocupa de cómo son tratados los datos importantes que necesitan de un procesamiento especial (como los caracteres BREAK). TP4 tiene dos flujos de mensajes independientes, los datos normales y los acelerados multiplexados de manera conjunta. En cualquier instante únicamente un mensaje acelerado puede estar activo. TCP utiliza el campo Acelerado para indicar que cierta cantidad de octetos, dentro de la TPDU actualmente en uso, es especial y debería procesarse fuera de orden.

La octava diferencia es la ausencia del concepto de superposición en TP4 y su presencia en TCP. Esta diferencia no es tan significativa como al principio podría parecer, dado que es posible que una entidad de transporte ponga dos TPDU, por ejemplo, DT y AK en un único paquete de red.

La novena diferencia se relaciona con la forma como se trata el control de flujo. TP4 puede utilizar un esquema de crédito, pero también se puede basar en el esquema de ventana de la capa de red para regular el flujo. TCP siempre utiliza un mecanismo de control de flujo explícito con el tamaño de la ventana especificado en cada TPDU.

La décima diferencia se relaciona con este esquema de ventana. En ambos protocolos el receptor tiene la capacidad de reducir la ventana en forma voluntaria. Esta posibilidad genera potencialmente problemas, si el otorgamiento de una ventana grande y su contracción subsiguiente llegan en un orden incorrecto. En TCP no hay ninguna solución para este problema; en tanto en TP4 éste se resuelve por medio del número de subsecuencia que está incluido en la contracción, permitiendo de esta manera que el emisor determine si la ventana pequeña siguió, o precedió, a la más grande.

Finalmente, la onceava y última diferencia existente entre los dos protocolos, consiste en la manera como se liberan las conexiones. TP4 utiliza una desconexión abrupta en la que una serie de TPDU de datos pueden ser seguidos directamente por una TPDU DR. Si las TPDU de datos se llegaran a perder, el protocolo no los podría recuperar y la información, al final se perdería. TCP utiliza una comunicación de ida-vuelta-ida para evitar la pérdida de datos en el momento de la desconexión. El modelo OSI trata este problema en la capa de sesión. Es importante hacer notar que la Oficina Nacional de Normalización de Estados Unidos estaba tan disgustada con esta propiedad de TP4, que introdujo TPDU adicionales en el protocolo de transporte para permitir la desconexión sin que hubiera una pérdida de datos. Como consecuencia de esto, las versiones de Estados Unidos y la internacional de TP4 son diferentes.

7.8 La nueva Versión de IP (IPng)

La nueva versión del protocolo IP recibe el nombre de IPv6, aunque es también conocido comúnmente como IPng (*Internet Protocol Next Generation*). El número de versión de este protocolo es el 6 frente a la antigua versión utilizada en forma mayoritaria. Los cambios que se introducen en esta nueva versión son muchos y de gran importancia, aunque la transición desde la versión antigua no debería ser problemática gracias a las características de compatibilidad que se han incluido en el protocolo. IPng se ha diseñado para solucionar todos los problemas que surgen con la versión anterior, y además ofrecer soporte a las nuevas redes de alto rendimiento (como ATM, Gigabit Ethernet, etc.)

Una de las características más llamativas es el nuevo sistema de direcciones, en el cual se pasa de los 32 a los 128 bit, eliminando todas las restricciones del sistema actual. Otro de los aspectos mejorados es la seguridad, que en la versión anterior constituía uno de los mayores problemas. Además, el nuevo formato de la cabecera se ha organizado de una manera más efectiva, permitiendo que las opciones se sitúen en extensiones separadas de la cabecera principal.

7.8.1 Formato de la Cabecera

El tamaño de la cabecera que el protocolo IPv6 añade a los datos es de 320 bit, el doble que en la versión antigua. Sin embargo, esta nueva cabecera se ha simplificado con respecto a la anterior. Algunos campos se han retirado de la misma, mientras que otros se han convertido en opcionales por medio de las extensiones. De esta manera los *routers* no tienen que procesar parte de la información de la cabecera, lo que permite aumentar de rendimiento en la transmisión. El formato completo de la cabecera sin las extensiones es el siguiente:

- Versión: Número de versión del protocolo IP, que en este caso contendrá el valor 6. *Tamaño: 4 bit.*

- Prioridad: Contiene el valor de la prioridad o importancia del paquete que se está enviando con respecto a otros paquetes provenientes de la misma fuente. *Tamaño: 4 bit.*

- Etiqueta de flujo: Campo que se utiliza para indicar que el paquete requiere un tratamiento especial por parte de los *routers* que lo soporten. *Tamaño: 24 bit.*

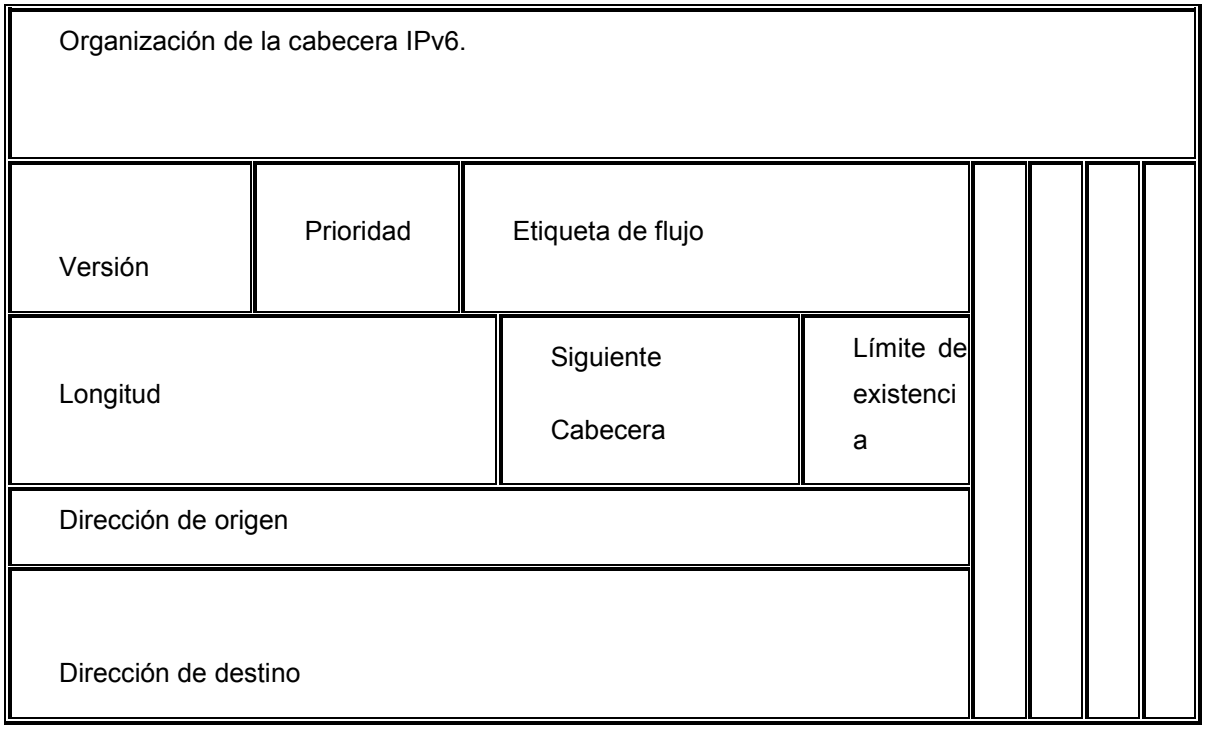
- Longitud: Es la longitud en bytes de los datos que se encuentran a continuación de la cabecera. *Tamaño: 16 bit.*

- Siguiente cabecera: Se utiliza para indicar el protocolo al que corresponde la cabecera que se sitúa a continuación de la actual. El valor de este campo es el mismo que el de protocolo en la versión 4 de IP. *Tamaño: 8 bit.*

- Límite de existencia: Tiene el mismo propósito que el campo de la versión 4, y es un valor que disminuye en una unidad cada vez que el paquete pasa por un nodo. *Tamaño:8 bit.*

- Dirección de origen: El número de dirección del *host* que envía el paquete. Su longitud es cuatro veces mayor que en la versión 4. *Tamaño: 128 bit.*

- Dirección de destino: Número de dirección de destino, aunque puede no coincidir con la dirección del *host* final en algunos casos. Su longitud es cuatro veces mayor que en la versión 4 del protocolo IP. *Tamaño: 128 bit.*



Las extensiones que permite añadir esta versión del protocolo se sitúan inmediatamente después de la cabecera normal, y antes de la cabecera que incluye el protocolo de nivel de transporte. Los datos situados en cabeceras opcionales se procesan sólo cuando el mensaje llega a su destino final, lo que supone una mejora en el rendimiento. Otra ventaja adicional es que el tamaño de la cabecera no está limitado a un valor fijo de bytes como ocurría en la versión 4.

Por razones de eficiencia, las extensiones de la cabecera siempre tienen un tamaño múltiplo de 8 bytes. Actualmente se encuentran definidas extensiones para *routing* extendido, fragmentación y ensamblaje, seguridad, confidencialidad de datos, etc.

7.8.2 Direcciones en la Versión 6

El sistema de direcciones es uno de los cambios más importantes que afectan a la versión 6 del protocolo IP, donde se han pasado de los 32 a los 128 bit (cuatro veces mayor). Estas nuevas direcciones identifican a un interfaz o conjunto de interfaces y no a un nodo, aunque como cada interfaz pertenece a un nodo, es posible referirse a éstos a través de su interfaz.

El número de direcciones diferentes que pueden utilizarse con 128 bits es enorme. Teóricamente serían 2^{128} direcciones posibles, siempre que no apliquemos algún formato u

organización a estas direcciones. Este número es extremadamente alto, pudiendo llegar a soportar más de 665.000 trillones de direcciones distintas por cada metro cuadrado de la superficie del planeta Tierra. Según diversas fuentes consultadas, estos números una vez organizados de forma práctica y jerárquica quedarían reducidos en el peor de los casos a 1.564 direcciones por cada metro cuadrado, y siendo optimistas se podrían alcanzar entre los tres y cuatro trillones.

Existen tres tipos básicos de direcciones IPng según se utilicen para identificar a un interfaz en concreto o a un grupo de interfaces. Los bits de mayor peso de los que componen la dirección IPng son los que permiten distinguir el tipo de dirección, empleándose un número variable de bits para cada caso. Estos tres tipos de direcciones son:

- Direcciones *unicast:* Son las direcciones dirigidas a un único interfaz de la red. Las direcciones *unicast* que se encuentran definidas actualmente están divididas en varios grupos. Dentro de este tipo de direcciones se encuentra también un formato especial que facilita la compatibilidad con las direcciones de la versión 4 del protocolo IP.
- Direcciones *anycast:* Identifican a un conjunto de interfaces de la red. El paquete se enviará a un interfaz cualquiera de las que forman parte del conjunto. Estas direcciones son en realidad direcciones *unicast* que se encuentran asignadas a varios interfaces, los cuales necesitan ser configurados de manera especial. El formato es el mismo que el de las direcciones *unicast*.
- Direcciones *multicast:* Este tipo de direcciones identifica a un conjunto de interfaces de la red, de manera que el paquete es enviado a cada una de ellos individualmente.

Las direcciones de *broadcast* no están implementadas en esta versión del protocolo, debido a que esta misma función puede realizarse ahora mediante el uso de las direcciones *multicast*.

CAPITULO 8.- VOZ SOBRE IP

8.1 Introducción

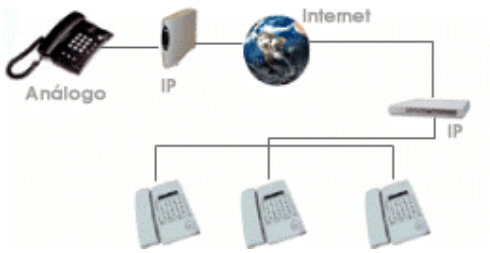
Esta tecnología conjuga dos mundos históricamente separados: la transmisión de voz y la de datos. Se trata de transportar la voz, previamente convertida a datos, entre dos puntos distantes. Esto posibilitaría utilizar las redes de datos para efectuar las llamadas telefónicas, y desarrollar una única red que se encargue de cursar todo tipo de comunicación, ya sea vocal o de datos.

El crecimiento y fuerte implantación de las redes IP, tanto en local como en remoto, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que permitan la calidad de servicio en redes IP, han creado un entorno donde es posible transmitir telefonía sobre IP lo que no significará en modo alguno la desaparición de las redes telefónicas modo circuito, sino que habrá, al menos temporalmente, una fase de coexistencia entre ambas.

8.2 Definición

Los productos de telefonía por Internet se denominan: Telefonía IP (IP telephony) Voz sobre Internet -Voice over the Internet (VOI)- o Voz sobre IP -Voice over IP (VOIP).

La Voz sobre IP es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos. La Telefonía IP es una aplicación inmediata de esta tecnología, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un PC, gateways y teléfonos estándares.



8.3 Elementos de la Voz sobre IP

El modelo de Voz sobre IP está formado por tres principales elementos:

- El cliente. Este elemento establece y termina las llamadas de voz. Codifica, empaqueta y transmite la información de salida generada por el micrófono del usuario. Asimismo, recibe, decodifica y reproduce la información de voz de entrada a través de los altavoces o audífonos del usuario. Cabe destacar que el elemento cliente se presenta en dos formas básicas: la primera es una suite de software corriendo en una PC que el usuario controla mediante una interfase gráfica (GUI); y la segunda puede ser un cliente "virtual" que reside en el gateway.

- Servidores. El segundo elemento de la Voz sobre IP está basado en servidores, los cuales manejan un amplio rango de operaciones complejas de bases de datos, tanto en tiempo real como fuera de él. Estas operaciones incluyen validación de usuarios, tasación, contabilidad, tarificación, recolección, distribución de utilidades, enrutamiento, administración general del servicio, carga de clientes, control del servicio, registro de usuarios y servicios de directorio entre otros.

- Gateways. El tercer elemento lo conforman los gateways de Voz sobre IP, los cuales proporcionan un puente de comunicación entre los usuarios. La función principal de un gateway es proveer las interfases con la telefonía tradicional apropiada, funcionando como una plataforma para los clientes virtuales.

Estos equipos también juegan un papel importante en la seguridad de acceso, la contabilidad, el control de calidad del servicio (QoS; Quality of Service) y en el mejoramiento del mismo.

8.4 Características de Voz sobre IP

Por su estructura el estándar proporciona las siguientes características:

Permite el control del tráfico de la red, por lo que se disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento de las redes de datos.

Proporciona el enlace a la red telefónica tradicional.

Al tratarse de una tecnología soportada en IP presenta las siguientes ventajas adicionales:

Es independiente del tipo de red física que lo soporta. Permite la integración con las grandes redes de IP actuales.

Es independiente del hardware utilizado.

Permite ser implementado tanto en *software* como en hardware, con la particularidad de que el hardware supondría eliminar el impacto inicial para el usuario común.

8.5 Protocolos de Voz sobre IP

Hoy en día, existen dos protocolos para transmitir voz sobre IP, ambos definen la manera en que los dispositivos de este tipo deben establecer comunicación entre sí, además de incluir especificaciones para codecs (codificador-decodificador) de audio para convertir una señal auditiva a una digitalizada compresa y viceversa.

H.323

H.323 es el estándar creado por la Unión Internacional de Telecomunicaciones (ITU) que se compone por un protocolo sumamente complejo y extenso, el cual además de incluir la voz sobre IP, ofrece especificaciones para vídeo-conferencias y aplicaciones en tiempo real, entre otras variantes.

Session Initiation Protocol (SIP)

Session Initiation Protocol (SIP) fue desarrollado por la IETF (Internet Engineering Task Force) específicamente para telefonía IP, que a su vez toma ventaja de otros protocolos existentes para manejar parte del proceso de conversión, situación que no se aplica en H.323 ya que define sus propios protocolos bases.

8.6 El Estándar Voz sobre IP

Desde hace tiempo, los responsables de comunicaciones de las empresas tienen en mente la posibilidad de utilizar su infraestructura de datos, para el transporte del tráfico de voz interno de la empresa. No obstante, es la aparición de nuevos estándares, así como la mejora y abaratamiento de las tecnologías de compresión de voz, lo que está provocando finalmente su implantación.

Realmente la integración de la voz y los datos en una misma red es una idea antigua, pues desde hace tiempo han surgido soluciones desde distintos fabricantes que, mediante el uso de multiplexores, permiten utilizar las redes WAN de datos de las empresas (típicamente conexiones punto a punto y frame-relay) para la transmisión del tráfico de voz. La falta de estándares, así como el largo plazo de amortización de este tipo de soluciones no ha permitido una amplia implantación de las mismas.

Es innegable la implantación definitiva del protocolo IP desde los ámbitos empresariales a los domésticos y la aparición de un estándar, el VoIP (Voz

sobre IP), no podía hacerse esperar. La aparición del VoIP (Voz sobre IP) junto con el abaratamiento de los DSP's (Procesador Digital de Señal), los cuales son claves en la compresión y descompresión de la voz, son los elementos que han hecho posible el despegue de estas tecnologías. Para este auge existen otros factores, tales como la aparición de nuevas aplicaciones o la apuesta definitiva por VoIP (Voz sobre IP) de fabricantes como Cisco Systems o Nortel-Bay Networks. Por otro lado los operadores de telefonía están ofreciendo o piensan ofrecer en un futuro cercano, servicios IP de calidad a las empresas.

Por lo dicho hasta ahora, vemos que nos podemos encontrar con tres tipos de redes IP:

- Internet. El estado actual de la red no permite un uso profesional para el tráfico de voz.
- Red IP Pública. Los operadores ofrecen a las empresas la conectividad necesaria para interconectar sus redes de área local en lo que al tráfico IP se refiere. Se puede considerar como algo similar a Internet, pero con una mayor calidad de servicio y con importantes mejoras en seguridad. Hay operadores que incluso ofrecen garantías de bajo retardo y/o ancho de banda, lo que las hace muy interesante para el tráfico de voz.
- Intranet. La red IP implementada por la propia empresa. Suele constar de varias redes LAN (Ethernet conmutada, ATM, etc.) que se interconectan mediante redes WAN tipo Frame-Relay/ATM, líneas punto a punto, RDSI para el acceso remoto, etc. En este caso la empresa tiene bajo su control prácticamente todos los parámetros de la red, por lo que resulta ideal para su uso en el transporte de la voz.

A finales de 1997 el VoIP Forum del IMTC ha llegado a un acuerdo que permite la interoperabilidad de los distintos elementos que pueden integrarse en una red VoIP (Voz sobre IP). Debido a la ya existencia del estándar H.323 del ITU, que cubría la mayor parte de las necesidades para la integración de la voz, se decidió que el H.323 fuera la base del VoIP (Voz sobre IP). De este modo, el VoIP(Voz sobre IP) debe considerarse como una clarificación del H.323, de tal forma que en caso de conflicto, y a fin de evitar divergencias entre los estándares, se decidió que H.323 tendría prioridad sobre el VoIP (Voz sobre IP). El VoIP (Voz sobre IP) tiene como principal objetivo asegurar la interoperabilidad entre equipos de diferentes fabricantes, fijando aspectos tales

como la supresión de silencios, codificación de la voz y direccionamiento, estableciendo nuevos elementos para permitir la conectividad con la infraestructura telefónica tradicional. Estos elementos se refieren básicamente a los servicios de directorio y a la transmisión de señalización por tonos multifrecuencia (DTMF).

El VoIP/H.323 comprende a su vez una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación:

- Direccionamiento:

1. RAS (Registration, Admision and Status). Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través de el Gatekeeper.
2. DNS (Domain Name Service). Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS.

- Señalización:

1. Q.931 Señalización inicial de llamada.
2. H.225 Control de llamada: señalización, registro y admisión, y paquetización/ sincronización del stream (flujo) de voz.
3. H.245 Protocolo de control para especificar mensajes de apertura y cierre de canales para streams de voz.

- Compresión de voz:

1. Requeridos: G.711 y G.723.
2. Opcionales: G.728, G.729 y G.722.

- Transmisión de voz:

1. UDP. La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.
2. RTP (Real Time Protocol). Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

- Control de la transmisión:

1. RTCP (Real Time Control Protocol). Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.

<table>
<tr><td colspan="7">Establecimiento de llamada y Control</td></tr>
<tr><td colspan="2"></td><td colspan="4">Presentación</td></tr>
<tr><td colspan="2">Direccionamiento</td><td colspan="2">Compresión de audio G.711 ó G.723</td><td>DTMF</td><td></td><td>Direcciona-miento</td></tr>
<tr><td>RAS(H.225)</td><td>DNS</td><td colspan="2">RTP/RTCP</td><td>H.245</td><td>Q.931 (H.225)</td><td>DNS</td></tr>
<tr><td colspan="3">Transporte UDP</td><td colspan="4">Transporte TCP</td></tr>
<tr><td colspan="7">Red (IP)</td></tr>
<tr><td colspan="7">Enlace</td></tr>
<tr><td colspan="7">Físico</td></tr>
</table>

Pila de protocolos en VoIP (Voz sobre IP)

Hasta ahora hemos visto la posibilidad de utilizar nuestra red IP para conectar las centralitas a la misma, pero el hecho de que VoIP se apoye en un protocolo de nivel 3, como es IP, nos permite una flexibilidad en las configuraciones que en muchos casos está todavía por descubrir. Una idea que parece inmediata es que el papel tradicional de la centralita telefónica quedaría distribuido entre los distintos elementos de la red VoIP. En este escenario, tecnologías como CTI (computer-telephony integration) tendrán una implantación mucho más simple. Será el paso del tiempo y la imaginación de las personas involucradas en estos entornos, los que irán definiendo aplicaciones y servicios basados en VoIP.

Actualmente podemos partir de una serie de elementos ya disponibles en el mercado y que, según diferentes diseños, nos permitirán construir las aplicaciones VoIP. Estos elementos son:

Teléfonos IP.

Adaptadores para PC.

Hubs Telefónicos.

Gateways (pasarelas RTC / IP)

Gatekeeper.

Unidades de audioconferencia múltiple. (MCU Voz)

Servicios de Directorio.

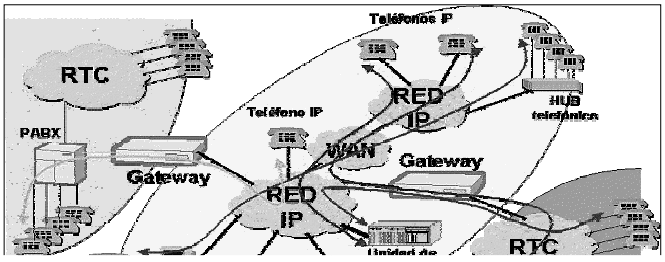


Figura 1.9.6.- Elementos de una red VoIP (Voz sobre IP)

Las funciones de los distintos elementos son fácilmente entendibles a la vista de la figura anterior, si bien merece la pena recalcar algunas ideas.

El Gatekeeper es un elemento opcional en la red, pero cuando está presente, todos los demás elementos que contacten dicha red deben hacer uso de él. Su función es la de gestión y control de los recursos de la red, de manera que no se produzcan situaciones de saturación de la misma.

El Gateway es un elemento esencial en la mayoría de las redes pues su misión es la de enlazar la red VoIP con la red telefónica analógica o RDSI. Podemos considerar al Gateway como una caja que por un lado tiene una interfase LAN y por el otro dispone de uno o varios de las siguientes interfaces:

FXO. Para conexión a extensiones de centralitas ó a la red telefónica básica.
FXS. Para conexión a enlaces de centralitas o a teléfonos analógicos.
E&M. Para conexión específica a centralitas.
BRI. Acceso básico RDSI (2B+D).
PRI. Acceso primario RDSI (30B+D).
G703/G.704. (E&M digital) Conexión especifica a centralitas a 2 Mbps.

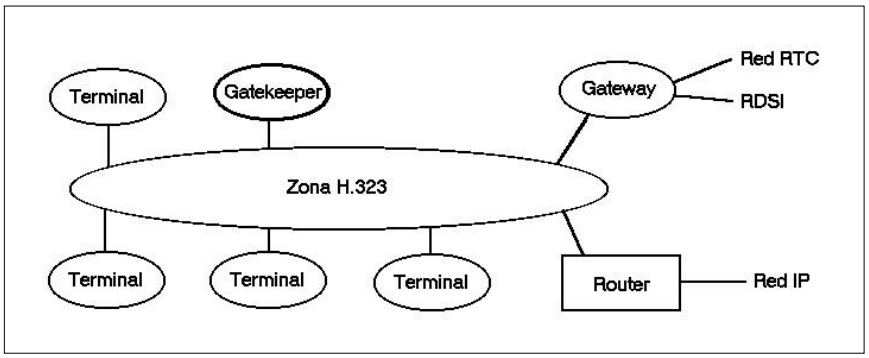
Un aspecto importante a resaltar es el de los retardos en la transmisión de la voz. Hay que tener en cuenta que la voz no es muy tolerante con estos. De hecho, si el retardo introducido por la red es más de 300 milisegundos, resulta casi imposible tener una conversación fluida. Debido a que las redes de área local no están preparadas en principio para este tipo de tráfico, el problema puede parecer grave. Hay que tener en cuenta que los paquetes IP son de longitud variable y el tráfico de datos suele ser a ráfagas. Para intentar obviar

situaciones en las que la voz se pierde porque tenemos una ráfaga de datos en la red, se ha ideado el protocolo RSVP, cuya principal función es trocear los paquetes de datos grandes y dar prioridad a los paquetes de voz cuando hay una congestión en un router. Si bien este protocolo ayudará considerablemente al tráfico multimedia por la red, hay que tener en cuenta que RSVP no garantiza una calidad de servicio como ocurre en redes avanzadas tales como ATM que proporcionan QoS de forma estándar.

8.7 Arquitectura de red

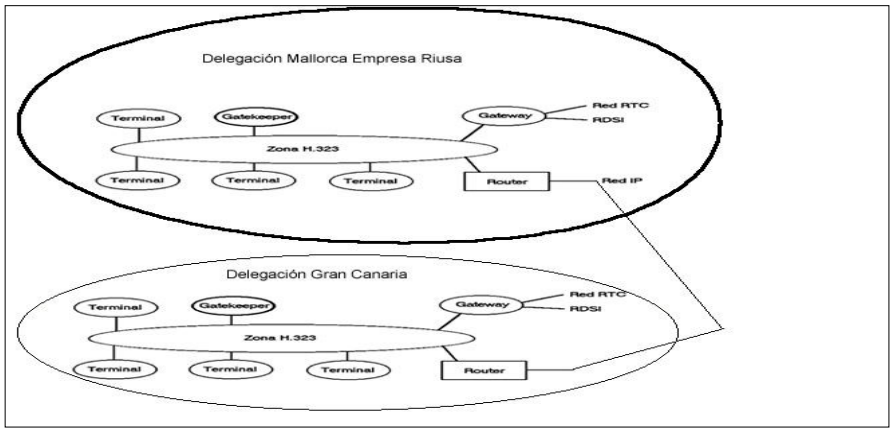
El propio estándar define tres elementos fundamentales en su estructura:

- Terminales: Son los sustitutos de los actuales teléfonos. Se pueden implementar tanto en software como en hardware.
- Gatekeepers: Son el centro de toda la organización VoIP, y serian el sustituto para las actuales centralitas. Normalmente implementadas en software, en caso de existir, todas las comunicaciones pasarían por él.
- Gateways: Se trata del enlace con la red telefónica tradicional, actuando de forma transparente para el usuario.



Con estos tres elementos la estructura de la red quedaría como muestra la figura.

El Gateway sirve de enlace entre la **RTC** /**RDSI** y la zona H.323 (VoIP). A su vez existe un Gatekeeper que realiza el control de llamadas y la gestión del sistema de direccionamiento. El router permitiría enlazar con otras redes H.323 sin necesidad de utilizar la RTC, resultando todas las llamadas a zonas H.323 totalmente gratuitas, con la ventaja de ahorro de costos que esto supone para las empresas.



La figura muestra la conexión entre dos delegaciones de una misma empresa conectadas mediante VoIP.

8.8 Calidad del Servicio (QoS)

Este es el principal problema que presenta hoy en día la implantación tanto de VoIP como de todas las aplicaciones de Xo**IP**. Garantizar la calidad de servicio sobre una red **IP**, en base a retardos y ancho de banda, actualmente no es posible, es por eso que se presentan diversos problemas en cuanto a garantizar la calidad del servicio.

- Anchos de Banda:

En la tabla adjunta se muestra la relación existente entre los distintos algoritmos de compresión de voz utilizados y el ancho de banda requerido por los mismos:

VoCodecs	Ancho de Banda (BW)
G.711 PCM	64 kbps
G.726 ADPCM	16, 24, 32, 40 kbps
G.727 E-ADPCM	16, 24, 32, 40 kbps
G.729 CS-ACELP	8 kbps

G.728 LD-CELP	16 kbps
G.723.1 CELP	6.3 / 5.3 kbps

Ancho de 4Banda requerido por los VoCodecs actuales

Retardo:

Una vez establecidos los retardos de tránsito y el retardo de procesado la conversación se considera aceptable por debajo de los 150 ms.

Calidad de servicio:

La calidad de servicio se está logrando en base a los siguientes criterios:

- La supresión de silencios, otorga más eficiencia a la hora de realizar una transmisión de voz, ya que se aprovecha mejor el ancho de banda.
- Compresión de cabeceras aplicando los estándares RTP/RTCP.
- Priorización de los paquetes que requieran menor latencia. Las tendencias actuales son: CQ (Custom Queuing). Asigna un porcentaje del ancho de banda disponible. PQ (Priority Queuing). Establece prioridad en las colas. WFQ (Weight Fair Queuing). Se asigna la prioridad al tráfico de menos carga. DiffServ: Evita tablas de encaminados intermedios y establece decisiones de rutas por paquete.
- La implantación de IPv6 que proporciona mayor espacio de direccionamiento y la posibilidad de tunneling.

8.9 Comparación Voz sobre IP y Telefonía Tradicional

Voz sobre IP es transmitir Voz utilizando IP. Si bien es una tecnología novedosa, tiene muchas características similares y otras diferentes a las de la telefonía tradicional.

Por eso, a continuación se explica brevemente el esquema de una red telefónica tradicional, y luego las coincidencias y diferencias con la tecnología de Voz sobre IP (Voz sobre IP).

Telefonía Tradicional

Arquitectura de una Central Telefónica

Las centrales telefónicas suelen estar diseñadas para tener una muy alta disponibilidad (se suele decir que son carrier class, dado que se dice están disponibles el 99.9% del tiempo, que representa alrededor de 5 minutos al año de interrupción de servicio).

Procesamiento de Llamadas

Hasta la central, la voz va en forma analógica. Actualmente ya no existen centrales analógicas, todo lo que hay desde que llega la señal a la central y sale de la otra central hacia el otro abonado, es digital.

La placa de abonado es la que se encarga de hacer la conversión de una señal analógica a una digital y viceversa. La señal se convierte a un PCM de 64kbps, que es una señal digital sin pérdida de información y sin compresión, es el formato que se está utilizando desde prácticamente sus comienzos. También es la placa de abonado la que decodifica los tonos de discado (DTMF). Es decir que, se utiliza el concepto de señalización en banda: comandar a la central utilizando la misma banda por la que se habla.

Conexión entre Centrales

La llamada que sale de nuestra central tiene que llegar hasta la central donde está la persona con la que queremos hablar. No hay doscientos millones de cables entre una y otra, sino que hay un enlace, el cual puede ser de diversos tipos. Este enlace se debe multiplexar para que todos los abonados de la central puedan hablar por teléfono.

Esta multiplexación es la que hace una diferencia a la hora de la calidad del servicio para el usuario. El sistema de multiplexación que utilizan las centrales telefónicas se llama TDM: Time Division Multiplex. Consiste en dividir el stream de datos en partes iguales de 64k (llamadas time-slots), de manera que los datos correspondientes al primer abonado van en el primer time-slot, los correspondientes al segundo en el segundo, y así sucesivamente.

Suponiendo un enlace de 2 Mbps de ancho de banda, como se transmiten 64k, podría haber hasta 32 abonados hablando a la vez. Con esta multiplexación en tiempo se separan y luego vuelven a unir los streams de voz que van de una central a otra, de manera transparente para el que lo está utilizando.

Lo bueno de esta tecnología es que como se divide por un tiempo fijo, se puede garantizar el time-slot y saber que siempre lo que corresponde al primer abonado va en el primer time-slot y así, está garantizado el ancho de banda necesario para poder hablar sin interrupciones.

Esto, en particular, es muy opuesto a lo que es IP, o cualquier enlace de paquetes en los que pueda haber colisiones, se pierdan paquetes, etc. Ya que en esos enlaces es muy difícil

garantizar que la calidad inicial se mantenga a lo largo de toda la conversación, puede pasar que haya paquetes que lleguen antes que otros, que se sature la conexión y muchos otros factores que afectan a la calidad final del audio.

En definitiva, TDM es una de las diferencias esenciales entre la telefonía común y la de Voz sobre IP, permite tener una red predictiva y garantizar calidad.

Ruteo, Señalización y Protocolos

Un tema importante es el "ruteo" entre centrales, es decir, como sabe la central del abonado con que central se tiene que conectar.

Vamos a denominar señalización a la información relacionada con una llamada que se transmite entre dos equipos. Podemos dividirla en dos grupos: la que refiere al abonado y las llamadas en sí, y otra parte entre las centrales .

A través de la señalización, la central puede ubicar a qué otra central tiene que llamar, a qué abonado dentro de esa central hay que llamar, saber que se cortó la comunicación, que dio ocupado, etc.

Las centrales entre sí se comunican utilizando diversos protocolos, los cuales generalmente son estándares públicos, aunque en muchos casos las especificaciones no son fáciles (o baratas) de conseguir. Los protocolos más comunes son tres: R2, PRI y SS7.

Se necesita que las dos centrales que se están queriendo comunicar puedan hablar un mismo protocolo, de manera que si se quieren intercomunicar dos centrales que no soportan los mismos protocolos, es necesario que utilicen una central intermedia que traduzca la información.

Acerca del enlace por el cual se pasa tanto la señalización como la voz en sí, existen muchísimos tipos. Los más conocidos y comunes son E1 o E3 (europeos), con sus variantes T1 o T3 (utilizadas principalmente en los Estados Unidos). Son cables de cobre, muy parecidos al cable coaxial, que pueden ser de 75 o 120 ohms. El E1 tiene 2Mbps (32 canales de 64kbps), el E3 tiene 32Mbps (512 canales de 64kbps).

Sin embargo, no se pueden ocupar todos los canales para pasar todos los abonados. En necesario poder avisar que hay llamadas y ese tipo de información. Por ejemplo, en el caso de una E1 se suelen utilizar 30 canales para el paso de la voz, 1 para framing (el 0) y 1 para señalización (el 15). En el de framing se suele encontrar (entre otras cosas) el CRC de los otros 31 (aunque depende de la configuración), de manera que si un determinado frame esta corrupto, se lo puede notar y actuar en consecuencia.

Para telefonía IP hay muchos protocolos. Los vamos a separar en 3 partes: codificación de la voz, transmisión de la voz y señalización.

Codificación de la Voz

La transmisión ya no se va a hacer en PCM, como en la telefonía tradicional. La voz se puede comprimir: si una persona se queda callada, por ejemplo, no es necesario transmitir el sonido completo del silencio. Hay muchos codecs de compresión. Como todo codec, cuanto más se comprime, más procesador se necesita. Hay codecs con pérdida que comprimen de 64k a 4k, incluso hasta 3.1k.

Señalización

Tal como vimos anteriormente, es necesario tener un protocolo para poder indicar a qué máquina se quiere llamar y demás. Existen actualmente varios protocolos para señalización.

El protocolo que más se está usando actualmente es SIP: Session Initiation Protocol. Se trata de un protocolo que tiene una característica muy particular: está estandarizado por la IETF (Internet Engineering Task Force) y, en consecuencia, es muy abierto y de fácil acceso.

SIP es un protocolo de texto plano que se utiliza sobre TCP, ya que en el caso de la señalización es importante que no se pierda la información. Tiene una arquitectura que está muy bien pensada, no trata de meter todo el mundo telefónico en IP, ni todo IP en el mundo telefónico.

Normalmente, cuando se usa SIP, el protocolo que se utiliza para enviar la voz es RTP (Real Time Protocol), que se usa sobre UDP.

No todos los sistemas utilizados por los Proveedores de Servicios de Telefonía por Internet son compatibles (Gateway, Gatekeeper) entre sí. Este ha sido uno de los motivos que ha impedido que la telefonía IP se haya extendido con mayor rapidez. Actualmente esto se está corrigiendo, y casi todos los sistemas están basados en el protocolo H.323. El estándar VoIP o protocolo fue definido en 1996 por la ITU (International Telecommunications Union) y proporciona a los diversos fabricantes una serie de normas con el fin de que puedan evolucionar en conjunto. Por su estructura el estándar proporciona las siguientes ventajas: Permite el control del tráfico de la red, por lo que se disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento de las redes de datos. Proporciona el enlace a la red telefónica tradicional. Al tratarse de una tecnología soportada en IP es independiente del tipo de red física que lo soporta. Permite la integración con las grandes redes de IP actuales. Es independiente del hardware utilizado. Y permite ser implementado tanto en software como en hardware, con la particularidad de que el hardware supondría eliminar el impacto inicial para el usuario común.

CAPITULO 9.- TELEFONIA IP

9.1 Introducción

La telefonía IP conjuga dos mundos históricamente separados: la transmisión de voz y la de datos. Se trata de transportar la voz, previamente convertida a datos, entre dos puntos distantes. Esto posibilitaría utilizar las redes de datos para efectuar las llamadas telefónicas, y yendo un poco más allá, desarrollar una única red que se encargue de cursar todo tipo de comunicación.

9.2 La Telefonía Local con IP

Los elementos necesarios para que se puedan realizar llamadas vocales a través de una red IP dependen en gran medida de qué terminal se utiliza en ambos extremos de la conversación. Estos pueden ser terminales IP o no IP.

Entre los primeros está el teléfono IP, un ordenador multimedia, un fax IP,...
Entre los segundos está un teléfono convencional, un fax convencional,...
Los primeros son capaces de entregar a su salida la conversación telefónica en formato de paquetes IP, además de ser parte de propia red IP, mientas que los segundos no, por lo que necesitan de un dispositivo intermedio que haga esto antes de conectarlos a la red IP de transporte.

Hay que señalar que en el caso de que uno o ambos extremos de la comunicación telefónica sean un terminal IP, es importante conocer de qué modo están conectados a Internet. Si es de forma permanente, se les puede llamar en cualquier momento. Si es de forma no permanente, por ejemplo, a través de un Proveedor de Acceso a Internet (PAI) vía módem, no se les puede llamar si en ese momento no están conectados a Internet.

9.3 Llamadas Teléfono a Teléfono

En este caso tanto el origen como el destino necesitan ponerse en contacto con un Gateway. Supongamos que el teléfono A descuelga y solicita efectuar una llamada a B. El Gateway de A solicita información al Gatekeeper sobre como alcanzar a B, y éste le responde con la dirección IP del Gateway que da servicio a B. Entonces el Gateway de A convierte la señal analógica del teléfono A en un caudal de paquetes IP que encamina hacia el Gateway de B, el cuál va regenerando la señal analógica a partir del caudal de paquetes IP que recibe con destino al teléfono B. El Gateway de B se encarga de enviar la señal analógica al teléfono B.

Por tanto tenemos una comunicación telefónica convencional entre el teléfono A y el Gateway que le da servicio (Gateway A), una comunicación de datos a través de una red IP, entre el Gateway A y el B, y una comunicación telefónica convencional entre el Gateway que da servicio al teléfono B (Gateway B), y éste. Es decir, dos llamadas telefónicas convencionales, y una comunicación IP. Si las dos primeras son metropolitanas, que es lo normal, el margen con respecto a una llamada telefónica convencional de larga distancia o internacional, es muy grande.

9.4 Llamadas de PC a Teléfono o Viceversa

En este caso sólo un extremo necesita ponerse en contacto con un Gateway. El PC debe contar con una aplicación que sea capaz de establecer y mantener una llamada telefónica. Supongamos que un ordenador A trata de llamar a un teléfono B. En primer lugar la aplicación telefónica de A ha de solicitar información al Gatekeeper, que le proporcionará la dirección IP del Gateway que da servicio a B. Entonces la aplicación telefónica de A establece una conexión de datos, a través de la Red IP, con el Gateway de B, el cuál va regenerando la señal analógica a partir del caudal de paquetes IP que recibe con destino al teléfono B. Fijaos como el Gateway de B se encarga de enviar la señal analógica al teléfono B.

Por tanto tenemos una comunicación de datos a través de una red IP, entre el ordenador A y el Gateway de B, y una comunicación telefónica convencional entre el Gateway que da servicio al teléfono B (Gateway B), y éste. Es decir, una llamada telefónica convencional, y una comunicación IP.

9.5 Llamadas PC a PC

En este caso la cosa cambia. Ambos ordenadores sólo necesitan tener instalada la misma aplicación encargada de gestionar la llamada telefónica, y estar conectados a la Red IP, Internet generalmente, para poder efectuar una llamada IP. Al fin y al cabo es como cualquier otra aplicación Internet, por ejemplo un chat.

CAPITULO 10.- ETHERNET Y GIGABYTE ETHERNET

10.1. Redes Ethernet

La cantidad de información que se maneja en las empresas modernas hace necesaria la implementación de sistemas que permitan compartir, modificar, almacenar y, en general, tratar de manera muy rápida y eficiente, todos los datos y archivos correspondientes a su propio funcionamiento.

Para llevar a cabo estas funciones se crearon las redes de computadoras. Estas se podrían clasificar en dos grupos principales: las redes WAN (Red de área amplia) y las redes LAN (Red de área local). Estas últimas se utilizan para interconectar computadoras, periféricos o estaciones de trabajo distribuidos en un edificio o entre un grupo cercano de edificios, con el propósito de compartir archivos, programas, impresoras, etc.

10.2. Historia

En 1973, Robert Metcalfe escribió una tesis para obtener el grado de PhD en el MIT (Instituto Tecnológico de Massachusets - USA), en la que describió la investigación que realizó acerca de las LAN. Posteriormente se trasladó a la compañía Xerox, donde formó un equipo de trabajo, junto con David Bogge y algunos otros colegas, para desarrollar la red Ethernet, basada en las ideas contenidas en su trabajo de tesis. Varias compañías la adoptaron con rapidez y posteriormente Intel fabricó un controlador para ella en un solo chip.No pasó mucho tiempo antes de que Ethernet se convirtiera en casi una norma para todas las LAN.

10.3. Topología de la red

Existen dos opciones para implementar una red Ethernet. La primera consiste en conectar todas los computadoras sobre el cable de la red directamente. Esta opción se conoce como topología tipo bus. La segunda consiste en utilizar un dispositivo llamado hub o concentrador, en el cual se conecta cada uno de los cables de red de las computadoras. Esta topología se conoce como hub. La figura 1.11.1 y 1.11.2 muestra como sería la conexión para cada caso.

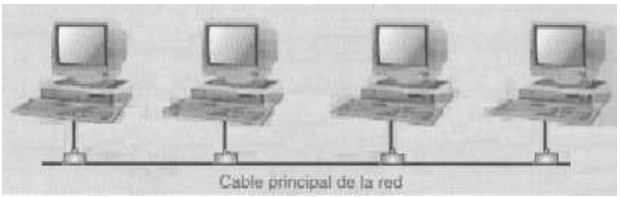


Figura 1.11.1.- bus

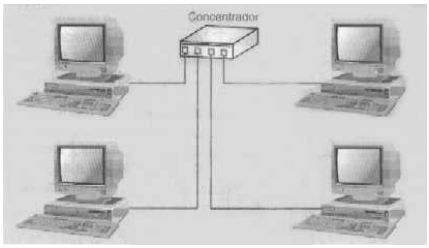


Figura 1.11.2 hub.

Un hub no realiza ningún tipo de conmutación, simplemente está compuesto por repetidores que retransmiten todas las señales recibidas por una computadora a las otras, en la misma forma de una red tipo bus, sin alterar de ninguna manera la información que circula a través de él. Estos dispositivos tienen además un conjunto de LED's que indica el estado de la conexión de los usuarios. Con el uso del hub se tiene la ventaja de aislar a un usuario que tenga problemas en el cable de conexión, de esta forma se evita que los otros usuarios sufran contratiempos. La figura 1.11.3 muestra un concentrador que se puede encontrar en el mercado.

Figura 1.11.3.- concentrador

Una red configurada como tipo hub puede conectarse a un bus o cable principal de red, ya que el concentrador además de las conexiones para los computadoras, tiene la posibilidad de conectarse a un cable coaxial, que podría ser el cable principal de un edificio. Esto permite que se incremente el número de usuarios. El ejemplo típico sería un ediñcio en el cual los usuarios de cada piso están conectados a un hub o concentrador. Los hub de todos los pisos están unidos entre sí por un bus o cable principal de la red.

Tarjeta de red Ethernet

Cada computador debe tener instalada una tarjeta de red, la cual incorpora los conectores necesarios para que el usuario pueda conectarse al canal. Existen tarjetas Ethernet de uno o

varios conectores. La figura 1.11. 4 muestra una tarjeta con conector para cable coaxial (conector BNC) y conector para cable UTP (conector RJ45).

Esta tarjeta se debe introducir en el interior del computador. Posee un microprocesador que se encarga de controlar todos los aspectos relacionados con la comunicación y otros como el empaquetamiento y desempaquetamiento de la información que se transmite y recibe, la codificación y decodificación, detección de errores, y en general todas las tareas necesarias para que el computador solamente se preocupe por entregarle la información que se desea transmitir y viceversa.

Figura 1.11.4

10.4 Cables y conectores que se utilizan.

En este tipo de redes se pueden utilizar el cable coaxial, cable UTP (par trenzado sin blindaje) y fibra óptica. El cable coaxial se emplea sobre todo en la configuración tipo bus (las computadoras se conectan entre sí, obviando el concentrador), banda base (baseband). El término banda base significa que el cable es alimentado por una sola fuente de voltaje. De esta forma el canal actúa como un mecanismo de transporte, a través del cual se propagan los pulsos digitales de voltaje.

Se utilizan dos tipos de cable coaxial: cable delgado (thin wire) de 0.25 pulgadas de diámetro y cable grueso (thick wire) de 0.5 pulgadas. Por lo general, los dos pueden operar a la misma velocidad, 10 Mbps (10 millones de bits por segundo), pero en el cable delgado se presenta una mayor atenuación. La máxima distancia en que se puede transmitir sin necesidad de amplificadores o repetidores es de 200 metros para el cable delgado y 500 para el grueso.

El cable coaxial delgado es mucho más flexible y utiliza conectores tipo BNC normales. Se puede conectar directamente a las tarjetas de red que hay en cada computadora. De esta forma se obtiene una cadena de computadoras conectadas al cable coaxial (topología tipo bus).

El cable grueso, por su naturaleza rígida, no puede llevarse hasta cada computadora. Por lo general, este cable se instala en canaletas o corredores. En este caso, se debe utilizar un dispositivo electrónico llamado transceiver, el cual se conecta al cable de red principal y de allí

se puede tomar una derivación hacia la computadora. El cable que se conecta entre la computadora y el transceiver tiene en sus extremos un aditamento llamado AUI (attachment unit interface), que le permite conectarse en ambos extremos.

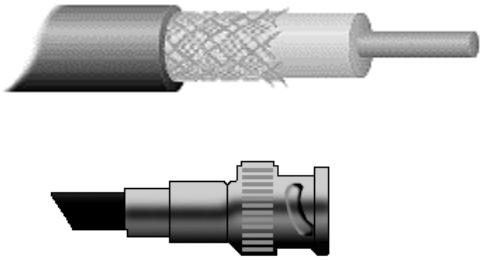


figura 1.11.5 : cable coaxial utilizado en las redes ethernet

figura 1.11.6 : conector bnc

El cable UTP o par trenzado sin blindaje, se utiliza generalmente en topologías hub/bus, para conectar las computadoras hasta el hub o concentrador. Su principal ventaja es la flexibilidad, que lo hace fácil de instalar en cualquier conducto o canaleta. La velocidad de transmisión que se puede lograr en este cable es de l00Mbps, utilizando tarjetas Fast Ethernet. Con el cable UTP se utilizan los conectores tipo RJ45, los cuales tienen el mismo aspecto de un conector para teléfono, pero con 8 hilos en lugar de 4. La figura 4 muestra los diferentes conectores que se pueden emplear.

Figura 1.11.7 : cable UTP utilizado en las redes ethernet.

Figura 1.11. 8: conector RJ45

La fibra óptica es el medio que permite obtener mayores velocidades. Como la información se transmite en forma de impulsos luminosos, se pueden obviar muchos problemas causados generalmente por interferencias electromagnéticas. Esto hace que se utilice principalmente para unir tramos largos de una red o dos redes diferentes separadas por una distancia considerable.

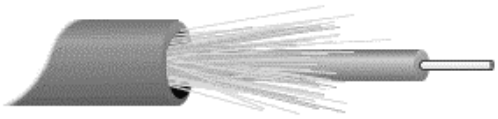


Figura 1.11.9 : fibra optica

A continuación describiremos el nombre técnico con que se denomina cada tipo de cable:

10Base2. Se denomina así a los tramos de cable coaxial delgado. Significa que puede operar a una velocidad de 10 Mbps, banda base y en una longitud de hasta 200 metros.

10Base5. Tramos de cable coaxial grueso. Opera a velocidad de 10 Mbps y cubre distancias hasta de 500 metros.

10BaseT. Emplea cable UTP. Permite operación a 100 Mbps en distancias de hasta 100 metros. Se emplea para conectar cada computadora al hub.

10BaseF. Se utiliza fibra óptica. La velocidad y la distancia aumentan considerablémente.

10.5 Transceiver.

Este dispositivo permite conectarse a los cables coaxiales de la red, ya sea para implementar una nueva rama de la red o una simple derivación para una sola computadora. Este aparato tiene un dispositivo tipo tornillo que penetra el interior del cable coaxial y hace contacto con el conductor central, sin necesidad de cortarlo; la parte exterior del tornillo hace contacto con el conductor exterior para garantizar de esta manera una buena conexión eléctrica. Normalmente, estos dispositivos pueden tener un conector AUI para hacer conexión con una computadora o con un concentrador, y uno tipo coaxial para conectarse al cable principal de red o simplemente generar otra rama de la misma.

El transceiver tiene internamente un circuito electrónico que le permite transmitir y recibir los datos a través del cable y proteger el cable principal contra fallas que se presenten en la computadora o la rama que está derivada de él. El cable que va del transceiver a la computadora tiene 5 pares de cable trenzado: uno para alimentar los circuitos del transceiver, dos para enviar y recibir datos y los otros dos para realizar funciones de control. Este cable tiene en cada extremo un conector AUI.

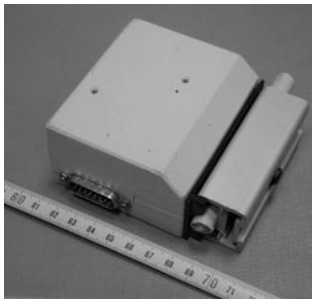


figura 1.11.10 : transceptor

figura 1.11.11 : conectores AUI

10.6. Transmisión de información en la red

Para garantizar que las computadoras conectadas en la red puedan comunicarse sin problemas, deben cumplir una serie de normas que se conocen generalmente con el nombre de protocolo. La red Ethernet utiliza un protocolo llamado CSMA/CD (Carrier Sense Multiple Access / Carrier Detect), que quiere decir: Acceso múltiple por detección de portadora con detección de colisión. A continuación haremos una breve descripción de su funcionamiento.

Como todas las computadoras están conectadas sobre el mismo bus, se dice que el cable opera en acceso múltiple. Esto significa que cuando una computadora quiere mandar información hacia otra computadora, debe colocar en el cable todo el paquete de información a ser transmitido. Dicho paquete incluye los datos sobre qué usuario los envía y qué usuario los recibe, además de la información en sí.

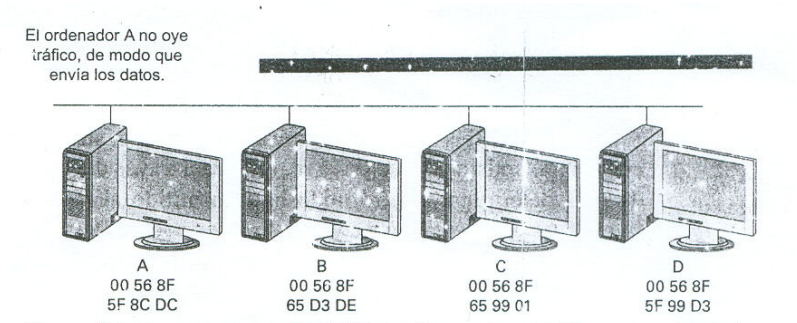


Figura 5.4. Un nodo en una red Ethernet escucha el tráfico antes de enviar un bastidor de datos.

figura 1.11.12.

Antes de iniciar, el equipo que va a transmitir debe "escuchar' el canal para saber que está libre (CS, detección de portadora) (figura 1..11.12). En caso de estar ocupado, debe esperar un tiempo y volver a intentarlo nuevamente. En caso de estar libre, puede empezar a transmitir los datos correspondientes.

Como se puede deducir, si dos computadoras "escuchan' el canal al mismo tiempo y éste se encuentra desocupado, empezarán a transmitir sus datos sobre el cable, lo que generará lo que se conoce con el nombre de colisión de información (figura 1.11.13). En este caso, las computadoras se retiran por un tiempo y luego cada una intenta nuevamente hacer su transmisión. Además, las computadoras que colisionaron colocan una señal en el cable de red que indica que se presentó un choque de datos o información.

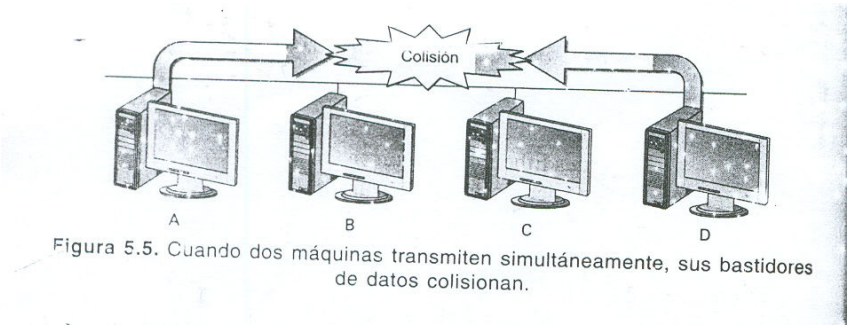


Figura 5.5. Cuando dos máquinas transmiten simultáneamente, sus bastidores de datos colisionan.

Figura 1.11.13 : colisión

Esta es una característica muy importante de este tipo de red, ya que cada computadora se retira del canal y no intenta por el contrario, seguir con su transmisión, lo que contribuye notablemente a reducir el tiempo de fallas en la línea. Las tarjetas de red y los transceiver tienen un circuito electrónico que se encarga de realizar las funciones que permiten “escuchar” el canal y detectar las colisiones.

10.7.- Formato de la Información

Los paquetes de información (también conocidos como tramas) que envía cada computadora por la red deben tener un formato específico y cumplir unas normas establecidas, para que sean comprendidas por todos los usuarios de la red. Esas normas cobijan aspectos como la longitud de los paquetes, polaridad o voltaje de los bits, códigos para detección de errores, etc.

En la figura 1.11.14 se muestra el formato de una trama o paquete de información. Cada trama empieza con un preámbulo de 7 bytes iguales (10101010). Esto genera una onda cuadrada de 10 MHz, durante un tiempo de 5.6 micro seg, con el objeto de que el receptor se sincronice con el reloj de transmisor. Después viene un byte llamado Inicio de trama (10101011), con el fin de marcar el comienzo de la información propiamente dicha.

figura 1.11.14

Los bytes correspondientes a la dirección de destino y de origen se utilizan para saber a quién va el mensaje y quién lo envía. Además, existe un carácter especial que puede indicar que el mensaje va dirigido a un grupo de usuarios o a todos los usuarios. El byte que indica la longitud del campo de datos indica al receptor cuantos bytes de información útil o verdadera debe esperar a continuación. Los datos corresponden al archivo en particular que se está enviando.

Los bytes de relleno se emplean para garantizar que la trama total tenga una longitud mínima de 64 bytes (sin contar el preámbulo ni el Inicio de trama), en caso de que el archivo de datos sea muy corto. Esto se hace con el fin de desechar las tramas muy cortas (menores de 64 bytes) que puedan aparecer en el cable de la red, como consecuencia de transmisiones abortadas por colisiones.

El código de redundancia sirve para hacer detección de errores. Si algunos bits de datos llegan al receptor erróneamente (por causa del ruido), es casi seguro que el código de redundancia será incorrecto y, por lo tanto, el error será detectado.

10.8 Gigabyte Ethernet

En marzo de 1996, el comité 802 de IEEE aprobó el proyecto estándar Gigabit Ethernet 802.3z. A la vez muchas 54 compañías expresaron el interes de participar en el proyecto de estandarización, la Alianza Gigabit Ethernet fue formada en mayo de 1996 por 11 compañías: 3Com, Bay Networks, Cisco Systems, Compaq Computer, Granite Systems, Intel Corporation, LSI Logic, Packet engines, Sun Microsystems Computer Company, UB Networks y VLSI Technology.

La alianza representa un esfuerzo de multi-vendor para proveer sistemas abiertos e inter-operables de productos Gigabit ethernet. Los objetivosde la alianza son:

- Ser una extensión de soporte para las redes existentes Ethernet y Fast Ethernet que requieren la demanda de un mayor ancho de banda.
- Proponer el desarrollo de técnicas para la inclusión en el estándar.
- Establecer pruebas de procedimientos y procesos de inter-operabilidad.

10.9 Capa Física

La capa física de Gigabit Ethernet esta formada por un mixto o híbrido entre las tecnología Ethernet y la Especificación de Canales por Fibra ANSI X3T11. Gigabit Ethernet es acepta finalmente 4 tipos de medios físicos, los cuales son definidos en 802.3z (1000Base-X) y 802.3ab (1000Base-T)

1000Base-X

En el estándar 1000Base-X la capa física es el Canal de Fibra. El Canal de Fibra es una tecnología de interconexión entre workstation, supercomputadoras, dispositivos de almacenamiento de información y perifericos. El Canal de Fibra tiene una arquitectura de 4 capas. La más baja tiene 2 capas FC-0 (Interfaz y Medio) y FC-1 (Codificador y Decodificador), estas son usadas en Gigabit Ethernet.
Hay 3 tipos de medios de trasmisión que son incluidos en el estándar 1000Base-X:

- 1000Base-SX: usa una fibra multi-modo, 850nm.
- 1000Base-LX: puede ser usada tanto mono-modo y multi-modo, 1300mn.
- 1000Base-CX: usa un cable par trenado de cobre (STP).

Distancias soportadas por los distintos tipos de cable:

Cable Type	Distance
Single-mode Fiber (9 micron)	3000 m using 1300 nm laser (LX)
Multi mode Fiber (62.5 micron)	300 m using 850 nm laser (SX) 550 m using 1300 nm laser (LX)
Multi mode Fiber (50 micron)	550 m using 850nm laser (SX) 550 m using 1300 nm laser (LX)
Short-haul Copper	25 m

100Base-T

El estándar 1000Base-T de Gigabit Ethernet emplea como medio de trasmisión un cable UTP, usando 4 pares de líneas de categoría 5 UTP.

10.10. Capa MAC

La capa MAC de Gigabit Ethernet usa el mismo protocolo de Ethernet CSMA/CD. La máxima longitud del cable usado para interconectar las estaciones está limitado por el protocolo CSMA/CD. Si 2 estaciones detectan el medio desocupado y comienzan la trasmisión ocurrirá una colisión.

Ethernet tiene una trama mínima de 64 bytes, la razón de tener un tamaño mínimo en la trama es para prever que las estaciones completen la trasmisión de una trama antes de que le primer bit sea detectado al final del cable, donde este puede chocar con otra trama. Sin embargo, el tiempo mínimo de detección de colisión es el tiempo que toma una señal en propagarse por desde un extremo a otro del cable. Este tiempo mínimo es llamado Slot Time or Time Slot, que es el número de bytes que pueden ser trasmitidos en un Time Slot, en Ethernet el Slot Time es de 64 bytes, la longitud mínima de trama).

La longitud máxima de un cable en Ethernet es de 2.5 Km (con un máximo de 4 repetidores). Como la tasa de bit se incrementa hace aumente la velocidad de transmisión. Como resultado, si el mismo tamaño de la trama y la longitud del cable se mantienen, entonces la estación puede también trasmitir una trama a gran velocidad y no detectar una colisión al final del otro cable. Entonces, una de las siguientes cosas se deben hacer: (i) Mantener una longitud máxima del cable e incrementar el time slot (y por eso, un tamaño mínimo en la trama) o (ii) Mantener un mismo time slot y decrementar la longitud del cable o ambos. En Fast Ethernet la longitud máxima del cable es reducida a 100 metros, dejando el tamaño de la trama en mínimo y el time slot intacto.

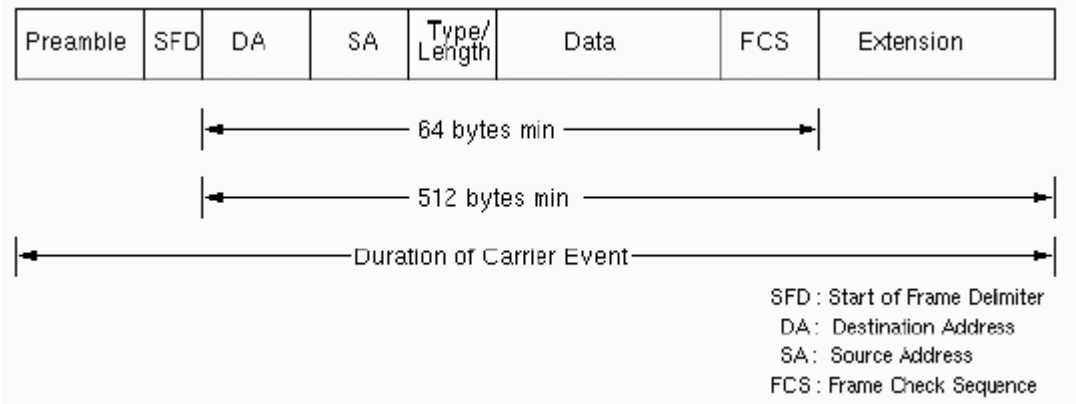
Gigabit Ethernet mantiene los tamaños mínimos y máximos de las tramas de Ethernet. Desde que Gigabit Ethernet es 10 veces más rápida que Fast Ethernet mantiene el mismo tamaño del slot, máxima longitud del cable deberá ser reducida a 10 metros, el cual no es muy usado. En lugar de ello, Gigabit Ethernet usa un gran tamaño del slot, siendo de 510 bytes. Para mantener la compatibilidad con Ethernet, el mínima tamaño de la trama no es incrementado, pero el "carrier event" es extendido. Si la trama es más corta que 512 bytes, entonces agregamos símbolos de extensiones. Hay símbolos especiales, los cuales no sucede en la carga útil o devalor.

10.11 Carrier Extension

Gigabit Ethernet deberá ser inter-operable con las redes existentes 802.3. Carrier Extension es una ruta del 802.3 que mantiene los tamaños de trama máximos y mínimos con distancias significativas de cableado. Para que el carrier sea extendido dentro de la trama, los símbolos de extensión de no-data son incluidos in la ventana de colisiones (collision window), que es, la

trama entera extendida considerada por la colisión y caída. Sin embargo, la secuencia de chequeo en la trama (FCS, siglas en ingles) es calculada solamente en la trama original (sin los símbolos de extensión). Los símbolos de extensión son removidos antes que el FCS sea chequeado por el receptor. Por lo que la capa LLC (control del Enlace Lógico) es ni siquiera avisado de la carrier extension.

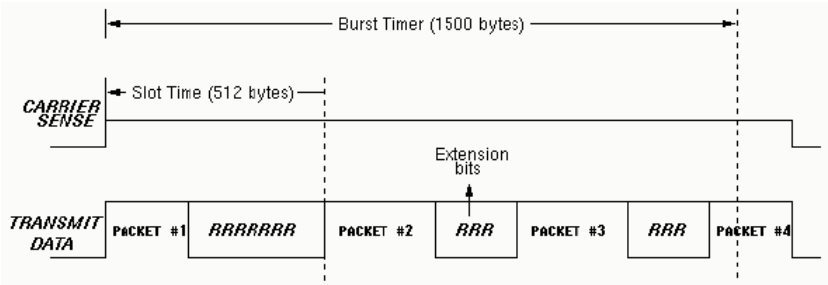
En la siguiente gráfica se muestra el formato de la trama Ethernet cuando el Carrier Extension es usado.



10.12. Packet Bursting

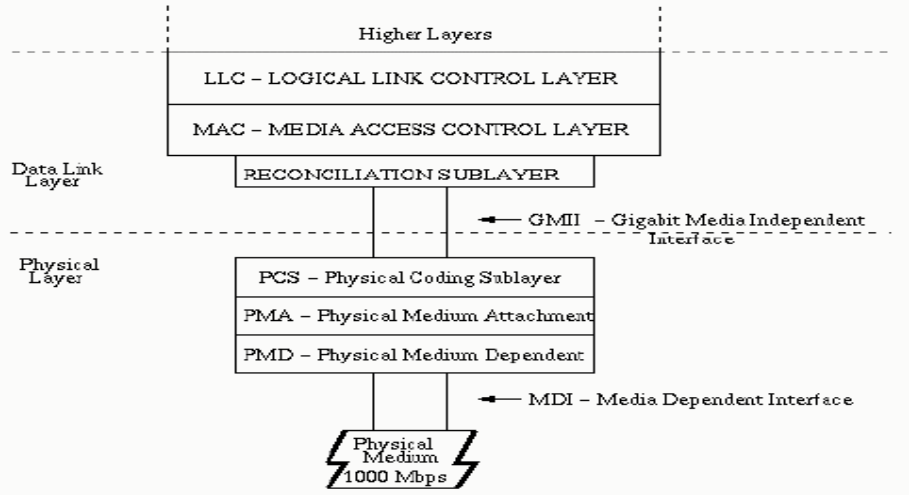
Carrier Extension es una solución simple, pero gasta un ancho de banda. 448 bytes de rellenos pueden ser enviados en pequeños paquetes.

Packet Bursting es una extensión de Carrier Extension. Packet Bursting es "Carrier Extension más unos paquetes agregados" (Brust). Cuando una estación tiene un número de paquetes a trasmitir, el primer paquete coloca al time slot si es necesario usando carrier extension. Los siguientes paquetes son trasmitidos unos detrás de otro, con el mínimo intervalo inter-packet (IPG, siglas en ingles inter-packet gap) hasta que finalice el tiempo de burst (de 1500 bytes). El Packet Bursting sustancialmente incrementa el troughput.
En la siguiente figura se muestra como trabaja el Packet Burst



Gigabit Interfase Independiente del Medio (GMII Gigabit Media Independent Interface) La GMII es la interfaz entre la capa MAC y la capa física. Esto permite que algunas de las capas físicas ser usada con la capa MAC. Existe una extensión de la MII (Media Independent Interface) usada en Fast Ethernet. Este usa la misma interfaz de gestion como MII. Este soporta trasmisión de datos de 10, 100 y 1000 Mbps. Posse separadamente un receptor de 8-bit de ancho y un trasmisor que agrega datos, tal que puede soportar opoeraciones como Full-Duplex y Half-Duplex.

Las diferentes capas de la arquitectura del protocolo Gigabit Ethernet se muestra en la figura siguiente:



La GMII posee 2 medios de señales del status: uno indica la presencia del carrier y el otro indica la ausencia de colisión. La sub-capa de reconciliación (RS, Reconciliation Sublayer, siglas en ingles) proyecta estas señales a señalización física (PLS, Physical Signalling, siglas en ingles) primitivas conocida por la sub-capa MAC existente. Con la GMII es posible conectar diferentes tipos de medios tales como cable UTP, fibra optica mono-modo y multi-modo, mientras se sigue usando el mismo controlador MAC. La GMII está dividida en 3 sub-capas: PCS, PMA, PMD.

PCS (Physical Coding Sublayer)

La PCS es la sub-capa de la capa GMII que provee una interfaz uniforme para la reconciliación de capas por todo el medio físico. Usa codigo 8B/10B empleado por canales de fibra. En estos tipos de códigos 8 bits están representados por 10 bits "grupos de códigos". Algunos grupos de códigos representas datos simbólicos de 8 bits. Otros son símbolos de control. Los símbolos de extensión usados en el Carrier Extension son un ejemplo de símbolos de control.

Las indicaciones de Carrier Sense y Collision Detec son generados por esta sub-capa. Esta sub-capa también maneja los procesos de auto negociación por el cual la arjeta de Red (NIC, siglas en Ingles) se comunica con la Red para determinar la velocidad de la misma (10, 100 o 1000 Mbps) y el modo de operación (half-duplex o full-duplex).

PMA (Physical Medium Attachment).

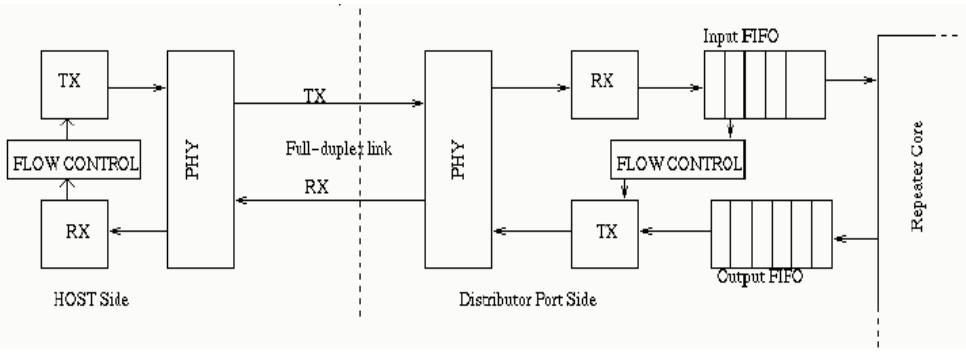
Esta sub-capa provista de un medio independiente por la sub-capa PCS para soportar diferentes medios físicos de bit-orientados serialmente. Esta capa forma grupos de códigos seriales por trasmisión y desambla los códigos de grupos seriales cuando los bits son recibidos.

PMD (Physical Medium Dependent).

Esta sub-capa proyecta el medio físico para la sub-capa PCS. Esta capa define la señalización de la capa físicas usada por diferentes medios. La MDI (Medium Dependent Interface, siglas eningles), la cual es parte de PMD es actualmente la interfaz de la capa física. Esta capa define la actual capa física de unión, como los conectores de los diferentes medios de trasmisión.

10.13.- Distribuidor de Buffer

Ethernet hoy en día soporta el medio Full-Duplex, la capa física como la capa MAC. Sin embargo, este todavía soporta operaciones Half-Duplex para mantener la compatibilidad. Existen nuevos dispositivo que poseen una funcionalidad como el HUB(concentreador), que posee un modo de operación Full-Duplex, tal dispositivo es llamado por distintos nombres como: Buffered Distributor, Full Duplex Repeater y Buffered Repeater.



El principio básico del CSMA/CD es usado como método de acceso a la red y no a un enlace. Un Buffered Distributor es un multi-puerto repetidor con enlaces Full-Duplex.

A continuación se muestra la arquitectura del Buffered Distributor:

Cada puerto tiene una entrada FIFO queue y una salida FIFO queue. Una trama llegando a una entrada queue es trasmitida a todas las salidas queues, excepto al puerto por donde está

entrando. Dentro del distribuidor el CSMA/CD arbitración se hace a las tramas de salida queues.
Las colisiones no pueden ocurrir a lo largo del enlace, la distancia restringida no es muy larga. La restricción en la longitud del cable es una característica del medio físico y no del protocolo CSMA/CD.
Como los envíos FIFO pueden crecer, el control de flujo basado en la trama es usado entre el puerto y la estación de envío.

Este es definido en el estándar 802.3x, el cual ya es usado en los switches Ethermet.

Lo que motiva a desarrollar los Buffered Distributor es el costocomparado con un Gigabit switch y no como una necesidad de acomodar el medio Half-Duplex. El Buffered Distributor provee una conectividad Full-Duplex.

10.14. Topologías

En esta sección se discuten diferentes topologías en el cual Gigabit Ethernet puede ser usado. Gigabit Ethernet es esencialmente un "campo de tecnología", que es para usar como un backnbone en una red de campo ancho, también puede ser usado entre routers, switches y concentradores o hub. Además puede ser usado para conectar servidores, servers farms y workstation de alto poder.

Esencialmente 4 tipos de hardware son necesarios para actualizar un red existente Ethernet/Fast Ethernet en una red Gigabit Ethernet:

Una tarjeta de interfaz Gigabit Ethernet (NICs)

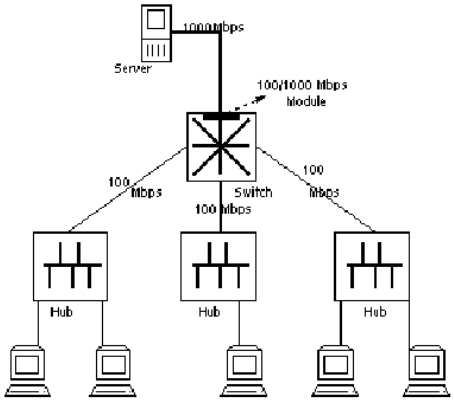
Agregar switches que conecten un número de segmentos Fast Ethernet a Gigabit Ethernet.

Switches Gigabit Ethernet.

Repetidores Gigabit Ethernet (Buffered Distributor)

Actualización en las conexiones server-switch

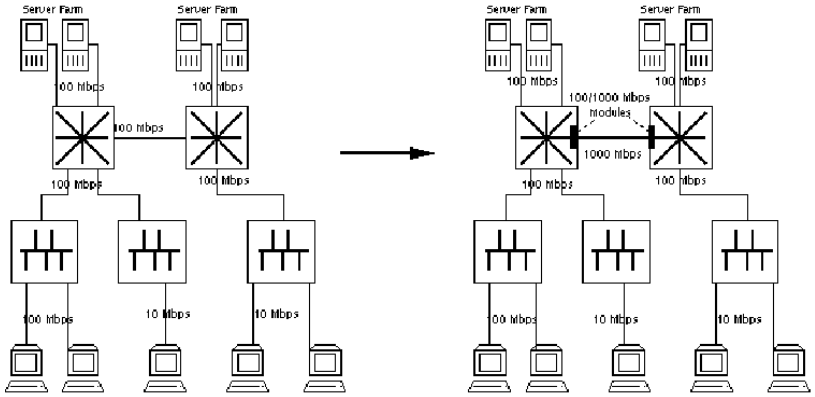
Las mejores redes tienen centralizada file server y compute server. Un servidor da respuestas a un número de clientes, lo cual hace que necesite mayor ancho de banda. Conectando servidores a switches con Gigabit Ethernet



Conexión Switch-Server

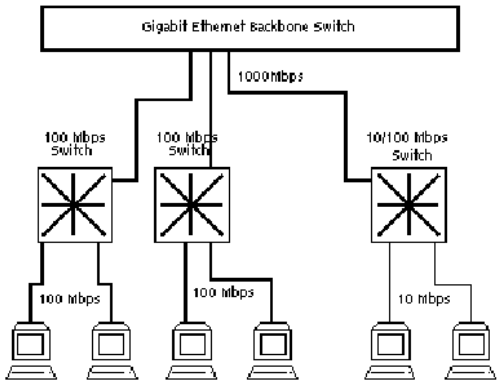
Actualización en las conexiones Switch-Switch

Otra actualización se encuentra en las conexiones entre los switches Fast Ethernet y los switches de 100/1000 de Gigabit Ethernet. Ver la figura a continuación:



Actualización del backbone Fast Ethernet

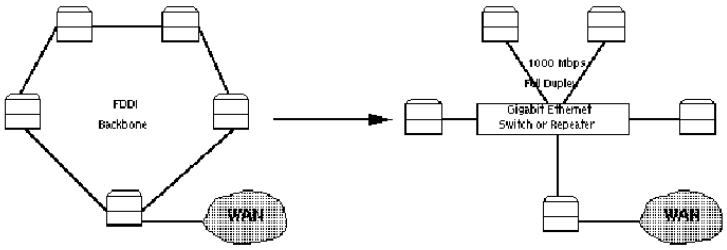
Un Backbone Fast Ethernet podemos encontrar multiples switches 10/100 Mbps. Este puede ser actualizado o sustituido por un switche Gigabit Ethernet siempre y cuando soporte multiples switches 100/1000 Mbps así como routers y concentradores o hubs que tienen interfaces Gigabit Ethernet. Una vez que el backbone ha sido actualizado, servidores de alto funcionamiento o arquitectura robusta pueden ser conectados directamente al backbone. Este incrementará el troughtput para aplicaciones que requieren mayor ancho de banda.



Actualización del backbone

Actualizando el backbone compartido del FDDI

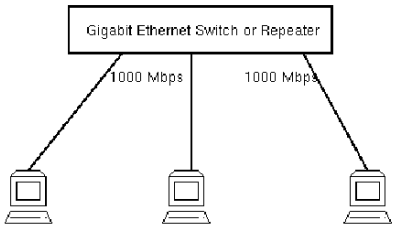
El FDDI es una estructura tecnológica de backbone. Un backbone FDDI puede actualizarse remplazando concentradores FDDI o routers Ethernet a FDDI por switches o repetidores Gigabit Ethernet.



Actualización de un backbone FDDI

Actualizando el alto funcionamiento de una estación de trabajo o Workstation

Las estaciones de trabajos son cada día más y más poderosas y necesitan conectarse a redes de grandes ancho de banda. Actualmente una Workstation pueden trasmitir por el bus más de 100 Mbps. Gigabit Ethernet puede ser conectado a estas estaciones de trabajo de altas velocidades.



Actualización para el alto funcionamiento de las estaciones de trabajo

CAPITULO 11.- DISPOSITIVOS DE RED

11.1. Concentradores

Un concentrador es un dispositivo que permite centralizar el cableado de una red. También conocido con el nombre de *hub*.

Nace a partir de un elemento de concentración de cableado, principalmente para redes del tipo CSMA/CD. Los primeros concentradores no eran mas que repetidores de señal. Esta primera función de los concentradores ya permitía a los administradores de la red dividirla en segmentos diferenciados mejorando la gestión de la misma aislando y controlando el trafico.

Un concentrador recibe conexiones de todos los equipos conectados al mismo, de manera que existe una linea física entre cada equipo y el concentrador. El concentrador tiene un elemento interna denominado plano posterior (backplane) , al que se conectan todas estas conexiones, formando efectivamente un bus para todos ellos.

Un concentrador funciona repitiendo cada paquete de datos en cada uno de los puertos con los que cuenta, excepto en el que ha recibido el paquete, de forma que todos los puntos tienen acceso a los datos. También se encarga de enviar una señal de choque a todos los puertos si detecta una colisión. Son la base para las redes de topología tipo estrella. Como alternativa existen los sistemas en los que los ordenadores están conectados en serie, es decir, a una línea que une varios o todos los ordenadores entre sí, antes de llegar al ordenador central. Llamado también repetidor multipuerto, existen 3 clases.

- Pasivo: No necesita energía eléctrica.
- Activo: Necesita alimentación.
- Inteligente: También llamados *smart hubs* son *hubs* activos que incluyen microprocesador.

Dentro del modelo OSI el concentrador opera a nivel de lacapa fisica, al igual que los repetidores, y puede ser implementado utilizando únicamente tecnología analógica. Simplemente une conexiones y no altera las tramas que le llegan.

Visto lo anterior podemos sacar las siguientes conclusiones:

1. El concentrador envía información a ordenadores que no están interesados. A este nivel sólo hay un destinatario de la información, pero para asegurarse de que la recibe el concentrador envía la información a todos los ordenadores que están conectados a él, así seguro que acierta.

2. Este tráfico añadido genera más probabilidades de colisión. Una colisión se produce cuando un ordenador quiere enviar información y emite de forma simultánea con otro ordenador que hace lo mismo. Al chocar los dos mensajes se pierden y es necesario retransmitir. Además, a medida que añadimos ordenadores a la red también aumentan las probabilidades de colisión.

3. Un concentrador funciona a la velocidad del dispositivo más lento de la red. Si observamos cómo funciona vemos que el concentrador no tiene capacidad de almacenar nada. Por lo tanto si un ordenador que emite a 100 megabit/segegundo le trasmitiera a otro de 10 megabit/segundo algo se perdería del mensaje. En el caso del ADSL los routers suelen funcionar a 10 megabit/segundo, si lo conectamos a nuestra red casera, toda la red funcionará a 10 megabit/segundo, aunque nuestras tarjetas sean 10/100 megabit/segundo

4. Un concentrador es un dispositivo simple, esto influye en dos características. El precio es barato. Un concentrador casi no añade ningún retardo a los mensajes.

Los concentradores fueron muy populares hasta que se abarataron los switch que tienen una función similar pero proporcionan más seguridad contra programas como los sniffer. La disponibilidad de switches ethernet de bajo precio ha dejado obsoletos, pero aún se pueden encontrar en instalaciones antiguas y en aplicaciones especializadas.

figura 1.12.1 : concentrador de 4 puertos

Los concentradores de cableado se clasifican dependiendo de la manera en que internamente realizan las conexiones y distribuyen los mensajes a esta característica se le llama topología logica ; existen dos tipos principales .

Concentradores con topología lógica bus (HUB): estos dispositivos hacen que la dred se comporte como un bus, enviando las señales que les llegan por todas las salidas conectadas.

Concentradores con topología lógica en anillo (MAU): estos por su parte, se comportan como si la red fuera un anillo, enviando la señal que les llega por un puerto al siguiente.

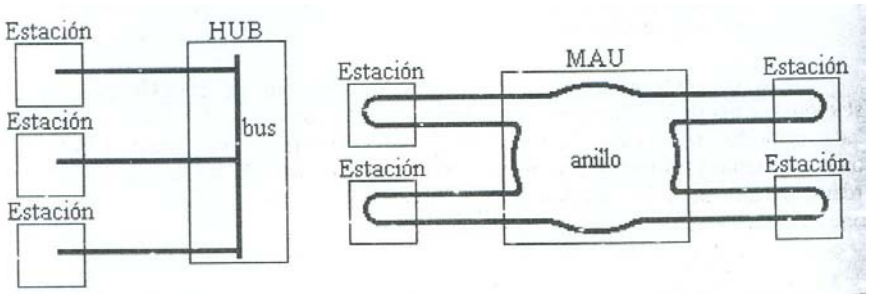


Figura 1.12.2 : topologías física y lógica de los concentradores. Vistos desde afuera, la red tiene siempre una topología física en estrella, pero, si se observan las conexiones internas de los concentradores, la red tiene una topología lógica diferente.

11.2. Repetidores

Un repetidor es un dispositivo que permite conectar dos segmentos de red. Esencialmente se trata de considerar dos segmentos de red como si fuese uno solo, salvando de esta forma las reswtricciones de distancias que establece el protocolo dado. Un repetidor coge las señales eléctricas entrantes, las convierte en código binario y después retransmite las señales eléctricas. Un repetidor no funciona como un amplificador. El amplificador potencia las señales, los defectos y todo, como una copiadora duplicando un mal original. Un repetidor, por su parte, recrea las, señales desde cero. Los repetidores resuelven la necesidad de un mayor alcance y mejoran la tolerancia a errores.

Aunque el uso de repetidores puede extender la longitud de la red hay que tener ciertas precauciones al utilizarlos. Un repetidor simplemente retransmite todo lo que recibe de manera que al extender la red se esta añadiendo a la misma todo el trafico de las dos partes, con lo que resultara mas fácil que ésta se sature. Asimismo el numero de repetidores que se pueden instalar es limitado.

Ventajas de los repetidores

Los repetidores tienen tres ventajas clave. Primera, amplían la distancia que puede cubrir una red. Segunda, proporcionan una medida de la tolerancia a errores, limitando el impacto de las roturas de cable al segmento en el que se produce la rotura. Tercera, pueden enlazar segmentos que usan diferentes tipos de cables Ethernet.

Un repetidor aumenta la distancia máxima posible entre máquinas enlazando juntos dos segmentos. Cada segmento conserva su propia limitación de distancia. Si un repetidor conecta dos segmentos IOBase2:, por ejemplo, la distancia máxima que puede separar dos máquinas

en segmentos diferentes es 2 x 185 = 370 metros Usando esta ecuación, dos segmentos 10Base5 conectados por un repetidor pueden cubrir 1000 metros (2 x 500 metros).

Los repetidores también añaden cierto grado de tolerancia a errores en una red. Si uno de los segmentos se rompe, sólo falla ese segmento. Los ordenadores del segmento adyacente siguen funcionando, sin verse afectados al comunicarse dentro de su propio segmento.

11.3. Token Ring

Token Ring, también conocida como IEEE 802.5, compitió directamente, al final sin éxito, con Ethernet como opción para conectar ordenadores de mesa a una LAN. Aunque Token Ring posee una cuota de mercado mucho menor que Ethernet, la base instalada de Token Ring ha permanecido extremadamente leal. Las redes Token Ring más comunes ofrecen mayor velocidad (16 Mbps) y eficiencia que Ethernet 10BaseT y la gente de Token Ring incluso ha establecido estándares Token Ring de 100 y 1000 Mbps.

Las redes Token Ring pueden parecerse mucho a las redes Ethemet 10BaseT, incluso usando cables UTP idénticos en algunos casos. Aunque estos dos tipos de redes comparten la misma topología estrella física, Token Ring utiliza una topología lógica anillo, en lugar de una topología. lógica bus.

11.3.1.- Topologia lógica anillo.

Las redes Token Ring usan una topología lógica anillo (fig 1). un nodo Token Ring se comunica directamente con sólo otras dos máquinas: sus vecinas corriente arriba y corriente abajo . Para controlar el acceso al anillo. Token Ring emplea un sistema de paso de señal.

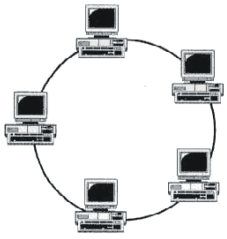


figura 1.- las redes token ring usan una topología lógica anillo

11.3.2.- Paso de señal

La piedra angular del paso de señales es un bastidor especial llamado la señal (fig. 2). Este bastidor permite a los sistemas de una red Token Ring en efecto "coger turnos" para enviar datos. La regla es que ningún dispositivo puede transmitir datos a menos que tenga en este momento la señal.

Un bastidor Token Ring empieza con la propia señal, pero por lo demás contiene prácticamente la misma información que un bastidor Ethernet: la dirección MAC de origen, la dirección MAC de destino, los datos a transmitir y una secuencia de comprobación de bastidor (FCS) que se usa para comprobar que no hay errores en los datos

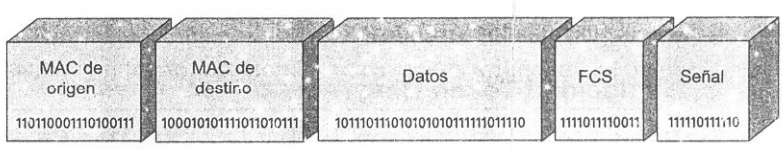


figura 2 .- un bastidor token ring

Cuando recibe un bastidor, un nodo Token Ring comprueba la dirección MAC de destino para determinar si debe procesar los datos que contiene o enviar el bastidor a su vecino corriente abajo. Cuando el destinatario deseado procesa los datos, crea un nuevo bastidor que incluye un código especial indicando que el bastidor fue recibido correctamente. El nodo receptor envía entonces este bastidor hacia el nodo emisor. Cuando el nodo emisor obtiene el bastidor con el codigo "recibido en buen estado", quita el bastidor del cable y envía una nueva señal libre: este es un nuevo bastidor que contiene sólo la señal.

La señal libre dice a cualquier nodo que la recibe que el anillo está disponible. Un nodo con datos que enviar debe esperar hasta que recibe la señal libre; crea entonces un bastidor de datos, que incluye una señal, y envía el nuevo bastidor a su vecino corriente abajo. Una vez más, cuando el nodo emisor recibe la confirmación de que el receptor pretendido recibió el bastidor genera una nueva señal libre, dando a la siguiente maquina de la cola acceso al anillo.

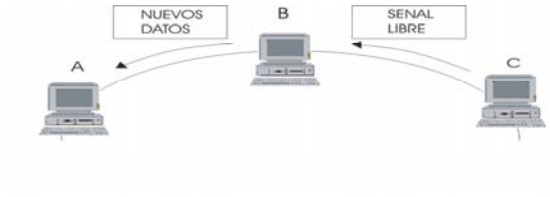


FIG 3.- después de recibir una señal libre, el nodo A puede enviar nuevos datos a su vecino corriente abajo.

Una red de paso de señal envía bastidores de datos de forma más eficiente que una red que usa CSMA/CD porque no se dan colisiones. Una estación puede tener que esperar a una señal libre para poder enviar datos, pero si tiene la señal sabe que ninguna otra estación intentará enviar datos al mismo tiempo. Por su parte, una red basada en CSMA/CD, como Ethernet, puede desperdiciar un ancho de banda significativo resolviendo colisiones. El paso de señal es un método determinista para resolver qué máquina debe tener acceso al cable en un momento dado. Determinista significa que el cable se concede de forma predecible, en lugar de con un proceso aleatorio como CSMA/CD.

Las redes Token Ring pueden ir a 4 ó 16 Mbps, velocidades que parecen lentas comparadas con los 10 Y 100 Mbps de los estándares Ethernet (las nuevas versiones de Token Ring mejoran estas velocidades). Los puros números, sin embargo, no cuentan toda la historia. Las redes Token Ring usan todos los bits de su ancho de banda para enviar datos. Las redes Etbernet, por el contrario, desperdician significativas cantidades de ancho de banda resolviendo colisiones. La velocidad a la que opera el anillo depende del dispositivo mas lento del anillo. Una red token ring que consista en cinco nodos token ring 4/16 Mbps y un nodo token ring a 4 Mbps irá a 4 Mbps.

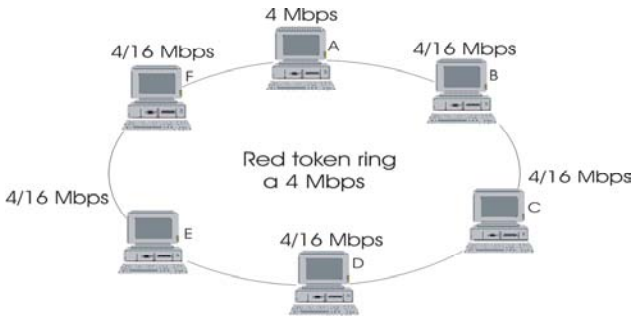


Figura 4.- el dispositivo más lento en el anillo determina la velocidad de todo el anillo.

Las redes Token Riag pueden configurarse para dar a algunos sistemas mayor prioridad de acceso a la señal. Es concebible que un arquitecto de redes establezca una prioridad alta para un PC determinado, garantizando que tendrá acceso a la señal más a menudo que los otros nodos de la red. Las redes Token Ring reales raramente aprovechan esta capacidad de priorizar el tráfico, haciendo que esa característica sea menos útil de lo que pudiera parecer.

11.3.3.- Estrella física.

La topología física anillo comparte la misma vulnerabilidad a la rotura del cable que la topología física bus. Cuando el cable usado en una topología física bus como l0Base2 se rompe, toda la red se va abajo debido a las reflexiones eléctricas. Una topología física anillo también falla

completamente si se rompe el cable, pero por una razón distinta. En una topología anillo, todo el Tráfico viaja en una dirección.

Si el anillo se rompe, el tráfico nunca puede completar el viaje en redondo alrededor de la red, de modo que ,ningún nodo genera una señal libre .Para evitar los problemas inherentes a una topología física anillo. Token Ring usa una topología física estrella.

Figura 5 : topología en anillo

Token Ring oculta el anillo lógico dentro de un concentrador, conocido como Unidad de acceso multiestación (MAU), Los nodos individuales se conectan al concentrador a través de cables par trenzado sin blindar (UTP) o par trenzado blindado STP.

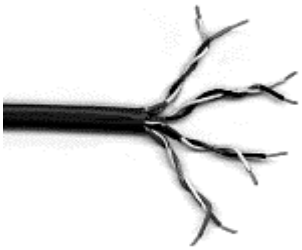


Figura 6: cable UTP

11.3.4. Token Ring sobre STP

Originalmente, las redes Token Ring usaban una versión muy blindada del cable par trenzado conocida como par trenzado blindado (STP). STP consiste en dos pares de alambres de cobre rodeados por una camisa de metal. La camisa de metal de STP sirve a la misma función que el blindaje usado en cables coaxiales: impedir que la interferencia eléctrica afecte a los alambres usados para enviar señales. Cuando se usa STP, un solo MAU Token Ring puede admitir hasta 260 ordenadores. El cable STP que conecta un ordenador con el concentrador no puede ser más largo de 100 metros. Aunque el blindaje pesado del cable STP]o convierte en la opción ideal para entornos con niveles altos de interferencia eléctrica, el alto coste de ese blindaje hace que sea caro para la mayoría de las instalaciones.

Token Ring usa un conector especial Tipo 1 para STP .Los conectores Token Ring Tipo 1 no son RJ-45. En su lugar, IBM diseñó un conector hermafrodita exclusivo llamado Conector de datos tipo IBM (IDC) o Conector de datos universal (UDC). Estos conectores no son machos ni hembras; están diseñados para enchufarse uno en otro. Las tarjetas de red Token Ring usan un conector hembra de nueve agujas y un cable Token Ring estándar tiene un conector hermafrodita en un extremo y un conector macho de nueve agujas en el otro.

11.3.5. Conectar MAU

Conectar varios concentradores Token Ring para formar una red mas grande requiere que se extienda el anillo. Los MAU Token ring tienen dos puertos especiales , etiquetados Ring in y Ring out. Estas conexiones especiales pueden enlazar varios MAU para formar un solo anillo. El puerto ring in en el primer MAU debe conectarse con el puerto ring out del segundo MAU , y viceversa para formar un solo anillo lógico.. Lógicamente los dos MAU parecen el mismo anilloo a los dispositivos acoplados a ellos (figura 8). Se pueden combinar hasta 33 MAU requiere el uso de puentes y enrutadores.

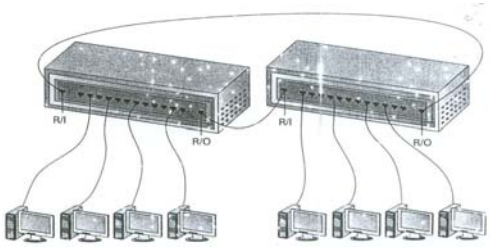


figura 8.- Cuando se vinculan correctamente , los dos MAU forman un solo anillo lógico.

11.4. Puentes (Bridge)

11.4.1 Descripción

Según crece la demanda de anchura de banda en la red el numero de maquinas que pueden coexistir pacíficamente dentro de un dominio colisión ethernet se contrae. Un dispositivo especial, llamado puente, pude enlazar juntos segmentos ethernet para formar redes más grandes, los puentes no solo conectan segmentos, también filtran él trafico entre los segmentos ahorrando preciosa anchura de banda.

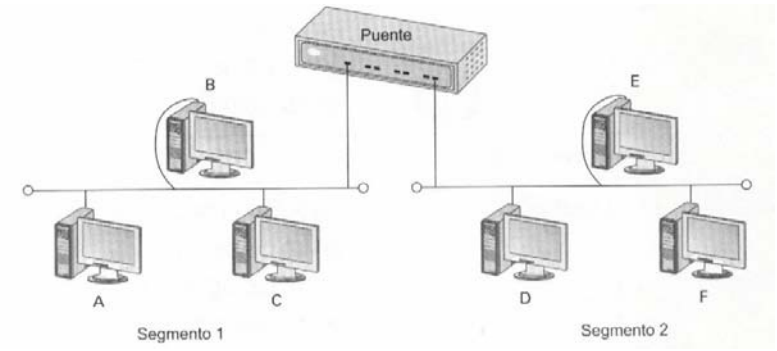
Los puentes filtran y reenvían él trafico entre dos o más redes basándose en las direcciones MAC contenidas en los bastidores o tramas de datos. Filtrar él trafico significa impedir que cruce de una red a la siguiente, reenviar él trafico significa hacer pasar él trafico originado en un lado del puente hasta el otro lado.

En la siguiente figura se muestra dos segmentos ethernet conectados por un puente. El puente se representa aquí como una simple caja, pues la verdadera apariencia física de un puente puede variar mucho. El puente puede ser un dispositivo independiente parecido a un repetidor ethernet o a un concentrador o puede ser un PC con dos NIC que ejecutan un software de puente especial.

El puente incluso puede estar integrado en un dispositivo multifunción que proporcione otras funciones además de actuar como puente. No importa su apariencia todos los puentes realizan la misma función: filtrar y reenviar él trafico de red inspeccionando las direcciones MAC de cada bastidor que llega al puente.

MAC (médium access control, control de acceso al medio) y se utilizan para conectar o extender redes similares, es decir redes que tienen protocolos idénticos, (como es token ring con token ring, ethernet con ethernet, etc.) y conexiones a redes de área extensa.

Dos segmentos ethernet conectados por un puente.



11.4.2 Modo de Operación

Un puente ethernet recién instalado se comporta inicialmente exactamente igual que un repetidor, pasando bastidores de un lado a otro. Pero la diferencia es que, un puente controla y registra él trafico de red llegando por fin a un punto en el que pueda empezar a filtrar y a reenviar.

Esto hace que el puente sea más inteligente que un repetidor. El tiempo que tarda un nuevo puente en reunir información suficiente para empezar a filtrar y reenviar suele ser solo de unos segundos. Veamos un punte en acción.

En la figura de arriba, la maquina A envía un bastidor a la maquina D cuando el bastidor designado a la maquina D llega al puente, este no conoce la ubicación de la maquina D,

por lo que reenvía el bastidor al segmento 2, en este punto, el puente empieza a construir una lista de direcciones MAC incluyendo el segmento del que proceden.

Al reenviar el paquete a la maquina D, el puente registra que recibió un bastidor desde la dirección MAC de la maquina A en el segmento 1. Ahora que el puente conoce la ubicación de al menos una maquina, puede empezar a filtrar, al final, cada maquina habrá enviado por lo menos algunos bastidores y el puente tendrá una lista completa con la dirección MAC y ubicación de cada maquina. Para el ejemplo usado aquí, la tabla siguiente (la lista de un puente de verdad no tendrá las letras de maquina las incluimos aquí solo como descripción.)

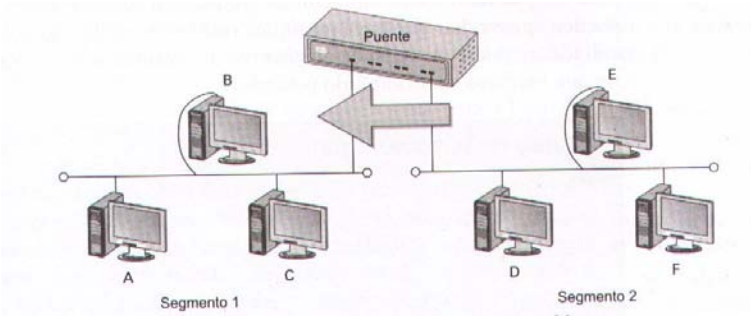
TABLA

Lista de direcciones MAC en un puente.

Segmento 1	
Máquina	**Dirección MAC**
A	00 45 5D 32 5E 72
B	9F 16 C6 55 4D EE
C	9F 16 C6 99 DF F1
Segmento 2	
Máquina	**Dirección MAC**
D	9F 16 C6 85 E5 55
E	9F 16 C6 DD 41 11
F	00 45 5D 00 25 19

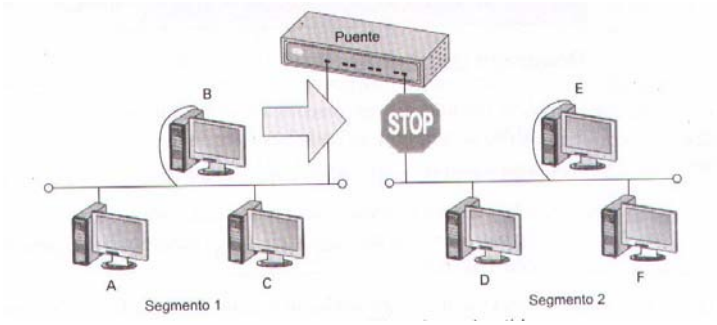
Una vez que el puente tiene la tabla completa con la dirección MAC de cada maquina y el lado del puente en el que se encuentra, mira cada bastidor entrante y decide si reenviarlo o no al otro lado. Supongamos que la maquina A decide enviar otro bastidor a la maquina D. cuando la maquina D responde a la maquina A, el puente reenvía el bastidor al segmento 1 porque sabe que la maquina A reside en el segmento 1 .

Puente reenviando un bastidor.



Si la maquina C envía un bastidor a la maquina A, la maquina B recibirá también ese bastidor porque todas residen en el mismo segmento, sin embargo, el puente reconoce que ninguna maquina del segmento 2 necesita ver el bastidor, que sé esta enviando desde la maquina C a la maquina A en el segmento 1 filtra este bastidor en consecuencia

Puente filtrando un bastidor



Las maquinas de cada lado pueden ser perfectamente felices sin tener noticias de la presencia del puente, cuando un puente reenvía un bastidor copia ese bastidor exactamente, incluso usando la dirección MAC de la maquina remitente como dirección MAC de origen en la nueva copia del bastidor, añadir un puente a una red no requiere de que se configuren los otros nodos de la red simplemente se conectan los cables y el puente se ocupa del resto.

Como los puentes reenvían bastidores de datos sin cambiar los propios bastidores, el formato de bastidor utilizado a cada lado del puente debe ser el mismo los puentes filtran cierto trafico innecesario, ahorrando precioso ancho de banda aumentan el ancho de banda disponible en una red filtrando él trafico pero los puentes tienen limitaciones, no pueden conectar redes distintas y no pueden aprovechar que hay múltiples rutas entre nodos, resolver esas dificultades requiere otro tipo de dispositivo: Un Ruteador o Switch.

11.4.3 Tipos de Puentes

- Locales: sirven para enlazar directamente dos redes físicamente cercanas.
- Remotos o de área extensa: se conectan en parejas, enlazando dos o más redes locales, formando una red de área extensa, a través de líneas telefónicas.

Se puede realizar otra división de los *bridges* en función de la técnica de filtrado y envío *(bridging)* que utilicen:

- *Spanning Tree Protocol Bridge o Transparent Protocol Bridge* (Protocolo de Arbol en Expansión o Transparente, STP).

Estos *bridges* deciden qué paquetes se filtran en función de un conjunto de tablas de direcciones almacenadas internamente. Su objetivo es evitar la formación de lazos entre las redes que interconecta. Se emplea normalmente en entornos Ethernet.

- *Source Routing Protocol Bridge* (*Bridge* de Protocolo de Encaminamiento por Emisor, SRP).

El emisor ha de indicar al bridge cuál es el camino a recorrer por el paquete que quiere enviar. Se utiliza normalmente en entornos TokenRing.

- *Source Routing Transparent Protocol Bridge* (*Bridge* de Protocolo de Encaminamiento por Emisor Transparente, SRTP). Este tipo de *bridges* pueden funcionar en cualquiera de las técnicas anteriores.

11.4.4 Ventajas y Desventajas de los Puentes

Ventajas de la utilización de *bridges*:

- Fiabilidad. Utilizando *bridges* se segmentan las redes de forma que un fallo sólo imposibilita las comunicaciones en un segmento.
- Eficiencia. Segmentando una red se limita el tráfico por segmento, no influyendo el tráfico de un segmento en el de otro.
- Seguridad. Creando diferentes segmentos de red se pueden definir distintos niveles de seguridad para acceder a cada uno de ellos, siendo no visible por un segmento la información que circula por otro.
- Dispersión. Cuando la conexión mediante repetidores no es posible debido a la excesiva distancia de separación, los *bridges* permiten romper esa barrera de distancias.

Desventajas de los *bridges*:

- Son ineficientes en grandes interconexiones de redes, debido a la gran cantidad de tráfico administrativo que se genera.

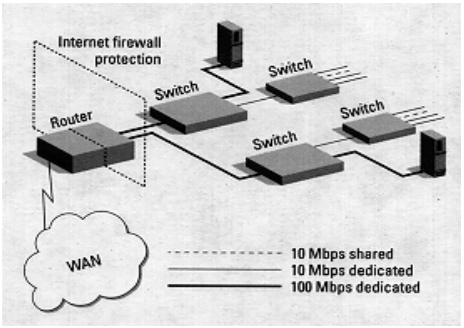
- Pueden surgir problemas de temporización cuando se encadenan varios *bridges*.
- Pueden aparecer problemas de saturación de las redes por tráfico de difusión.

Las aplicaciones de los *bridges* están en soluciones de interconexión de RALs similares dentro de una interconexión de redes de tamaño pequeño-medio, creando una única red lógica y obteniendo facilidad de instalación, mantenimiento y transparencia a los protocolos de niveles superiores. También son útiles en conexiones que requieran funciones de filtrado. Cuando se quiera interconectar pequeñas redes.

11.5 Ruteador (ROUTER)

11.5.1 Definición (conceptos generales)

Un ruteador es un dispositivo de *proposito general* diseñado para segmentar la red, con la idea de limitar tráfico de brodcast y proporcionar seguridad, control y redundancia entre dominios individuales de brodcast, también puede dar servicio de firewall y un acceso económico a una WAN.



El ruteador opera en la capa 3 del modelo OSI y tiene más facilidades de software que un switch. Al funcionar en una capa mayor que la del switch, el ruteador distinge entre los diferentes protocolos de red, tales como IP, IPX, AppleTalk o DECnet. Esto le permite hacer una decisión más inteligente que al switch, al momento de reenviar los paquetes.

11.5.2 Funcion de un Ruteador

El ruteador realiza s funciones basicas:El ruteador es responsable e crear y mantener tablas de ruteo para cada capa de protocolo de red, estas tablas son creadas ya sea estáticamente o dinámicamente.

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

La inteligencia de un rutedor permite seleccionar la mejor ruta, basandose sobre diversos factores, más que por la direccion MAC destino. Estos factores pueden incluir la cuenta de saltos, velocidad de la linea, costo de transmisión, retrazo y condiciones de tráfico. La desventaja es que el proceso adicional de procesado de frames por un ruteador puede incrementar el tiempo de espera o reducir el desempeño del ruteador cuando se compara con una simple arquitectura de switch.

Las funciones primarias de un ruteador son:

-Segmentar la red dentro de dominios individuales de brodcast.

-Suministrar un envio inteligente de paquetes. Y

-Soportar rutas redundantes en la red.

-Aislar el tráfico de la red ayuda a diagnosticar problemas, puesto que cada puerto del ruteador es una subred separada, el tráfico de los brodcast no pasaran a través del ruteador.

Otros importantes beneficios del ruteador son:

-Proporcionar seguridad a través de sotisficados filtros de paquetes, en ambiente LAN y WAN.

-Consolidar el legado de las redes de mainframe IBM, con redes basadas en PCs a través del uso de Data Link Switching (DLSw).

-Permitir diseñar redes jerarquicas, que delegen autoridad y puedan forzar el manejo local de regiones separadas de redes internas.

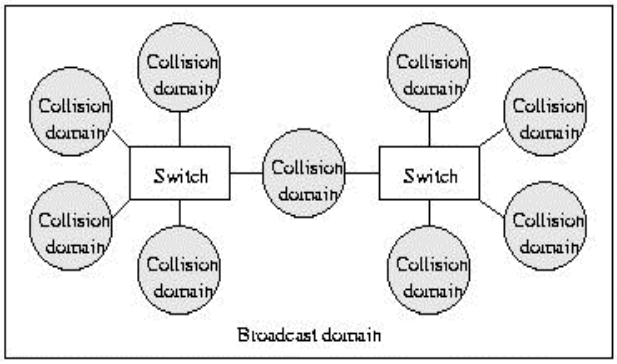
-Integrar diferentes tecnologías de enlace de datos, tales como Ethernet, Fast Ethernet, Token Ring, FDDI y ATM.

11.5.3 Aplicación de un Ruteador

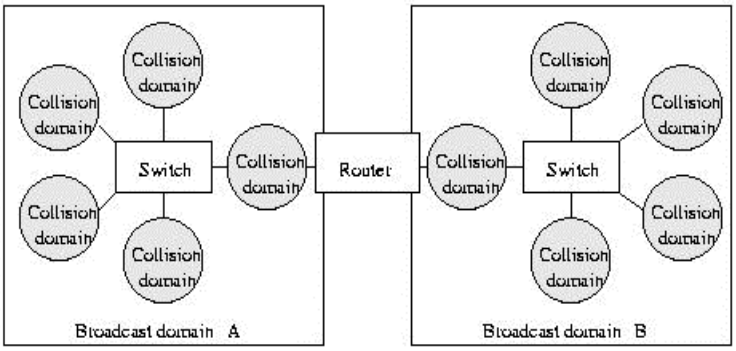
Segmentando Subredes con Ruteadores.

Una subred es un puente o un switch compuesto de dominios de broadcast con dominios individuales de colisión. Un ruteador esta diseñado para interconectar y definir los limites de los dominios de broadcast.

La figura muestra un dominio de broadcast que se segmento en dos dominios de colisiones por un switch, aquí el tráfico de broadcast originado en un dominio es reenviado al otro dominio.



En la siguiente figura muestra la misma red, después que fué segmentada con un ruteador en dos dominios diferentes de broadcast. En este medio el tráfico generado de broadcast no fluye a través del ruteador al otro dominio.

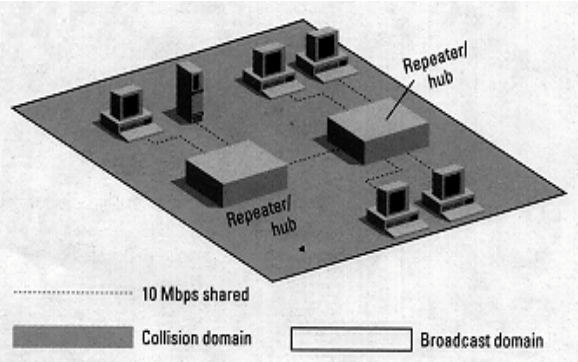


Diseñando Redes para Grupos de Trabajo

Un grupo de trabajo es una colección de usuarios finales que comparten recursos de cómputo; pueden ser grandes o pequeños, localizados en un edificio o un campus y ser permanente o un proyecto.

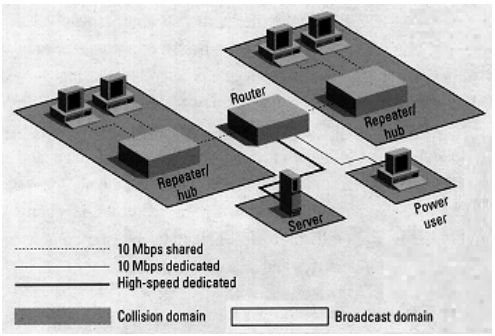
Pequeños Grupos de Trabajo.

En la figura se ve un típico ambiente de grupos de trabajo en una red interna. Tiene dos concentradores y puede crecer hasta 20, con 200 usuarios.



Aquí el administrador quiere máximizar el ancho de banda de los servidores y dividir las PCs en pequeños dominios de colisiones que compartan 10 Mbps y sólo un número límitado de usuarios poderosos requeriran 10 Mbps dedicados para sus aplicaciones.

Opción #1: Solución con Ruteador



El ruteador es configurado con una interface dedicada de alta velocidad al servidor y un número grande de interfaces ethernet, las cuales son asignadas a cada uno de los concentradores y usuarios poderosos. Y para instalarlo, el administrador de red divide los dominios grandes de broadcast y colisiones en dominios pequeños.

Ruteo como Política Segura

Cuando el número de usuarios en los grupos de trabajo se incrementa, el crecimiento de los broadcast puede eventualmente causar una legítima preocupación sobre lo siguiente:

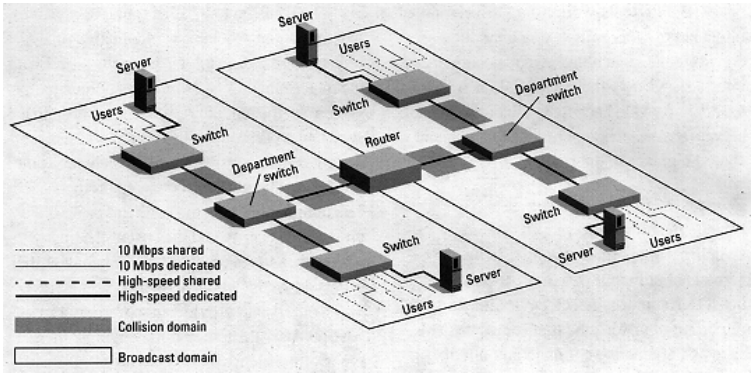
Redimiento en la red.

Problemas de aislamiento.

Los efectos de radiar el broadcast en el rendimiento del CPU de la estación final.

Segmentación Física

La figura ilustra como un ruteador segmenta físicamente la red dentro de dominios de broadcast. En este ejemplo, el administrador de red instala un ruteador como política de seguridad, además para evitar los efectos del broadcast, que alentan la red.



Notar que el ruteador tiene una interface dedicada para cada departamento o switch del grupo de trabajo. Esta disposición da al ruteador un dominio de colisión privado que aisla el tráfico de cada cliente/servidor dentro de cada grupo de trabajo. Si el patron del trafico esta entendido y la red esta propiamente diseñada, los switches haran todo el reenvio entre clientes y servidores. Sólo el tráfico que alcance al ruteador necesitará ir entre dominios individuales de broadcast o a través de una WAN.

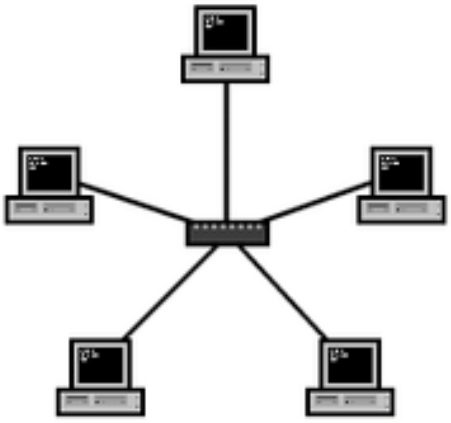
11.5.4 Futuro del Ruteo

El ruteo es la llave para desarrollar redes internas. El desafio es integrar el switch con ruteo para que el sistema aproveche el diseño de la red. Inicialmente los switches estarán en todas las organizaciones que requieran incrementar el ancho de banda y obtener la funcionalidad que necesitan. No obstante al incrementar la complejidad de la red, los administradores necesitarán controlar el ambiente de switch, usando segmentación, redundancia, firewall y seguridad. En este punto, la disponibilidad de ruteo sofisticado esencialmente crecerá y la red se escalará en grandes redes de switches.

11.6 Conmutadores (Switch)

11.6.1 Descripcion

Un switch es un dispositivo de interconexión de redes de ordenadores/computadoras que opera en la capa 2 del modelo OSI. Este interconecta dos o más segmentos de red, funcionando de manera similar a los puentes, pasando datos de una red a otra, de acuerdo con la dirección MAC de destino de los datagramas en la red.



Un conmutador en el centro de una **red en estrella**.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un *filtro* en la red, mejoran el rendimiento y la seguridad de las LANs .

Interconexión de conmutadores y puentes

Los puentes (bridges) y conmutadores (switches) pueden ser conectados unos a los otros, pero existe una regla que dice que sólo puede existir un único camino entre dos puntos de la red. En caso de que no se siga esta regla, se forma un bucle en la red, que produce la transmisión infinita de datagramas de una red a otra.

Sin embargo, esos dispositivos utilizan el algoritmo de spanning tree para evitar bucles, haciendo la transmisión de datos de forma segura.

Introducción al funcionamiento de los conmutadores

Conexiones en un *switch* Ethernet

Los conmutadores poseen la capacidad de aprender y almacenar las direcciones de red de nivel 2 (direcciones MAC) de los dispositivos alcanzables a través de cada uno de sus puertos. Por ejemplo, un equipo conectado directamente a un puerto de un conmutador provoca que el conmutador almacene su dirección MAC. Esto permite que, a diferencia de los concentradores o hubs, la información dirigida a un dispositivo vaya desde el puerto origen al puerto de destino. En el caso de conectar dos conmutadores o un conmutador y un concentrador, cada conmutador aprenderá las direcciones MAC de los dispositivos accesibles por sus puertos, por tanto en el puerto de interconexión se almacenan las MAC de los dispositivos del otro conmutador.

11.6.2 **Enrrutamientos**.

Bucles de red e inundaciones de tráfico

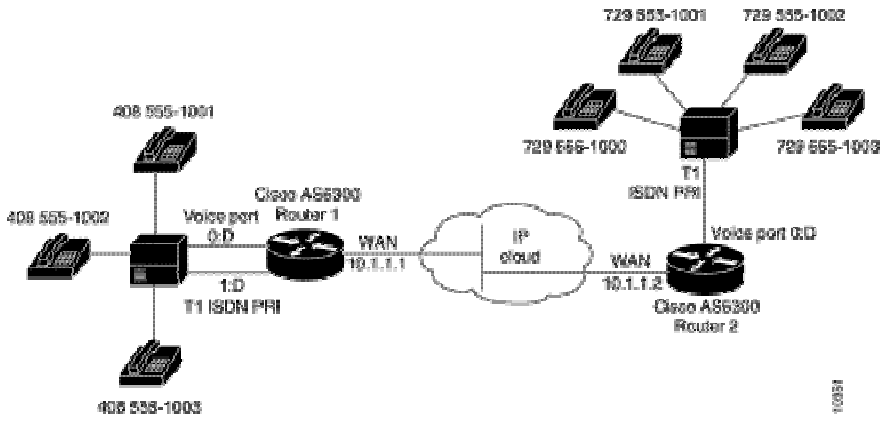
Como anteriormente se comentaba, uno de los puntos críticos de estos equipos son los bucles (ciclos) que consisten en habilitar dos caminos diferentes para llegar de un equipo a otro a través de un conjunto de conmutadores. Los bucles se producen porque los conmutadores que detectan que un dispositivo es accesible a través de dos puertos emiten la trama por ambos. Al llegar esta trama al conmutador siguiente, este vuelve a enviar la trama por los puertos que permiten alcanzar el equipo. Este proceso provoca que cada trama se multiplique de forma exponencial, llegando a producir las denominadas inundaciones de la red, provocando en consecuencia el fallo o caída de las comunicaciones.

Como se ha comentado se emplea el protocolo spanning tree para evitar este tipo de fallo.

11.7 Pasarelas (Gatway).

11.7.1. Descripción Gateways.

El tercer elemento lo conforman los gateways de Voz sobre IP, los cuales proporcionan un puente de comunicación entre los usuarios. La funcion principal de un gateway es proveer las interfases con la telefonía tradicional apropiada, funcionando como una plataforma para los clientes virtuales. Estos equipos también juegan un papel importante en la seguridad de acceso, la contabilidad, el control de calidad del servicio (QoS; Quality of Service) y en el mejoramiento del mismo.



11.7.2 Aplicación de las Pasarelas

Direccionamiento:

RAS (Registration, Admision and Status). Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través de el Gatekeeper.

DNS (Domain Name Service). Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS.

Señalización:

Q.931 Señalización inicial de llamada.

H.225 Control de llamada: señalización, registro y admisión, y paquetización/ sincronización del stream (flujo) de voz.

H.245 Protocolo de control para especificar mensajes de apertura y cierre de canales para streams de voz.

Compresión de voz:

Requeridos: G.711 y G.723.

Opcionales: G.728, G.729 y G.722.

Transmisión de voz:

UDP. La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.

RTP (Real Time Protocol). Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

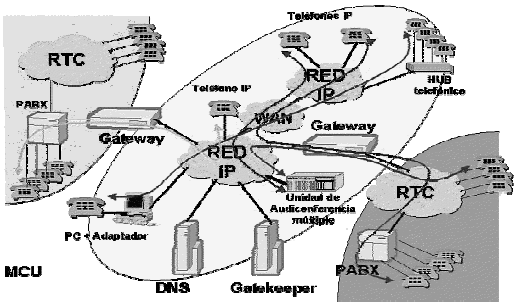
Control de la transmisión:

RTCP (Real Time Control Protocol). Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.

Gateways (pasarelas RTC / IP).

Gatekeeper.

Unidades de audioconferencia múltiple. (MCU Voz)



Servicios de Directorio.

Elementos de una red VoIP (Voz sobre IP)

Las funciones de los distintos elementos son fácilmente entendibles a la vista de la figura anterior, si bien merece la pena recalcar algunas ideas.

El Gatekeeper es un elemento opcional en la red, pero cuando está presente, todos los demás elementos que contacten dicha red deben hacer uso de él. Su función es la de gestion y control de los recursos de la red, de manera que no se produzcan situaciones de saturación de la misma.

El Gateway es un elemento esencial en la mayoría de las redes pues su misión es la de enlazar la red VoIP con la red telefónica analógica o RDSI. Podemos considerar al Gateway como una caja que por un lado tiene una interfase LAN y por el otro dispone de uno o varios de las siguientes interfaces:

FXO. Para conexión a extensiones de centralitas ó a la red telefónica básica.

FXS. Para conexión a enlaces de centralitas o a teléfonos analógicos.

E&M. Para conexión específica a centralitas.

BRI. Acceso básico RDSI (2B+D).

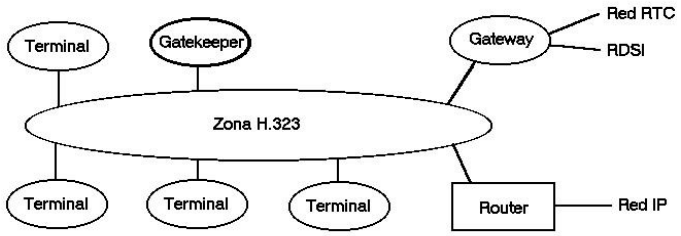
PRI. Acceso primario RDSI (30B+D).

G703/G.704. (E&M digital) Conexión especifica a centralitas a 2 Mbps.

Los distintos elementos pueden residir en plataformas físicas separadas, o nos podemos encontrar con varios elementos conviviendo en la misma plataforma. De este modo es bastante habitual encontrar juntos Gatekeeper y Gateway. También podemos ver cómo Cisco ha implementado las funciones de Gateway en el router.

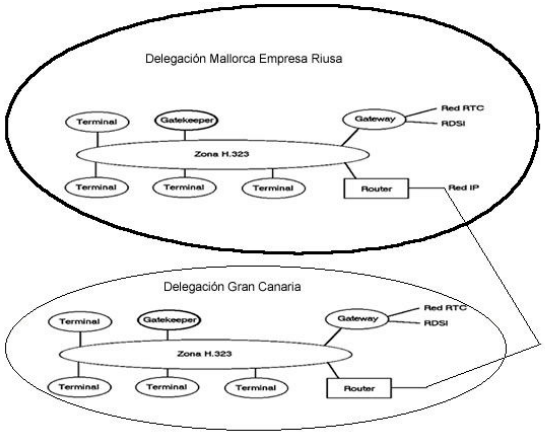
Gatekeepers: Son el centro de toda la organización VoIP, y serian el sustituto para las actuales centralitas. Normalmente implementadas en software, en caso de existir, todas las comunicaciones pasarían por él.

Gateways: Se trata del enlace con la red telefónica tradicional, actuando de forma transparente para el usuario.



Con estos tres elementos la estructura de la red quedaría como muestra la figura adjunta:

El Gateway sirve de enlace entre la RTC /RDSI y la zona H.323 (VoIP). A su vez existe un Gatekeeper que realiza el control de llamadas y la gestión del sistema de direccionamiento. El router permitiría enlazar con otras redes H.323 sin necesidad de utilizar la RTC, resultando todas las llamadas a zonas



11.8 Modems.

11.8.1. Descripcion

El módem es otro de los periféricos que con el tiempo se ha convertido ya en imprescindible y pocos son los modelos de pc que no estén conectados en red que no lo incorporen. Su gran utilización viene dada básicamente por dos motivos: Internet y el fax, aunque también le podemos dar otros usos como son su utilización como contestador automático incluso con funciones de centralita o para conectarnos con la red local de nuestra oficina o con la central de nuestra empresa.

11.8.2 Trasmisión de Datos

La transmisión de datos es el movimiento de información codificada de un lugar a otro de señales que portan dichos datos por medio de sistemas de comunicación eléctrica.

Las telecomunicaciones hacen referencia a la transmisión de datos a distancia. El teleprocesamiento permite que un sistema de computación utilice algún tipo de telecomunicación para procesar datos

11.8.3. Comunicación entre un Computador y Otro

La comunicación se logra mediante la utilización de las redes telefónicas y modem.

El módem puede estar en el gabinete de una PC (interno), o ser externo al mismo. Su función es permitir conectar un computador a una línea telefónica, para recibir o transmitir informacion.

En relación con la línea telefónica, el módem además de recibir/transmitir informacion, también se encarga de esperar el tono, discar, colgar, atender llamadas que le hace otro módem, etc.

Cuando un módem transmite, debe ajustar su velocidad de transmisión de datos, tipo de modulación, corrección de errores y de compresión. Ambos MODEM deben operar con el mismo estándar de comunicación.

Dos modems pueden intercambiar información en forma "full dúplex". Esto es, mientras el primero transmite y el segundo recibe, este ultimo también puede transmitir y el primero recibir. Así se gana tiempo, dado que un módem no debe esperar al otro a que termine, para poder transmitir, como sucede en "half dúplex".

El módem que llama, o sea que origina la comunicación se designa "originate" o "local", y el módem que contesta, responde, es el "answer" o "remoto".

Un módem puede contener en su interior dos cicuitos generadores de dos frecuencias (tonos) distintas, para enviar ceros y unos, en correspondencia con los que necesite enviar por vía telefónica.

Cuando un módem transmite tonos se dice que modula o convierte la señal digital binaria proveniente de un computador en dichos tonos que representan o portan bits.

Del mismo modo que el oído de la persona que en el extremo de la línea puede reconocer la diferencia de frecuencia entre los tonos del 0 y 1, otro módem en su lugar también detecta cual de las dos frecuencias esta generando el otro módem, y las convierte en los niveles de tensión correspondiente al 0 y al 1.

Esta acción del módem de convertir tonos en señales digitales, o sea en detectar los ceros y unos que cada tono representa, se llama demodulacion.

El tipo de modulación ejemplificada, con una frecuencia para el uno y otra para el cero, solo permite transmitir hasta 600 bits por segundo.

11.8.4. Protocolos de Comunicaciones.

En la comunicación modem-modem se debe cumplir otra secuencia de acciones y señales:

1: El módem local realiza una acción semejante a levantar el tubo, y luego disca el numero telefónico del módem remoto.

2: El módem remoto lleva a cabo una acción equivalente a levantar el tubo y emite un tono o serie de tonos particulares que indican que ha respondió el llamado, y que se puede comunicar a una velocidad (bps) y modulación (ambas normalizadas).

3: El módem local responde a la serie de tonos, y negocia con el módem remoto la mayor velocidad de transmisión posible.

Un módem debe ajustarse a dos protocolos:

El protocolo rs232c

Protocolo estándar, como los serie V de la ccitt.

11.8.4.1 Transmisión Asincrona de Datos o Protocolo "STAR-STOP" :

Los datos que maneja un módem están organizados en bytes separables, al igual que cuando se almacenan en una memoria principal.

En la transmisión asincronica los datos se envían como bytes independientes, separados, pudiendo mediar un temporal cualquiera t entre un byte y el siguiente. Es el modo de transmisión corriente vía módem usado en las PC, siendo en general el empleado por su sencillez para bajas velocidades de transmisión dedatos

Supongamos que se envía X dato de 8 bits, los 8 bits se envían en orden inverso a indicado. Aparecen los bit de control "start" (siempre 0) que indica comienzo de carácter, y "stop"(siempre 1) de final de byte enviado. En total son pues 10 bits (rendimiento del 80%). Para poder distinguir un bit del siguiente cada bit debe durar igual tiempo T.

Para tal fin sirve el bit de start, que permite sensar en momentos adecuados (en sincronismo) el valor de los bits siguientes hasta el "stop".

En la transmisión sincrónica se envía un paquete de bytes sin separación entre ellos, ni bits de start y stop (aunque existen bytes de comienzo y final). Así es factible enviar mas bytes por segundo.

BIT DE PARIDAD:

Supongamos que la PC que transmite envía A=01000001, pero por un ruido en la línea telefónica mientras el módem transmitía, se recibe 01000010, el código recibido será el de la letra C, sin que se pueda notar el error. Dado que ASCII básicamente se codifica en 7 bits, se puede usar el bit restante para detectar si se ha producido un solo error por inversión como el ejemplificado. Entre dos computadores que se comunican, se adopta la convención de que en cada carácter emitido o recibido debe haber un numero par de unos. El computador que esta enviando, da valor al bit restante citado, de modo que se cumpla dicha paridad. El computador que recibe debe verificar que cada carácter que le llega tenga la paridad convenida. Caso contrario pedirá su retransmisión pues implica que un bit llego errado

La paridad sirve para detectar si uno de los bits recibidos cambio de valor, que es la mayor probabilidad de errores en transmisión telefónica. Si los bits errados son dos, la paridad par

seguirá, y no hay forma de detectar un carácter mal recibido, pues este metodo supone solo un bit errado. Cuando se usa 8 bits sin paridad ("null parity"), con un bit de stop, se indica 8N1, que es la forma usual de comunicación entre dos PC.

Si como en el ejemplo dado, son 7 bits, con paridad par ("even parity") y un bit de stop, se indica 7E1.

Para el control del envío de archivos de programas existen los protocolos de archivo en los programas Xmodem, Zmodem y otros.

Estos programas dividen al archivo a enviar en bloques de igual tamaño, que se envían (byte a byte con paridad nula) con el agregado de un numero que es el resultado de un calculo polinomial sobre los bits de cada bloque. En el receptor sobre cada bloque recibido se realiza al mismo calculo. Si se obtiene el mismo numero agregado se envía un simple OK. De no recibirlo, se vuelve a transmitir el bloque.

11.8.5 Formas mas usuales de Modulación.

Una onda que cambia entre dos frecuencias para codificar uno y cero, esta modulada en frecuencia (FSK= Frecuency-Shift-Keying= Codificación por **cambio** de frecuencia)

Supongamos una onda portadora con modulación en amplitud, siendo que en el presente este tipo de variación de la forma de una onda se usa en combinación con cambios en la fase de la misma. Cada cambio de fase es como si la porción de onda que sigue a dicho cambio, se adelantara (o atrasara) con relación a lo que debiera ser una forma senoidal continua, pura. Esta forma de cambiar la señal portadora para representar combinaciones binarias, se denomina modulación en fase (PSK=Phase-Shift-Keying=Codificacion por cambio de fase). Resulta ser la más eficaz para transmitir datos binarios en líneas con ruido, siendo que requiere que el emisor y el receptor sean muy complejos.

En un módem actual, los cambios en la portadora pueden ser tanto de amplitud como de fase. La primer técnica conocida como QAM (Quadrature Amplitude Modulation), se concreto en las normas V.22 bis, para portadora modulada a 600 baudios, y con 4 bits por cambio , con lo cual se podía transmitir hasta 600x4= 2400 bps.

Mediante complejas técnicas se logro que la modulación se adaptara a cada instante al estado de la línea telefónica. Se agregaron otras técnicas que requieren efectos compensatorios del mismo tipo en el módem receptor. Se usan cinco velocidades de señalización, siendo la máxima de 3429 baudios, y la mínima de 2400. Cada velocidad implica una frecuencia distinta de portadora, por lo que esta técnica supone la transmisión en un ancho de banda variable según el estado de la línea.

11.8.6. Software necesario para Operar un MODEM:

Se los denomina programas de comunicaciones".

Típicamente puede realizar las siguientes funciones:

Atender el teléfono y transferir archivos hacia otro computador

Recibir archivos

Llevar un directorio de números telefónicos y parámetros de otros computadores.

Hacer que una PC emule una terminal de teclado y pantalla tipo VT100, ANSI o TTY en comunicaciones con grandes computadoras (mainframes)

Permitir tipear comandos y que sean visibles en el monitor.

Manejar buffers para guardar la ultima información que se fue de pantalla (scrollback)

Ayudar sobre la operatoria en curso.

Al ser inicializado un programa de este tipo, preguntara por la marca o tipo de módem conectado. El usuario tiene a su disposición en el modo comando un conjunto de ordenes para definir los contenidos de los registros S0, S1.... de un módem antes citados. De esta forma se establece como operara un módem.

Para que se le pueda emitir un comando desde el teclado, un módem debe estar en "modo comando". Los comandos se tipean precedidos por la sigla AT (ATtention), y modifican los contenidos binarios de los registros del módem.

Encontramos entre otros:

ATE1; ATV1; ATS0=n; ATB1; ATL2; etc.

Aunque el usuario no ordene comandos, el programa de comunicaciones cuando es llamado inicializa los registros del módem con valores default, que son datos fijos que contiene dicho programa.

11.8.7 Fax-Modem

11.8.7.1 Operativa de un Fax

Para entender la operatoria de un fax modem, primero debemos entender la de un fax común y corriente.

Dada una hoja con texto, el servicio de fax o facsímil permite obtener una copia de la misma en un lugar distante, a través de una línea telefónica establecida entre dos maquinas de fax.

Dos aparatos de fax comunicados telefónicamente son como dos fotocopiadoras tales que una de ellas lee la hoja a copiar, barriéndola mediante sensores fotoeléctricos, para convertir la imagen en un conjunto de puntos de valor 0 (blancos) y 1 (negros), que son transmitidos como señales eléctricas binarias hacia la otra fotocopiadora. El módem se encarga de convertir las señales binarias digitales en analógicas.

Esta recibe dichas señales y genera una reproducción de la hoja original. Cada maquina de fax contiene un teléfono, un sistema de barrido de imagen, un sistema de impresión y un módem.

La resolución se refiere a la densidad de puntos usada para reproducir un fax; puede tenerse en cada pulgada cuadrada, 98 líneas verticales y 203 horizontales. Estas ultimas se duplican para una resolución fina.

BIBLIOGRAFIA

-REDES DE COMPUTADORES.
ANDREW S. TANEUBAUM.
CUARTA EDICION, EDITORIAL PEARSON PRENTICE HALL.

-REDES INICIACION Y REFERENCIA
JESUS SANCHEZ ALLENDE, JOAQUIN LOPEZ
EDITORIAL MC GRAW HILL

- COMUNICACIONES Y REDES DE COMPUTADORES
WILLIAM STALLINGS
EDITORIAL PRENTICE HALL

- REDES DE ORDENADORES
TANENBAUM ANDREW S.
SEGUNDA EDICIÓN, EDITORIAL PRENTICE HALL.

-DOMINE TCP/IP
JOSE LUIS RAYA CABRERA Y VICTOR RODRIGO RAYA
EDITORIAL RA-MA.

REDES GLOBALES DE INFORMACION CON INTERNET Y TCP/IP
DOUGLAS E. COMER
TERCERA EDICION, EDITORIAL PRENTICE HALL

- TESIS.
IMPLEMENTACION DE UNA RED BASADA EN LOS PROTOCOLOS TCP / IP Y NSF
MARCOANTONIO CRUZ MENDOZA.

- TESIS
PRINCIPIO DE LAS REDES DE COMUNICACIONES DE DATOS.
ROSA MARIA AMADOR RAMÍREZ.