UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

INTERCONEXIÓN DE REDES LAN CON FRAME RELAY

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO ELECTRÓNICO

PRESENTADO POR:

LEONCIO ARMAS CASTRO

PROMOCIÓN
1995 – II

LIMA – PERÚ

2002

A mis padres Teodora y Leoncio,
a mi esposa Maiza y a mis hijas
Rosmery, Miluska y Melissa,
quienes llenan mi vida y
motivan mi superación.

INTERCONEXION DE REDES LAN CON FRAME RELAY

SUMARIO

El presente informe ofrece una visión general, sobre las redes LAN, así como las características principales las redes de conmutación de paquetes Frame Relay, ATM y SDH, además se describen los diversos equipos que intervienen para la interconexión de las redes LAN, se realiza una descripción del router Cisco, sus características y los comandos mas usados para su configuración, a fin de lograr la interconexión de las redes LAN.

ÍNDICE

PRÓLOGO

El tamaño, complejidad y el completo volumen del trafico de datos han ido creciendo a saltos. Nuevas aplicaciones semejantes a: Intercambio Electrónico de Datos (EDI), transferencia de archivos, CAM/CAD y el explosivo crecimiento de las Redes de Area Local (LANs); ha requerido la necesidad de que sea posible transmitir grandes volúmenes de datos a altas velocidades y en imprevisibles patrones llamados Burst (ráfagas de datos). Al mismo tiempo, la calidad de las líneas de las compañías telefónicas, nodos y redes han impulsado el cambio a la tecnología digital. Al mismo tiempo, el equipo de procesado de datos, equipo de comunicación de datos y software ha provocado la busca de nuevos niveles de sofisticación. Teniendo todo esto en cuenta y que la industria de telecomunicaciones se ha enfrentado con el dilema de mejorar incrementando los niveles de bursty en el trafico de datos ha reducido costos y ha aumentado las velocidades de transmisión.

Los usuarios de Frame Relay lo usan por la misma razón: la interconexión de LANs. No sorprende entonces que en un principio Frame Relay fuera diseñado para ello. Sin embargo, Frame Relay no es sólo por el ahorro de costes: también puede ser implantada por una mejor calidad de servicio. Una red Frame Relay puede ser altamente viable por poder escoger una nueva ruta en el caso del fallo de la línea y, por con siguiente un rico patrón de interconexión, Frame Relay puede reducir el número de saltos entre nodos intermedios dando tiempos de respuesta imprevistos.

CAPÍTULO I

REDES LAN

General

Con las redes de datos de área local, a las que simplemente llamamos redes LAN (Local Area Networks), se interconectan las comunidades distribuidas de DTE (Data Terminal Equipment) basadas en computadoras situados dentro de un mismo edificio o grupo localizado de edificios. Por ejemplo, con una LAN podemos conectar entre sí estaciones de trabajo distribuidas en las oficinas de un solo edificio o grupo de edificios, como podría ser el caso de un campus universitario, o para interconectar equipos computarizados distribuidos en una fábrica o complejo hospitalario. En virtud de que todos los equipos se encuentran dentro de un mismo establecimiento, es normal que la organización instale y mantenga la LAN, que por esta razón se conoce también como red de datos privada.

La diferencia principal entre un camino de comunicación establecido con una LAN y una conexión a través de una red de datos pública es que una LAN suele contar con tasas de transmisión de datos mucho más altas debido a las distancias físicas relativamente cortas que debe salvar. En el contexto del modelo de referencia de la Organización Internacional de Normas (ISO) para la Interconexión de Sistemas Abiertos (OSI), esta diferencia sólo se manifiesta en las capas inferiores,

dependientes de la red. En muchos casos, las capas de protocolo más altas del modelo de referencia son las mismas en ambos tipos de redes.

Hay dos tipos muy distintos de LAN: LAN por cable y LAN inalámbricas. Como lo indican sus nombres, las LAN por cable utilizan cableado (fijo) – par trenzado o cable coaxial – como medio de transmisión, en tanto que las LAN inalámbricas utilizan ondas de radio o de luz.

1.1 LAN POR CABLE

1.1.1 TOPOLOGÍA

Casi todas las WAN, al igual que la Red Telefónica Publica Conmutada (PSTN), tiene una topología de malla (también llamada de red). Empero, en el caso de las LAN la separación física de los DTE suscriptores permite usar topologías más simples. Las cuatro topologías comunes a todas ellas son las de estrella, bus, anillo y concentrador, como se muestra en la figura 1.1.

Tal vez el mejor ejemplo de una LAN basada en una topología de estrella sea la central de ramal automática privada (PABX: private automatic branch exchange) digital. En muchos sentidos una conexión establecida a través de una PABX analógica tradicional es similar a una conexión establecida a través de una PSTN analógica en cuanto a que todos los caminos a través de la red están diseñados para transportar voz analógica de ancho de banda limitado; por tanto, si con ellos queremos transportar datos, requeriremos modems. Sin embargo, la mayor parte de

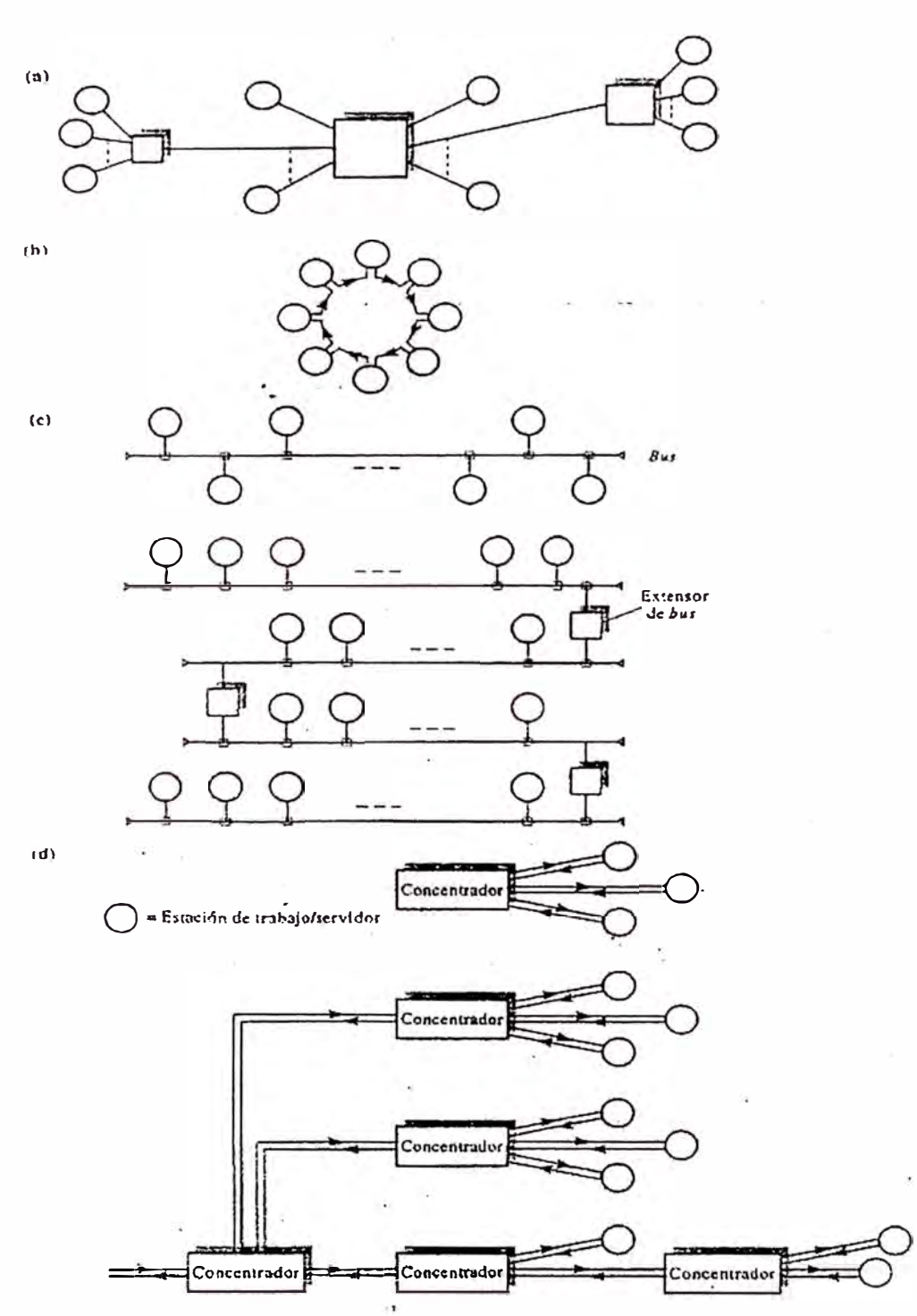
las PABX, modernas usa técnicas de conmutación digital dentro de la central, por lo que también reciben el nombre de centrales digitales privadas (PDX: private digital exchanges). Es más, la disponibilidad de circuitos integrados de bajo costo encargados de las funciones de conversión de analógico a digital y de digital a analógico ha permitido que, en poco tiempo, sea una práctica común el extender el modo digital hasta los conectores de los suscriptores. Esto significa que un camino conmutado de 64 kbps - la tasa de digitalización que suele usarse para la voz digital - está disponible en el conector de cada suscriptor, el cual entonces puede utilizarse tanto para datos como para voz.

Las topologías preferidas para las LAN que han sido diseñadas para funcionar como subredes de comunicación de datos que interconectan equipos computarizados locales son las de bus (lineal) y de anillo. En la práctica, las redes de bus suelen extrenderse a un conjunto de buses conectados entre sí, de modo que más bien parecen ser un árbol desarraigado. Por lo regular, cuando se utiliza una topología de bus, el cable de red único pasa por todos los lugares en los que hay un DTE que va a conectarse a la red, y se realiza una conexión física (derivación) al cable para que el DTE usuario pueda tener acceso a los servicios de red provistos. Mediante los circuitos y algoritmos de control de acceso al medio (MAC) apropiados se comparte el ancho de banda de transmisión disponible entre la comunidad de los DTE conectados.

Con una topología de anillo, el cable de la red pasa de un DTE a otro hasta que todos quedan interconectados en forma de lazo o anillo. Una característica de la topología de anillo es que existe un enlace punto a punto directo entre los DTE vecinos que

opera en un solo sentido. Los algoritmos de MAC apropiados aseguran que la comunidad de usuarios comparta el uso del anillo.

Figura 1.1 : Topologías de LAN: (a) estrella; (b) anillo; (c) bus; (d) concentrador/árbol



Las tasas de transmisión de datos empleadas en las topologías de anillo y de bus (por lo regular entre 1 y 10 Mbps) las hacen más apropiadas para inteconectar comunidades locales de equipos computarizados, como las estaciones de trabajo en un entorno de oficina o los controladores inteligentes de una planta de proceso.

Una variación del bus y el anillo es la topología de concentrador. Aunque estas redes parecen tener una topología estrella, el concentrador no es más que el cableado de bus o de anillo concentrado en una unidad central. Los alambres que conectan cada DTE al bus o anillo se extienden desde el concentrador. A diferencia de los PDX, el concentrador no realiza funciones de conmutación, y consiste simplemente en un conjunto de repetidores que retransmiten todas las señales recibidas de los DTE, a todos los demás DTE tal como se hace en las redes de bus o de anillo. Como puede apreciarse, los concentradores también pueden conectarse en una disposición jerárquica para formar una topología de árbol. Una vez más, la topología combinada funciona como una sola red de bus o de anillo, o como un conjunto interconectado de tales redes.

1.1.2 MEDIOS DE TRANSMISIÓN

Los tres principales tipos de medios de transmisión propios de las LAN son el par trenzado, cable coaxial y la fibra óptica.

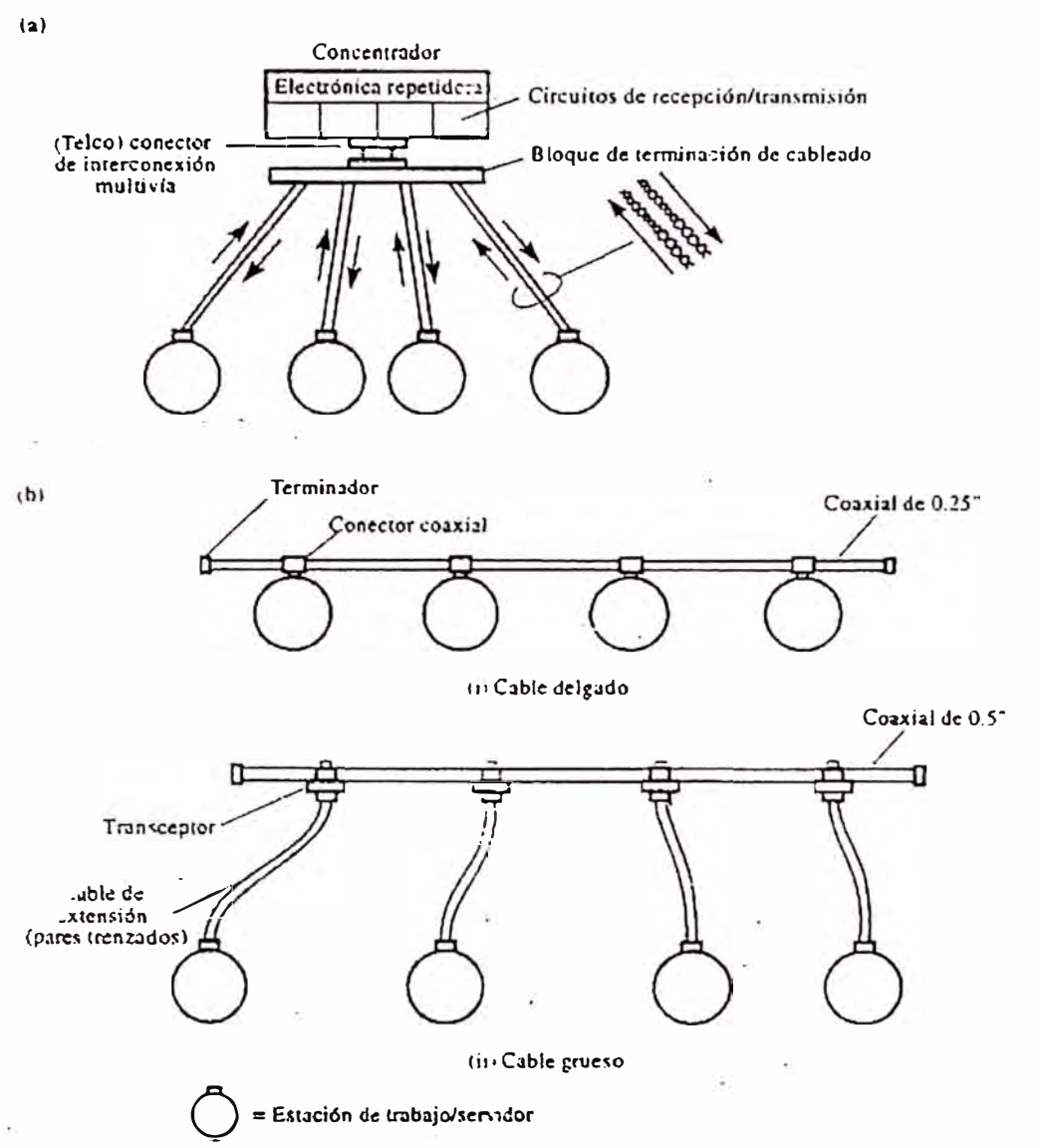
El par trenzado –tanto blindado como sin blindaje- se emplea primordialmente en las redes de concentrador. Como el par trenzado es menos rígido que el cable coaxial o la fibra óptica, es más fácil de instalar. Además, la mayor parte de los escritorios de oficina cuentan con conductos para cableado de telefonía que resultan apropiados

para los cables de par trenzado, así que es menos costoso instalar pares trenzados adicionales para transmitir datos que instalar nuevos conductos de cables coaxial o fibras. El esquema general se ilustra en la figura 1.2(a).

Existe un límite superior para la longitud de los cables de par trenzado que depende de la tasa de bits empleada. Por lo regular, el límite es de 100 m a 1 Mbps o, si se cuenta con circuitos adicionales de eliminación de diafonía, de 100 m a 10 Mbps. Una disposición característica consiste en un par trenzado entre cada uno de los DTE y el armario de cableado más cercano de un piso del edificio y cable coaxial para conectar los armarios de cableado de cada piso al concentrador principal del edificio. En las instalaciones que abarcan varios edificios, por lo regular es con fibra que se conecta al concentrador de cada edificio a un concentrador principal. Este último suele trabajar con una tasa de bits más alta y está configurado lógicamente como una red de anillo. Este tipo de disposición se conoce como cableado estructurado.

Con las LAN es muy utilizado el cable coaxial, sobre todo en las redes de bus, que operan con transmisión tanto de banda base como de banda ancha. Dos tipos de cable se emplean con banda base: cable delgado y cable grueso. Los términos se refieren al diámetro del cable: el cable delgado es de 0.25 pulgadas de diámetro, y el cable grueso es de 0.5 pulgadas de diámetro. Por lo regular, ambas trabajan con la misma tasa de bits –10 Mbps- pero el cable delgado produce una mayor atenuación de la señal; la distancia máxima entre repetidores con cable delgado es de 200 m, en comparación con los 500 m del cable grueso. Recordemos que con un repetidor se regenera una señal recibida a su forma original. Las dos modalidades de operación, cable delgado y grueso, se llaman 10 base 2 –10 Mbps, banda base, 200 m de longitud máxima- y 10 base 5 respectivamente.

Figura 1.2 : Medios de transmisión (a) par trenzado; (b) cable coaxial de banda base



Con frecuencia el cable coaxial delgado sirve para interconectar estaciones de trabajo en la misma oficina o laboratorio. El conector físico con el cable coaxial se enchufa directamente a la tarjeta de interfaz de la estación de trabajo. En contraste, el cable coaxial grueso, en virtud de su estructura más rígida, suele estar instalado aparte de las estaciones de trabajo, digamos a lo largo de un pasillo. Es preciso usar cableado

adicional –llamado cable de extensión- y circuitos electrónicos de transmisión y recepción –un transceptor- entre el punto de derivación del cable coaxial principal –llamada interfaz de unidad de conexión (AUI: attachment unit interface)- y el punto de conexión a cada estación de trabajo.

En la transmisión de banda ancha, en lugar de transmitir información al cable como dos niveles de voltaje correspondientes al flujo de bits transmitido (banda base), el ancho de banda total disponible (intervalo de frecuencias) del cable se divide en varias bandas de subfrecuencias más pequeñas o canales. Cada banda de subfrecuencias se usa, con la ayuda de un par de modems especiales, para suministrar un canal de comunicación de datos independiente. Esta forma de trabajar se llama multiplexión por división de frecuencias y dado que las frecuencias están en la banda de radio, los modems son modems de radiofrecuencia. Este principio, denominado operación de banda ancha, también se utiliza ampliamente en la industria de la televisión de antena comunitaria (CATV: community antenna television) para multiplexar varios canales de televisión en un solo cable coaxial. Por lo anterior, la banda ancha es una alternativa viable respecto a la banda base cuando la red proporciona una diversidad de servicios.

La fibra óptica se fabrica con vidrio o plástico y puede operar con tasas de datos bastantes mayores que las alcanzables con un cable de par trenzado o coaxial. Como los datos se transmiten mediante un haz de luz, la señal no resulta afectada por la interferencia electromagnética. Por ello, la fibra óptica es idónea para aplicaciones que exigen una tasa de datos muy alta o bien niveles altos de inmunidad a la interferencia electromagnética, como las plantas industriales que contienen una gran cantidad de equipos eléctricos. Además como la fibra no emite radiaciones

electromagnéticas que pudieran ser captadas por un espía, es apropiada para aplicaciones que exigen un alta nivel de seguridad.

Puesto que los datos se transmiten mediante un haz de luz, se emplean circuitos electrónicos de transmisión y recepción especiales que convierten energía eléctrica en óptica y viceversa. Además los conectores físicos que se emplean con la fibra óptica es más costosos que los que sirven para conectar cables de par trenzado o coaxiales, y también es mas difícil sacar derivaciones físicas de un cable de fibra. Por estas razones, usamos fibras ópticas en configuraciones de concentrador o en redes de anillo de alta velocidad y en otras redes que utilizan caminos de transmisión punto a punto. Dos ejemplos de esto último son las redes de interfaz de datos distribuida por fibra (FDDI: Fiber Distributed Data Interfaces) y las de cola distribuida y bus dual (DQDB: distributed-queue, dual-bus).

1.1.3 MÉTODOS DE CONTROL DE ACCESO AL MEDIO

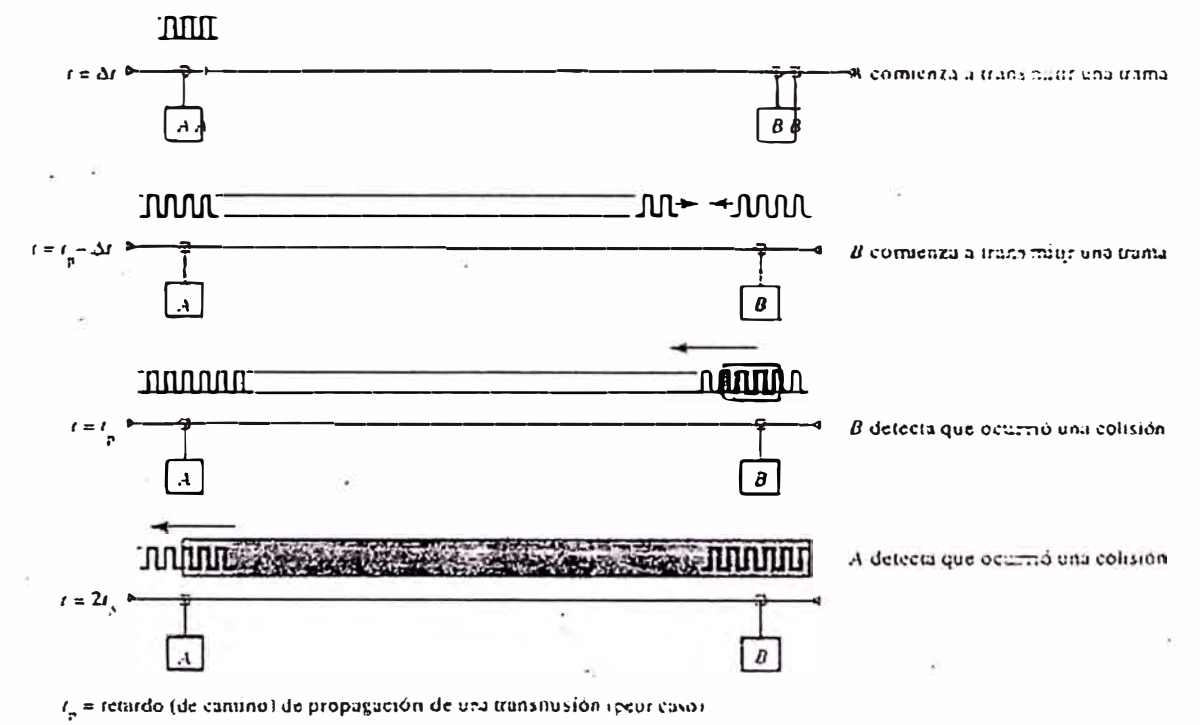
- **CSMA/CD**

En el método del Acceso Múltiple por Detección de Portadora con Detección de Colisión (CSMA/CD) sólo se usa con redes de bus. En esta topología de red, todos los DTE están conectados directamente al mismo cable, por el que se transmiten todos los datos entre cualquier par de DTE. Se dice que el cable opera en modo de múltiple acceso (MA).

Con esta modalidad de funcionamiento, dos DTE pueden intentar transmitir una trama por el cable al mismo tiempo, lo que causa la alteración de los datos de ambas

fuentes. A fin de reducir esta probabilidad, el DTE de origen, antes de transmitir una trama, primero escucha --electrónicamente- el cable para detectar si se está transmitiendo alguna trama. Si se detecta una señal portadora, el DTE aplaza su transmisión hasta que se haya transmitido la trama detectada, y solo entonces intenta enviar su trama. Aun así, dos DTE pueden determinar que no existe actividad en el bus y comenzar a transmitir sus tramas al mismo tiempo. Se dice entonces que tiene lugar una colisión, ya que el contenido de una trama chocará con la otra y los datos se alterarán, esto se ilustra en la figura 1.3.

Figura 1.3 : Esquema de Colisión con CSMA/CD



Al mismo tiempo que transmite el contenido de una trama, el DTE controla la señal de datos en él, Si la señal transmitida es distinta de la controlada, se da por hecho que ocurrió una colisión: colisión detectada (CD).

- **TESTIGO DE CONTROL**

Otro forma de controlar el acceso a un medio de transmisión compartido es mediante un testigo (permiso) de control. Este testigo se pasa de un DTE a otro según un conjunto definido de reglas que obedecen todos los DTE conectados al medio. Un DTE sólo puede transmitir una trama si posee el testigo, y después de haber transmitido la trama, entrega el testigo para que otro DTE pueda tener acceso al medio de transmisión. La secuencia de transmisión es la siguiente:

Primero se establece un anillo lógico que enlaza todos los DTE conectados al medio físico, y se crea un único testigo de control.

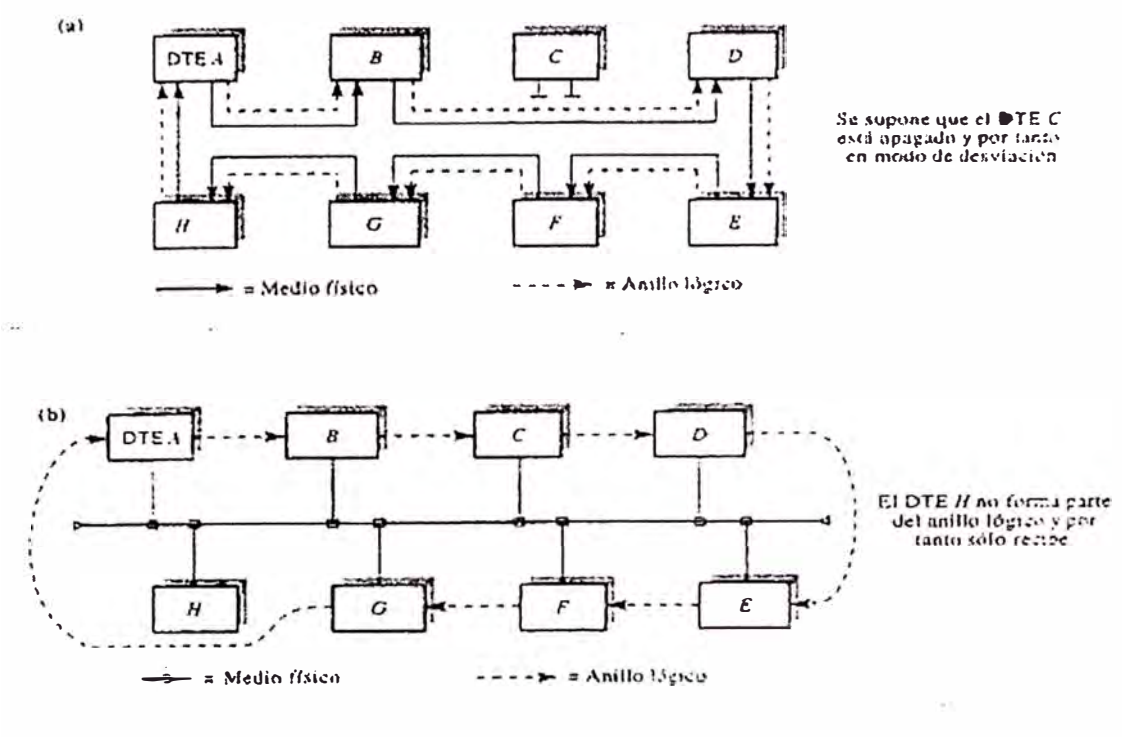
El testigo se pasa de un DTE a otro a través del anillo lógico hasta que lo recibe un DTE que desea transmitir una o más tramas.

El DTE que espera transmite entonces la o las tramas por el medio físico, después de lo cual pasa el testigo de control al siguiente DTE del anillo lógico.

Las funciones de control dentro de los DTE activos conectados al medio físico constituyen la base para la iniciación y la recuperación del testigo. Aunquie las funciones de control están replicadas en todos los DTE conectados al medio, sólo un DTE a la vez tiene la responsabilidad de efectuar la recuperación y la reiniciación.

No es necesario que el medio físico tenga una topología de anillo; también se puede controlar el acceso a una red de bus con un testigo. En la figura 1.4 se ilustra el establecimiento de un anillo lógico en dos tipos de redes.

Figura 1.4 : MAC por testigo de control: (a) anillo con testigo (b) bus con testigo



1.2 TIPOS DE LAN POR CABLE

Los dos tipos dominantes de LAN por cable que se han creado para interconectar comunidades locales de equipos computarizados son las de bus y las de anillo.

1.2.1 BUS CSMA/CD

Las redes de bus CSMA/CD tienen amplia aplicación en los entornos técnicos y de oficina. Por razones históricas, a una red de bus CSMA/CD también se le conoce como Ethernet. Por lo regular, se implementa como una red de cable coaxial de banda base de 10 Mbps o bien como una red de cable de par trenzado de 10 Mbps,

aunque en los documentos normativos se contemplan también otros medios de cable. Entre ellos los siguientes:

10 base 2,	Cable coaxial delgado (0.25 pulg. De diámetro) con una longitud de segmento máxima de 200 m.
10 base 5	Cable coaxial grueso (0.5 pulg. De diámetro) con una longitud de segmento máxima de 500 m.
10 base T	Topología de concentrador (estrella) con cables de extensión de par trenzado.
10 base F	Topología de concentrador (estrella) con cables de extensión de fibra óptica.

Sea cual sea el medio de transmisión, la tarjeta controladora de comunicaciones de cada DTE contiene lo siguiente:

Una unidad de control de acceso al medio (MAC), que se encarga de funciones como el encapsulamiento y el desencapsulamiento de las tramas para transmitirlas y recibirlas por el cable, la detección de errores y la implementación del algoritmo de MAC.

Una memoria de acceso aleatorio (RAM) de doble puerto que permite a la unidad de MAC recibir y transmitir tramas con la elevada tasa de bits del enlace, y al computador (anfitrión) leer/escribir el contenido de información de las tramas.

1.2.2 ANILLO CON TESTIGO

Las redes de anillo con testigo también se usan de manera preponderante en entornos técnicos y de oficina. Siempre que un DTE (estación) desea enviar una trama, espera el testigo antes de hacerlo. Al recibir el testigo, inicia la transmisión de la trama. Cada uno de los DTE del anillo repite la trama (es decir, recibe y luego retransmite cada uno de los bits) hasta que circula de vuelta al DTE originador, el cual lo saca del anillo. Además de repetir la trama, el destinatario conserva una copia de ella e indica que ya hizo esto asignando el valor correspondiente a los bits de respuesta al final de la trama.

1.2.3 BUS CON TESTIGO

En virtud de la naturaleza determinista de los métodos de MAC por testigo y de la capacidad para asignar prioridades a las transmisiones de tramas, las redes de bus con testigo se usan en la industria de la fabricación (para la automatización de fábricas) y en otros dominios afines, como la industria de control de procesos. En condiciones normales (libres de errores), el funcionamiento de este tipo de red es similar al de la red de anillo con testigo pero, debido a las diferencias en los dos métodos de accesos al medio (difundido en el caso del bus, secuencial en el anillo), es inevitable que haya diferencias en los procedimientos contemplados para la gestión del anillo lógico, como los de iniciación y de pérdida del testigo.

Por lo regular, en este tipo de redes se usa cable coaxial como medio de transmisión y suelen operar en una modalidad de banda ancha o en una modalidad de banda base

modificada, que se llama banda portadora. Los circuitos de modulación y de control de la interfaz realizan las siguientes funciones:

Codificación de datos por transmitir (modulación)

Decodificación de los datos recibidos (demodulación)

Generación de reloj

1.3 LAN INALÁMBRICAS

En los tipos de LAN que hemos visto hasta aquí, los medios físicos de transmisión han sido el cable de par trenzado o bien el cable coaxial. Un costo importante asociado a estas LAN es el de instalar el cableado físico, además se puede incurrir en un costo similar para cambiar el plan del cableado. Esta es una de las razones por las que han aparecido LAN inalámbricas, esto es, LAN que no utilizan cables físicos como medio de transmisión.

Una segunda razón es la aparición de las terminales manuales y de los computadores portátiles. Los avances tecnológicos han hecho que tales dispositivos puedan comportarse cada vez más favorablemente, en cuanto a su potencia, con muchos computadores estáticos.

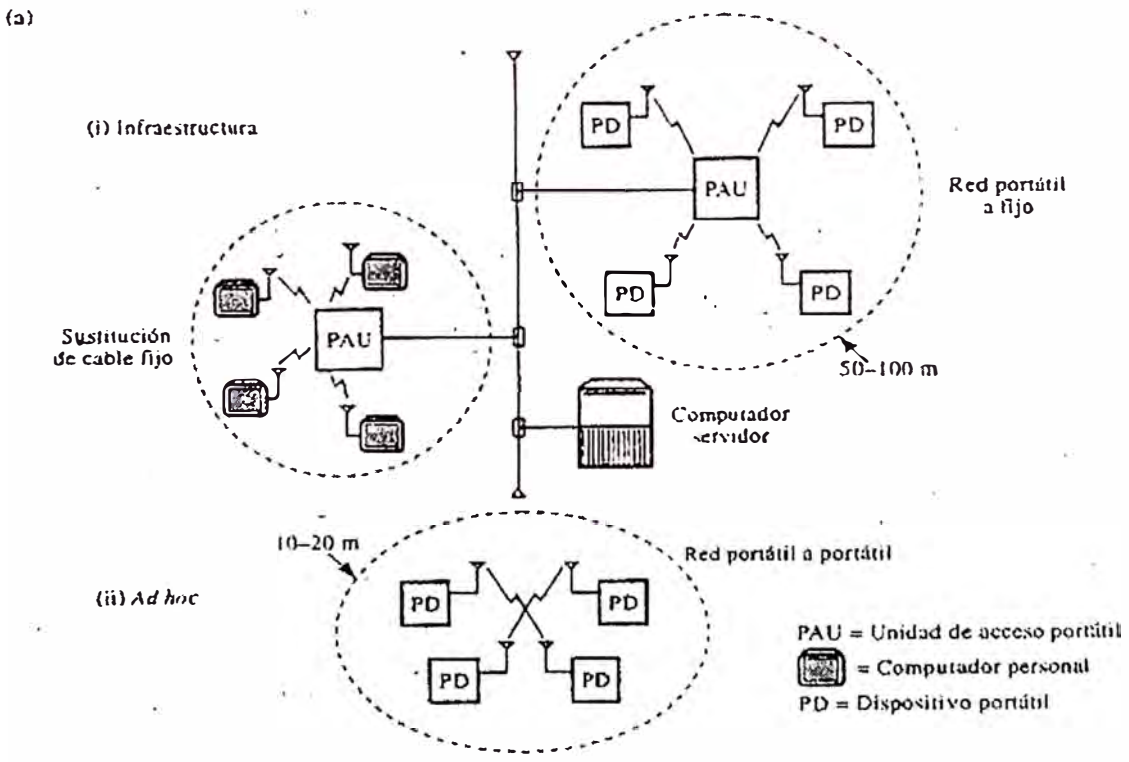
En la figura 1.5 se presenta un diagrama esquemático de las dos aplicaciones de LAN inalámbricas. Como podemos ver, en la primera aplicación, mediante un dispositivo intermedio llamado unidad de acceso portátil (PAU: portable access unit) se obtiene acceso a un computador servidor conectado a una LAN por cable. Por lo regular, el campo de cobertura de la PAU es de 50 a 100 m, y en una instalación grande hay muchas de estas unidades distribuidas dentro de un sitio. En conjunto, éstas

proporcionan acceso a la LAN del sitio –y por tanto a los computadores servidores- a través de una terminal manual, un computador portátil o un computador estático, todos los cuales pueden estar ubicados en cualquier punto del sitio. A este tipo de aplicación se le conoce como LAN inalámbrica de infraestructura.

En la segunda aplicación, cabe suponer que un conjunto de computadores portátiles quiera comunicarse entre sí para formar una LAN autónoma. Por ejemplo, esto puede hacerse dentro de una sala de conferencias durante una reunión, o en un aeropuerto. Como tales redes se crean por demanda, es común denominarlas LAN inalámbricas ad hoc.

Los dos tipos de medios que se emplean con las LAN inalámbricas son las ondas de radiofrecuencia y las señales ópticas de infrarrojo.

Figura 1.5 : LAN inalámbricas: (a) topologías de aplicación



- **ONDAS DE RADIO**

Las ondas de radiofrecuencia se utilizan ampliamente en muchas aplicaciones: entre ellas la difusión de radio y televisión y las redes de telefonía celular. Los requisitos para confinar las emisiones de radio a una banda de frecuencia específica y para que los receptores correspondientes sólo seleccionen las señales que caigan en dicha banda implica que, los circuitos asociados a los sistemas basados en radio sean más complejos que los empleados en los sistemas ópticos de infrarrojo.

Las diferentes características de propagación de radio dan pie a cuatro esquemas de transmisión que se usan en las LAN inalámbricas de radio: Espectro disperso por secuencia directa, Espectro disperso por salto de frecuencia, Modulación por portadora única y Modulación de múltiples subportadoras.

- **INFRARROJO**

Los emisores y detectores de luz infrarroja se han utilizado desde hace muchos años en diversas aplicaciones, entre ellas los sistemas de transmisión por fibra óptica y diversas aplicaciones de control remoto como las que comprenden los televisores, los reproductores de CD y las videograbadoras. Las emisiones infrarrojas tienen frecuencias mucho más altas que las ondas de radio –mayores que 10^{14} Hz- y por lo regular los dispositivos se clasifican según la longitud de onda de la señal infrarroja transmitida y detectada más que por su frecuencia. La longitud de onda se mide en nanometros (nm) –1 nm = 10^{-9} m- y es la distancia que recorre la luz durante un solo ciclo de la señal.

Una ventaja del infrarrojo respecto a la radio es la ausencia de disposiciones que regulan su uso. Además, el infrarrojo tiene una longitud de onda similar a la de la luz visible y, por tanto, presenta un comportamiento similar; por ejemplo se refleja en superficies brillantes y pasa a través del vidrio, pero no de las paredes ni otros objetos opacos.

Hay varias formas para transmitir datos con una señal infrarroja; entre ellas tenemos: Modulación directa y Modulación de portadora.

1.3.1 MÉTODOS DE CONTROL DE ACCESO AL MEDIO

Tanto el radio como el infrarrojo operan en un medio de difusión, es decir, todas las transmisiones son recibidas por todos los receptores que están dentro del campo de cobertura del transmisor. En consecuencia, así como necesitamos recurrir a un método de MAC con las LAN por cable de medio compartido –CSMA/CD, testigo de control, etc.- para asegurarnos que sea un solo transmisor el que esté usando el medio, también se necesita un método de MAC con las LAN inalámbricas. Los esquemas que más se usan para ello son CDMA, CSMA/CD, CSMA/CA, TDMA y FDMA.

1.4 PROTOCOLOS

Las diversas normas de protocolo para las LAN, que se ocupan de las capas físicas y de enlace en el modelo de referencia de la ISO, son las definidas en IEEE 802. Esta norma define una familia de protocolos, cada uno de los cuales tiene que ver con un

tipo de método de MAC específico. En la figura 1.6. se ilustran las diversas normas IEEE y su relación con el modelo de referencia ISO.

Las tres normas de MAC junto con las especificaciones de medio físico correspondientes están contenidas en los siguientes tres documentos de normas del IEEE:

IEEE 802.3: Bus CSMA/CD

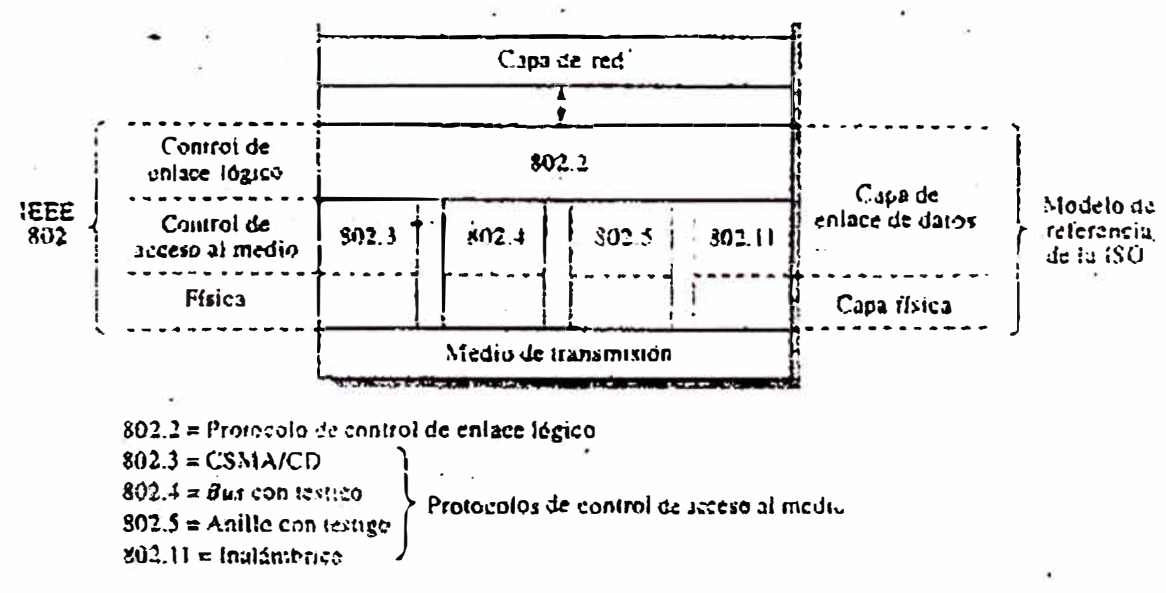
IEEE 802.4: Bus con testigo

IEEE 802.5: Anillo con testigo

IEEE 802.11: Inalámbrico

Las normas ISO pertinentes son las mismas, solo que se usa un 8 adicional: ISO 8802.3, etc.

Figura 1.6 : Conjunto de protocolos IEEE 802.



Las descripciones presentadas hasta ahora tienen que ver con las capas de MAC y físicas de estas cuatro normas. Aunque el funcionamiento interno de cada una es distinto, todas presentan un conjunto estándar de servicios a la capa de control de

enlace lógico (LLC), pensados para usarse junto con cualquiera de las normas de MAC básicas.

1.5 ETHERNET RÁPIDA

El objetivo de la Ethernet rápida es lograr que la velocidad se incremente en un orden de magnitud sobre la de la Ethernet 10 base T –IEEE 802.3-, pero conservando los mismos sistemas de cableado, el método de MAC y los formatos de trama.

La especificación IEEE 802.3 contempla una longitud de cable total –con repetidores- de 2.5 km. El peor retardo de programación de la señal es el tiempo que tarda una señal en programarse dos veces esta distancia. Según esta norma, el peor retardo de programación de la señal –incluyendo el retardo de los repetidores- es de 50 us, que es equivalente a 500 bits a 10 Mbps. A esto se agrega un margen de seguridad par producir un tamaño mínimo de 512 bits. Por supuesto, si se reduce esta longitud de cable mínima será aplicable el método de acceso CSMA CD con tasas de bits más altas. En ello se funda la norma de Ethernet rápida.

En la práctica, casi todas las instalaciones 10 base T requieren menos de 100m de cable para conectar al concentrador cada DTE. Ello significa que la distancia máxima entre dos DTE cualesquiera es de 200m, así que la peor longitud de camino, para fines de detección de colisiones, es de 400m. Desde luego, en estas condiciones es factible usar una tasa de bits más alta y seguirán siendo útiles el método de MAC CSMA/CD y el tamaño mínimo de trama de 512 bits. Como la norma establece una tasa de bits de 100 Mbps, también se le conoce como 100base T.

El principal problema con la Ethernet rápìda es como lograr una tasa de transferencia de datos de 100Mbps por 100m de cable de par trenzado no blindado (UTP). En la práctica, contamos con dos normas, una pensada para cables de grado de voz de categoría 3 y la otra para cables de par trenzado blindados (STP) de categoría 5, de más alta calidad, o bien con fibras ópticas. La primera se llama 100 base 4T, y la segunda, 100 base X.

A una tasa de transmisión de datos de 100 Mbps no es factible utilizar codificación de reloj –Manchester, por ejemplo- porque la tasa de reloj resultante sería demasiado alta y violaría el límite establecido para el cable UTP. En su lugar se emplean esquemas de codificación de bits, cuales aseguran que cada símbolo codificado contendrá suficientes transiciones y el receptor podrá mantener la sincronización de reloj.

Los esquemas de codificación en ambas normas se valen de uno o más grupos de cuatro bits de datos para formar cada símbolo codificado; por tanto, todas las transferencias de datos por la MII se realizan en nibbles o bocados de 4 bits. Las demás líneas de control se ocupan de la transferencia confiable de estos nibbles por la interfaz. Así, las funciones principales de la CS son: convertir los flujos de datos en serie transmitidos y recibidos en la interfaz de la subcapa de MAC en nibbles de 4 bits para transferirlos a través de la MII, y pasar a la subcapa de MAC las señales de detección de portadora y de detección de colisiones generadas por la subcapa PMD. Son diferentes las subcapas PMD con que las dos normas alcanzan una tasa de transmisión de datos de 100Mbps.

CAPÍTULO II

FRAME RELAY

General

Frame Relay constituye un método de comunicación orientado a paquetes para la conexión de sistemas informáticos. Se utiliza principalmente para la interconexión de redes de área local (LANs, Local Area Networks) y redes de área extensa (WANs, Wide Area Networks) sobre redes públicas o privadas. La mayoría de compañías públicas de telecomunicaciones ofrecen los servicios Frame Relay como una forma de establecer conexiones virtuales de área extensa que ofrezcan unas prestaciones relativamente altas.

En las redes que utilizan esta tecnología, las estaciones terminales comparten el medio de transmisión de la red de manera dinámica, así como el ancho de banda disponible.

Los paquetes de longitud variable se utilizan en transferencias más eficientes y flexibles. Posteriormente, estos paquetes se conmutan entre los diferentes segmentos de la red hasta que llegan a su destino. Las técnicas de multiplexaje estadístico controlan el acceso a la red en una red de conmutación de paquetes. La ventaja de esta técnica es que permite un uso más flexible y eficiente de ancho de banda. La

mayoría de las LAN más aceptadas en la actualidad, como Ethernet y Token Ring, son redes de conmutación de paquetes.

Aveces se describe a Frame Relay como una versión compacta de X.25 con menos características en cuanto a robustez, como el ventaneo y la retransmisión de los datos más recientes, que se ofrecen en X.25. Esto se debe a que Frame Relay normalmente opera a través de instalaciones WAN que ofrecen servicios de conexión más confiables y con un mayor grado de confiabilidad que las disponibles a finales de los años 70 e inicio de los 80, las cuales servían como plataformas habituales para las WANs X.25.

Frame Relay es un protocolo que opera en las capas físicas y de enlace de datos del modelo de referencia OSI, en tanto que X.25 también proporciona servicios de la capa de red (Capa 3, OSI). Por lo anterior, Frame Relay supera en desempeño y eficiencia de transmisión a X.25, y la tecnología Frame Relay resulta apropiada para las aplicaciones WAN actuales, como la interconexión LAN.

2.1 ESTANDARIZACIÓN DE FRAME RELAY

Frame Relay es una interfaz de usuario dentro de una red de conmutación de paquetes de área extensa, que típicamente ofrece un ancho de banda comprendida en el rango de 56 Kbps y 1.544 Mbps. Frame Relay se originó a partir de las interfaces de la Red Digital de Servicios Integrados (ISDN, Integrated Services Digital Network), la propuesta inicial para la estandarización de Frame Relay se presentó el CCITT (Comité Consultivo Internacional de Telefonía y Telegrafía) en 1984. Sin

embargo, por su falta de interoperabilidad y estandarización, Frame Relay no tuvo gran aceptación a finales de los 80.

En 1990 ocurrió un gran desarrollo en la historia de Frame Relay cuando las compañías Cisco, Digital Equipment, Northern Telecom y StrataCom formaron un consorcio para aplicarse al desarrollo de la tecnología Frame Relay. Dicho consorcio desarrolló una especificación que conformó el desarrollo básico de Frame Relay que se estaba analizando en el CCITT, pero ampliaba el protocolo con características que ofrecían facilidades adicionales en entornos complejos de interconectividad en redes. A estas extensiones de Frame Relay se les conoce en conjunto como LMI (Interfase de Administración Local).

Desde que la especificación del consorcio se desarrolló y publicó, muchos proveedores han anunciado su apoyo a esta definición extendida de Frame Relay. La ANSI (Instituto Nacional Americano de Estándares) y el CCIT estandarizaron, posteriormente sus propias variaciones a la especificación LMI original, y actualmente se utilizan dichas especificaciones estandarizadas con mayor frecuencia que la versión original.

En el ámbito internacional, la tecnología Frame Relay fue estandarizada por la ITU-T (Unión Internacional de Telecomunicaciones, Sector Telecomunicaciones). En Estados Unidos, Frame Relay es un estándar de ANSI.

2.2 DISPOSITIVOS FRAME RELAY

Las conexiones a una red Frame Relay requieren un encaminador y una línea desde las instalaciones del cliente hasta el puerto de entrada a Frame Relay en la compañía

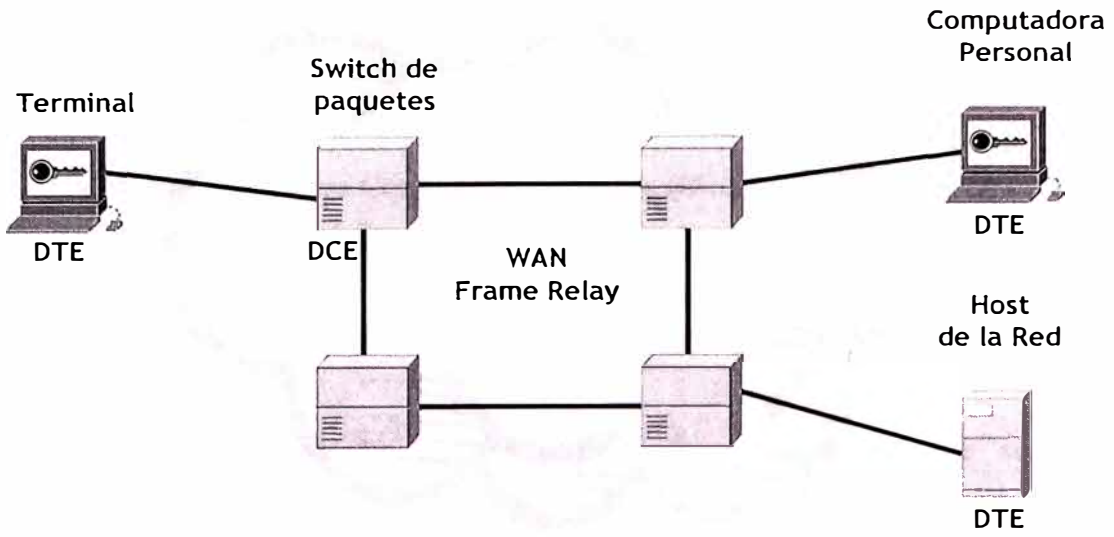
de telecomunicaciones. Los dispositivos conectados a una WAN Frame Relay caen dentro de una de dos categorías generales:

DTE (Equipo Terminal de Datos). Los DTEs, en general, se consideran equipo de terminal par una red específica y, por lo general, se localizan en las instalaciones de un cliente. De hecho, pueden ser propiedad del cliente. Algunos ejemplos de los dispositivos DTE son las terminales, computadoras personales, ruteadores y puentes.

DCE (Equipo Circuito Terminal de Datos). Los DCEs son dispositivos de interconectividad de redes propiedad de la compañía de larga distancia. El propósito del equipo DCE es proporcionar los servicios de temporización y conmutación en una red, que son en realidad los dispositivos que transmiten datos a través de la WAN. En la mayoría de los casos, éstos son switches de paquetes.

La conexión entre un dispositivo DTE y un DCE consta de un componente de la capa física y otro de la capa de enlace de datos. El componente físico define las especificaciones mecánicas, eléctricas y de procedimiento para la conexión entre dispositivos. Una de las especificaciones de interfase de la capa física que más se utiliza es la especificación del RS-232 (Estándar recomendado 232). El componente de la capa de enlace de datos define el protocolo que estable la conexión entre el dispositivo DTE, que puede ser un ruteador y el dispositivo DCE, que puede ser un switch. En este trabajo se examina una especificación de protocolo de uso común en las interredes WAN: el protocolo Frame Relay

Figura 2.1 : Dispositivos Frame Relay.



2.3 CIRCUITOS VIRTUALES FRAME RELAY

Frame Relay ofrece comunicación de la capa de enlaces de datos orientada a la conexión esto significa que hay una comunicación definida entre cada par de dispositivos y que estas conexiones están asociadas con el identificador de conexión. Este servicio se implementa por medio de un *circuito virtual Frame Relay*, que es una conexión lógica creada entre dos DTE a través de una PSN (Red de Commutación de Paquetes) Frame Relay.

Los circuitos Virtuales ofrecen una trayectoria de comunicación bidireccional de un dispositivo DTE a otro y se identifica de manera única por medio del DLCI (Identificador de Conexión de Enlace de Datos). Se puede multiplexar una gran cantidad de circuitos virtuales en un solo circuito físico para transmitirlos a través de la red. Con frecuencia esta característica permite conectar múltiples dispositivos DTE con menos equipo y una red compleja.

Un circuito virtual puede pasar por cualquier cantidad de dispositivos intermedios DCE (Switches) ubicados en la red Frame Relay PSN.

Los circuitos virtuales Frame Relay caen dentro de dos categorías:

SVCs (Circuitos Virtuales Conmutados) y PVCs (Circuitos Virtuales Permanentes).

2.3.1 CIRCUITOS VIRTUALES CONMUTADOS (SVC)

Son conexiones temporales que se utilizan en situaciones donde se requiere solamente de una trasferencia de datos esporádica entre los dispositivos DTE a través de la red Frame Relay. La operación de una sesión de comunicación a través de un SVC consta de cuatro estados:

Establecimiento de la llamada- Se establece el circuito virtual entre dos dispositivos DTE Frame Relay.

Transferencia de datos- Los datos se transmiten ente los dispositivos DTE a través del circuito virtual.

Ocioso- La conexión entre los dispositivos DTE aún está active, sin embargo no hay transferencia de datos. Si un SVC permanece en estado ocioso por un periodo definido de tiempo, la llamada puede darse por terminada.

Terminación de la llamada- Se da por terminado el circuito virtual entre los dispositivos DTE.

Una vez finalizado un circuito virtual los dispositivos DTE deben establecer un nuevo SVC si hay más datos que intercambiar. Se espera que los SVC se establezcan, conserven y finalicen utilizando los mismos protocolos de finalización que se usan en ISDN. Sin embargo, pocos fabricantes de equipo DCE Frame Relay

soportan SVCs. Por lo tanto, su utilización real es mínima en las redes Frame Relay actuales.

2.3.2 CIRCUITOS VIRTUALES PERMANENTES (PVC)

Son conexiones establecidas en forma permanente, que se utilizan en transferencia de datos frecuentes y constantes entre dispositivos DTE a través de la red Frame Relay. La comunicación a través de un PVC no requiere los estados de establecimiento de llamada y finalización que se utilizan con los SVCs.

Los PVCs siempre operan en alguno de los estados siguiente:

Transferencia de datos- Los datos se transmiten entre los dispositivos DTE a través del circuito virtual.

Ocioso- Ocurre cuando la conexión entre los dispositivos DTE está activa, pero no hay transferencia de datos. A diferencia de los SVCs los PVCs no se darán por finalizados en ninguna circunstancia ya que se encuentran en estado ocioso.

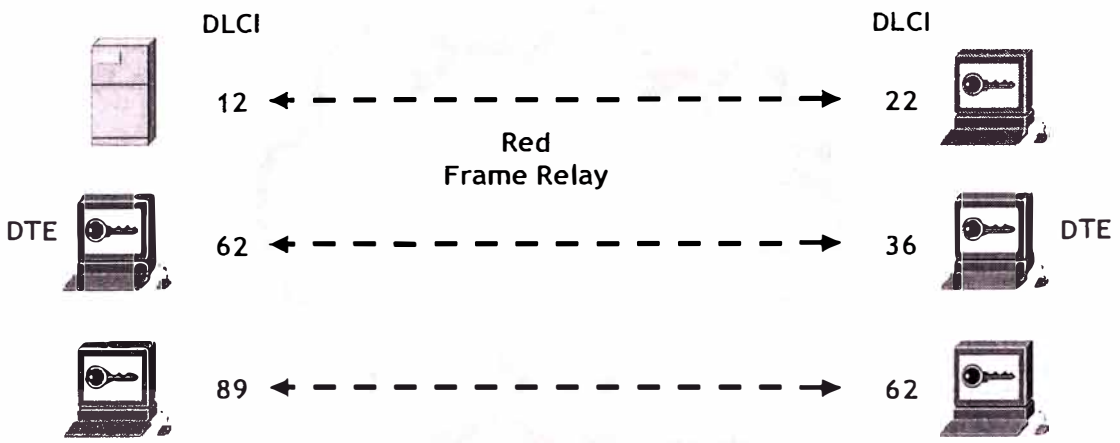
Los dispositivos DTE pueden comenzar la transferencia de datos en cuanto estén listos, pues el circuito está establecido de manera permanente.

2.3.3 IDENTIFICADOR DE CONEXION DE ENLACE DE DATOS (DLCI)

Los circuitos virtuales de Frame Relay se identifican a través de los DLCIs. Normalmente los valores de DLCI son asignados por el proveedor de los servicios de Frame Relay (por ejemplo, la compañía Telefónica). Los DLCIs Frame Relay tiene un significado local, lo que significa que su valor es único en la LAN, pero no

necesariamente en la WAN Frame Relay. La figura 2.2, muestra como a dos dispositivos DTE diferentes se les puede asignar el mismo valor de DLCI dentro de una WAN Frame Relay.

Figura 2.2 : Asignación de valores DLCI



2.4 MECANISMOS DE CONTROL DE CONGESTIÓN

Frame Relay reduce el gasto indirecto de la red, implementando mecanismos simples de notificación de congestión, en vez de un control de flujo explícito por circuito virtual. En general Frame Relay se implementa sobre medios de transmisión de red confiables para no sacrificar la integridad de los datos, ya que el control de flujo se puede realizar por medio de los protocolos de las capas superiores. La tecnología Frame Relay implementa dos mecanismos de notificación de congestión:

FECN (Notificación de Congestión Explícita Hacia Adelante)

BECN (Notificación de Congestión Explícita Hacia Atrás)

Tanto FECN como BECN son controlados por un solo bit incluido en el encabezado de la trama Frame Relay. Este también contiene un bit DE (Elegibilidad para descarte), que se utiliza para identificar el tráfico menos importante que se puede eliminar durante períodos de congestión.

El bit FECN es parte del campo de direcciones del encabezado de la trama Frame Relay. El mecanismo FECN se inicia en el momento que un dispositivo DTE envía tramas Frame Relay a la red. Si la red esta congestionada, los dispositivos DCE (switches) fijan el valor de los bits FECN de las tramas en 1. Cuando las tramas llegan al dispositivo DTE destino, el campo de direcciones (con el bit FECN en 1) indica que la trama se saturó en su trayectoria del origen al destino. El dispositivo DTE puede enviar esta información a un protocolo de las capas superiores para su procesamiento. Dependiendo de la implementación, el control de flujo puede iniciarse o bien la indicación puede ser ignorada.

El bit BECN es parte del campo de direcciones del encabezado de la trama Frame Relay. Los dispositivos DCE fijan el valor del bit BECN en 1 en las tramas que viajan en sentido opuesto a las tramas con el bit FECN igual a 1. Esto informa al dispositivo DTE receptor que una trayectoria específica en la red está congestionada. El dispositivo DTE puede enviar esta información a un protocolo de las capas superiores para su procesamiento. Dependiendo de la implementación, el control de flujo puede iniciarse o bien se puede ignorar la indicación.

2.4.1 ELIGIBILIDAD DE DESCARTES EN FRAME RELAY

El bit de Elegibilidad de Descarte (DE) se utiliza para indicar que una trama tiene una importancia menor que otras. El bit DE es parte del campo de Direcciones del encabezado de la trama Frame Relay.

Los dispositivos DTE pueden fijar el valor del bit DE de una trama en 1 para indicar que esta tiene una importancia menor respecto a las demás tramas. Al iniciarse la congestión de la red los dispositivos DCE descartaran las tramas con el bit DE fijado en 1 antes de descartar aquellas que no las tienen. Con lo anterior se disminuye la probabilidad de que los dispositivos DCE de Frame Relay eliminen datos críticos durante los períodos de congestión.

2.4.2 VERIFICACIÓN DE ERRORES EN FRAME RELAY

Frame Relay utiliza un mecanismo para la verificación de errores conocido como CRC (Verificación de Redundancia cíclica). La CRC compara dos valores calculados para determinar si se ha presentado errores durante la transmisión del origen al destino. Frame Relay disminuye el gasto indirecto al implementarse la verificación de errores en lugar de su corrección. Frame Relay por lo general se implementa en medios confiables de transmisión de red, por eso la integridad de los datos no se sacrifica debido a que la corrección de error se deja a los protocolos de las capas superiores que operan en la parte mas alta de Frame Relay

2.5 INTERFASE DE ADMINISTRACIÓN LOCAL EN FRAME RELAY

La Interfase de la Administración Local (LMI) es un conjunto de avances a la especificación básica de Frame Relay. LMI fue desarrollada en 1990 por Cisco Systems, StrataCom, Northern Telecom y Digital Equipment Corporation. Presenta varias características (llamadas extensiones) para la administración de interredes complejas. Entre las extensiones LMI más importantes de Frame Relay están el direccionamiento Global, los mensajes de estados de los circuitos virtuales y la multidifusión.

La extensión de direccionamiento global LMI otorga los valores al DLCI Frame Relay con un significado global mas que local. Los valores DLCI se convierten en direcciones DTE únicas en la WAN Frame Relay. La extensión global de direccionamiento agrega funcionalidad y buena administración a las interredes Frame Relay; por ejemplo, las interfaces de red individuales y los nodos terminales conectados a ellos se pueden intensificar por medio de técnicas estándar de descubrimiento y resolución de direcciones. Además, para los ruteadores ubicados en su periferia, toda la red Frame Relay aparece como una típica LAN.

Los mensajes de estados de los circuitos virtuales LMI permiten la comunicación y sincronización entre los dispositivos DTE y DCE Frame Relay. Estos mensajes se utilizan para reportar, de manera periódica, el estado de los PVCs, así se previene el envío de datos a agujeros negros (esto es, a través de los PVCs inexistentes).

La extensión de LMI para multidifusión permite que se asignen grupos de multidifusión. Con la multidifusión se ahorra ancho de banda, ya que permite que los

mensajes sobre la resolución de direcciones y de actualizaciones de ruteo sean enviados solamente a grupos específicos de ruteadores. La extensión también transmite reportes sobre el estado de los grupos de multidifusión en los mensajes de actualización.

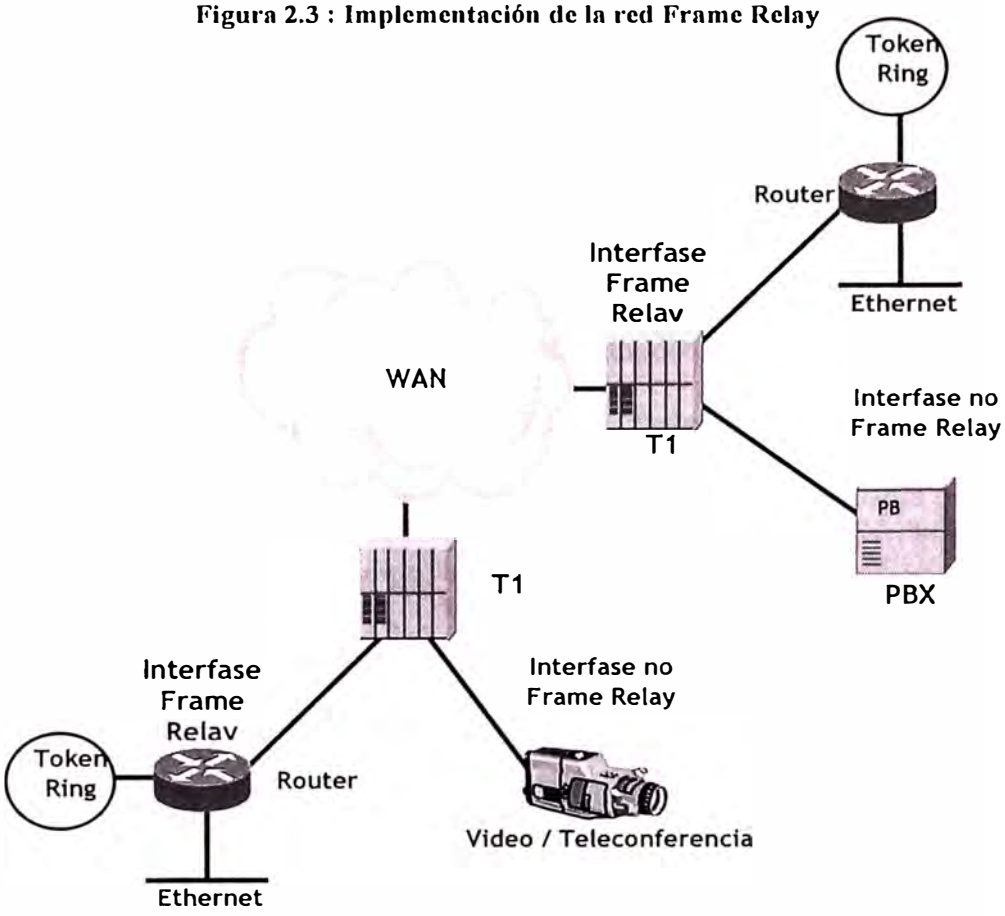
2.6 IMPLEMENTACIÓN DE LA RED FRAME RELAY

Una implementación habitual y privada de red Frame Relay consiste en equipar un multiplexor T1 con interfaces Frame Relay e interfaces que no sean Frame Relay. El tráfico de Frame Relay es enviado fuera de la interface Frame Relay y hacia la red de datos. El tráfico que no es de Frame Relay se direcciona hacia la aplicación o los servicios adecuados, como una PBX (Central Privada de Intercambio) de servicio telefónico o una aplicación de video conferencia, como se muestra en la figura 2.3.

Una Red Frame Relay típica consta de varios dispositivos DTE, como los ruteadores, conectados hacia los puertos remotos de un equipo multiplexor vía servicios tradicionales punto a punto como T1, T1 fraccional o circuitos de 56K.

La mayoría de las redes Frame Relay que se utilizan en la actualidad son equipadas por los proveedores de servicios que ofrecen los servicios de transmisión a clientes. A esto se le conoce como un servicio público de Frame Relay, pues Frame Relay se implementa tanto en las redes públicas ofrecidas por las compañías de larga distancia, como en las redes privadas empresariales.

Figura 2.3 : Implementación de la red Frame Relay



2.6.1 REDES PÚBLICAS DE LARGA DISTANCIA

En las redes públicas Frame Relay de larga distancia, el equipo de conmutación Frame Relay se ubica en las oficinas centrales de las compañías de larga distancia. A los suscriptores se les cobra determinada cantidad según el uso que hagan de la red, pero se les libera de la administración y mantenimiento de los equipos y servicios de la red Frame Relay.

Generalmente, el equipo DCE es propiedad del proveedor del servicio de telecomunicaciones. El equipo DCE puede ser propiedad del cliente, o bien del proveedor del servicio de telecomunicaciones como un servicio para el usuario.

Actualmente la mayoría de las redes Frame Relay son redes públicas que suministran servicios de larga distancia.

2.6.2 REDES PRIVADAS EMPRESARIALES

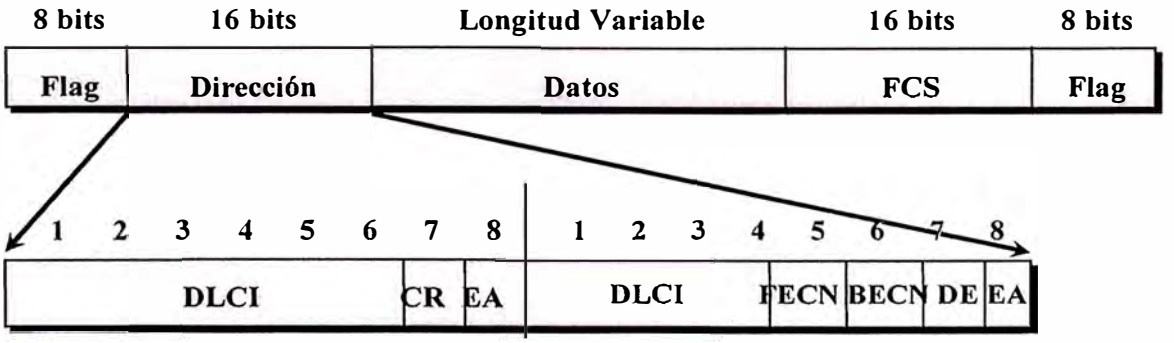
Las organizaciones a nivel mundial están utilizando cada vez más redes privadas Frame Relay. En las redes privadas Frame Relay, la administración y el mantenimiento de la red son responsabilidad de la empresa (o compañía privada). El cliente es el dueño de todo el equipo, incluyendo el de conmutación

2.7 FORMATOS DE LA TRAMA FRAME RELAY

Para entender mejor la funcionalidad de Frame Relay, ayuda mucho conocer la estructura de la trama de la tecnología Frame Relay, por ello presentamos el formato básico y la versión LMI de la trama Frame Relay.

- **TRAMA ESTÁNDAR FRAME RELAY**

Figura 2.4 : Campos de la trama estándar Frame Relay



La siguiente descripción resume los campos de la trama estándar Frame Relay, ilustrado en la figura 2.4.

Indicadores (Flags): Delimitan el comienzo y la terminación de la trama. El valor de este campo es siempre el mismo y se representa con el número hexadecimal 7E o el número binario 01111110.

Direcciones: Contiene la siguiente información

- **DLCI**: El DLCI de 10 bits es la esencia del encabezado de Frame Relay. Este valor representa la conexión virtual entre el dispositivo DTE y el switch. Cada conexión virtual que se multiplexe en el canal físico será representada por un DLCI único. Los valores del DLCI tienen solamente un significado local, lo que indica que son únicos para el canal físico en que residen; por lo tanto, los dispositivos que se encuentran en los extremos opuestos de una conexión pueden utilizar diferentes valores DLCI para hacer referencia a la misma conexión virtual.
- **Dirección extendida (EA)**: La EA se utiliza para indicar si el byte cuyo valor EA es 1, es el último campo de direccionamiento. Si el valor es 1, entonces se determina que este byte es el último octeto DLCI. Aunque todas las implementaciones actuales de Frame Relay utilizan un DLCI de dos octetos, esta característica permitirá que en el futuro se utilicen DLCIs más largos. El octavo bit de cada byte del campo de direcciones se utiliza para indicar el EA.
- **C/R**: El C/R es el bit que sigue al byte DLCI más significativo en el campo de direcciones. El bit C/R no está definido hasta el momento.

- **Control de Congestión**: Consta de 3 bits que controlan los mecanismos de notificación de congestión en Frame Relay. Estos son los bits FECN, BECN y DE, que son los últimos 3 bits en el campo de direcciones.
- **Notificación de Congestión Explícita Hacia delante (FECN)**: Es un campo de un solo bit que puede fijarse al valor de 1 por el switch para indicar a un dispositivo DTE terminal, como un ruteador, que ha habido congestión en la dirección de la transmisión de la trama desde el origen al destino. La ventaja principal de usar los campos FECN y BECN es la habilidad que tienen los protocolos de las capas superiores de reaccionar de manera inteligente ante estos indicadores de congestión. Hoy en día, los protocolos DECnet y OSI son los únicos protocolos de las capas superiores que implementan estas características.
- **Notificación de Congestión Explícita Hacia Atrás (BECN)**: Es un campo de un solo bit que, al ser establecido al valor de 1 por un switch, indica que la congestión experimentada en la red está en la dirección opuesta a la transmisión de la trama desde el origen al destino.
- **Elegibilidad para Descartes (DE)**: Este bit es fijado por el dispositivo DTE, como un ruteador, para indicar que la trama marcada es de menor importancia en relación con las otras tramas que se transmiten. Las tramas marcadas como "elegible para descartes" serán descartadas antes que cualquier otra trama en una red congestionada. Lo anterior representa un mecanismo básico de establecimiento de prioridad en las redes Frame Relay.

Datos: Contienen información encapsulada de las capas superiores. Cada trama en este campo de longitud variable incluye un campo de datos de usuario o carga útil

que varía en longitud y podrá tener hasta 16,000 bytes. Este campo sirve para transportar paquetes de protocolo de las capas superiores (PDU) a través de una red Frame Relay.

Secuencia de verificación de tramas (FCS): Asegura la integridad de los datos transmitidos. Este valor es calculado por el dispositivo de origen y verificado por el receptor para asegurar la integridad de la transmisión.

- **FORMATO DE LA TRAMA LMI**

Figura 2.5 : Campos de la trama LMI

Flag	LMI DLCI	Indicador de información no numerada	Discriminador de protocolos	Referencia de llamada	Tipo de mensaje	Elemento de información	FCS	Flag

La siguiente descripción resume los campos ilustrados en la figura 2.5.

Indicadores (Flags): Delimitan el comienzo y la terminación de la trama.

LMI DLCI: Identifica la trama como una trama LMI en vez de una trama básica Frame Relay. El valor DLCI específico del LMI definido por la especificación del consorcio LMI es DLCI = 1023.

Indicador de la información no numerada: Fija el bit sondeo/final en cero.

Discriminador de protocolos: Siempre contiene un valor que indica que es una trama LMI.

Referencia de llamada: Siempre contiene ceros. En la actualidad este campo no se usa ni tiene ningún propósito.

Tipo de mensaje: Etiqueta la trama con uno de los siguientes tipos de mensaje:

Mensaje de solicitud de status: Permite que un dispositivo de usuario solicite el status de la red

Mensaje de status: Responde a los mensajes de solicitud de status. Los mensajes de status incluyen mensajes de sobrevivencia y de status del PVC.

Elementos de información: Contiene una cantidad variable de IEs (Elementos Individuales de Información). Los IEs constan de los campos siguientes:

Identificador IE: Identifica de manera única el IE

Longitud del IE: Indica la longitud del IE

Datos: Consta de uno o más bytes que contienen datos encapsulados de las capas superiores.

FCS (secuencia de la Verificación de Tramas): Asegura la integridad de los datos transmitidos.

CAPÍTULO III

INTERCONECTIVIDAD DE RED FRAME RELAY

3.1 INTERCONEXIÓN DE REDES

Cuando se diseña una red de datos se desea sacar el máximo rendimiento de sus capacidades. Para conseguir esto, la red debe estar preparada para efectuar conexiones a través de otras redes, sin importar qué características posean.

El objetivo de la Interconexión de Redes (***internetworking***) es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías de forma transparente para el usuario. Este concepto hace que las cuestiones técnicas particulares de cada red puedan ser ignoradas al diseñar las aplicaciones que utilizarán los usuarios de los servicios.

Los dispositivos de interconexión de redes sirven para superar las limitaciones físicas de los elementos básicos de una red, extendiendo las topologías de esta.

Algunas de las ventajas que plantea la interconexión de redes de datos, son:

Compartición de recursos dispersos.

Coordinación de tareas de diversos grupos de trabajo.

Reducción de costos, al utilizar recursos de otras redes.

Aumento de la cobertura geográfica.

3.1.1 FUNCIONES BÁSICAS

Para superar las limitaciones físicas de los elementos básicos de una red, existen dispositivos cuyas funciones son las de extender las topologías de red. Estos elementos son: concentradores o *hubs*, repetidores, *bridges* o puentes, *routers* o encaminadores y *gateways* o pasarelas.

Los dispositivos de interconexión de redes proporcionan algunas de (o todas) las siguientes funciones básicas:

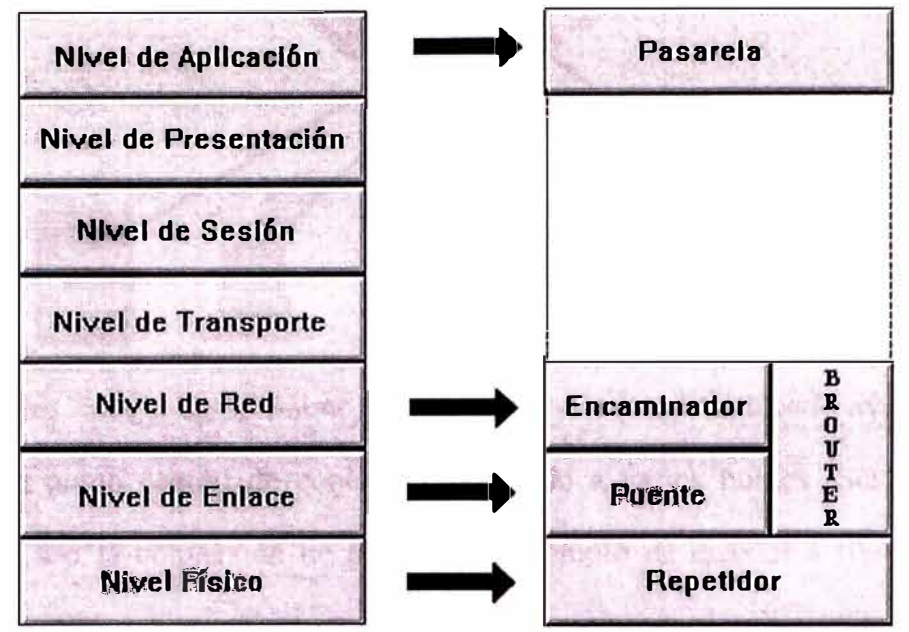
Extensión de la red : Permiten ampliar el rango de distancia que puede alcanzar una red.

Definición de segmentos dentro de la red : Al dividir la red en segmentos se consigue aumentar las prestaciones de la red ya que cada tramo soporta sólo su propio tráfico y no los de los otros segmentos.

Separación entre redes : Mediante estos dispositivos las grandes redes se pueden componer de otras más pequeñas interconectadas entre sí, de forma transparente para el usuario. Varias redes físicas pueden combinarse para formar una única red lógica.

En la figura 3.1 se representa la relación de los dispositivos de interconexión con los niveles del modelo de referencia OSI.

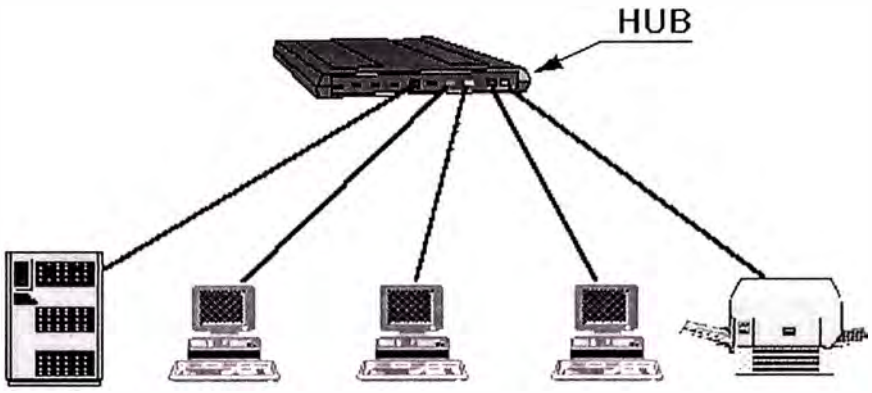
Figura 3.1 : Relación entre OSI y los dispositivos de interconexión



3.1.2 CONCENTRADORES (HUBS)

El término concentrador o *hub* describe la manera en que las conexiones de cableado de cada nodo de una red se centralizan y conectan en un único dispositivo. Se suele aplicar a concentradores Ethernet, TokenRing y FDDI (*Fiber Distributed Data Interface)* soportando módulos individuales que concentran múltiples tipos de funciones en un solo dispositivo. Normalmente los concentradores incluyen ranuras para aceptar varios módulos y un panel trasero común para funciones de encaminamiento, filtrado y conexión a diferentes medios de transmisión (por ejemplo Ethernet y TokenRing).

Figura 3.2 : Concentrador o HUB



Los primeros *hubs* o de "primera generación" son cajas de cableado avanzadas que ofrecen un punto central de conexión conectado a varios puntos. Sus principales beneficios son la conversión de medio (por ejemplo de coaxial a fibra óptica), y algunas funciones de gestión bastante primitivas como particionamiento automático cuando se detecta un problema en un segmento determinado.

Los *hubs* inteligentes de "segunda generación" basan su potencial en las posibilidades de gestión ofrecidas por las topologías radiales (TokenRing y Ethernet). Tiene la capacidad de gestión, supervisión y control remoto, dando a los gestores de la red la oportunidad de ofrecer un período mayor de funcionamiento de la red gracias a la aceleración del diagnóstico y solución de problemas. Sin embargo tienen limitaciones cuando se intentan emplear como herramienta universal de configuración y gestión de arquitecturas complejas y heterogéneas.

Los nuevos *hubs* de "tercera generación" ofrecen proceso basado en arquitectura RISC (*Reduced Instructions Set Computer*) junto con múltiples placas de alta velocidad. Estas placas están formadas por varios buses independientes Ethernet, TokenRing, FDDI y de gestión, lo que elimina la saturación de tráfico de los actuales productos de segunda generación.

A un *hub* Ethernet se le denomina "repetidor multipuerta". El dispositivo repite simultáneamente la señal a múltiples cables conectados en cada uno de los puertos del *hub*. En el otro extremo de cada cable está un nodo de la red, por ejemplo un ordenador personal. Un *hub* Ethernet se convierte en un *hub* inteligente (*smart hub*) cuando puede soportar inteligencia añadida para realizar monitorización y funciones de control.

Los concentradores inteligentes (*smart hub*) permiten a los usuarios dividir la red en segmentos de fácil detección de errores a la vez que proporcionan una estructura de crecimiento ordenado de la red. La capacidad de gestión remota de los *hubs* inteligentes hace posible el diagnóstico remoto de un problema y aísla un punto con problemas del resto de la LAN, con lo que otros usuarios no se ven afectados.

El tipo de *hub* Ethernet más popular es el *hub* 10BaseT. En este sistema la señal llega a través de cables de par trenzado a una de las puertas, siendo regenerada eléctricamente y enviada a las demás salidas. Este elemento también se encarga de desconectar las salidas cuando se produce una situación de error.

A un *hub* TokenRing se le denomina Unidad de Acceso Multiestación (MAU, *Multiestation Access Unit*). Las MAUs se diferencian de los *hubs* Ethernet porque las primeras repiten la señal de datos únicamente a la siguiente estación en el anillo y no a todos los nodos conectados a ella como hace un *hub* Ethernet. Las MAUs pasivas no tienen inteligencia, son simplemente retransmisores. Las MAUs activas no sólo repiten la señal, además la amplifican y regeneran. Las MAUs inteligentes detectan errores y activan procedimientos para recuperarse de ellos.

3.1.3 REPETIDORES

El repetidor es un elemento que permite la conexión de dos tramos de red, teniendo como función principal regenerar eléctricamente la señal, para permitir alcanzar distancias mayores manteniendo el mismo nivel de la señal a lo largo de la red. De esta forma se puede extender, teóricamente, la longitud de la red hasta el infinito.

Un repetidor interconecta múltiples segmentos de red en el nivel físico del modelo de referencia OSI. Por esto sólo se pueden utilizar para unir dos redes que tengan los mismos protocolos de nivel físico.

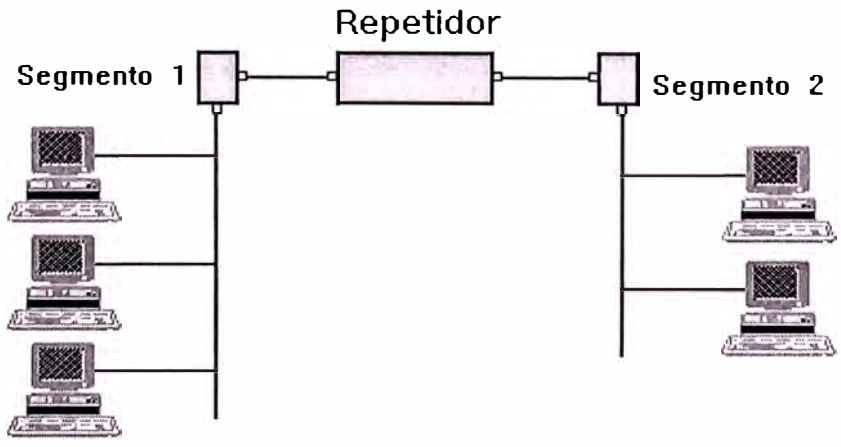
Los repetidores no discriminan entre los paquetes generados en un segmento y los que son generados en otro segmento, por lo que los paquetes llegan a todos los nodos de la red. Debido a esto existen más riesgos de colisión y más posibilidades de congestión de la red.

Se pueden clasificar en dos **tipos**:

Locales: cuando enlazan redes próximas.

Remotos: cuando las redes están alejadas y se necesita un medio intermedio de comunicación.

Figura 3.3 : Ejemplo de la utilización de un repetidor



Normalmente la utilización de repetidores está limitada por la distancia máxima de la red y el tamaño máximo de cada uno de los segmentos de red conectados. En las redes Ethernet, por problemas de gestión de tráfico en la red, no deben existir más de dos repetidores entre dos equipos terminales de datos, lo que limita la distancia máxima entre los nodos más lejanos de la red a 1.500 m. (enlazando con dos repetidores tres segmentos de máxima longitud, 500 m).

Ventajas:

Incrementa la distancia cubierta por la LAN

Retransmite los datos sin retardos.

Es transparente a los niveles superiores al físico.

Desventajas:

Incrementa la carga en los segmentos que interconecta.

Los repetidores son utilizados para interconectar LANs que estén muy próximas, cuando se quiere una extensión física de la red. La tendencia actual es dotar de más inteligencia y flexibilidad a los repetidores, de tal forma que ofrezcan capacidad de gestión y soporte de múltiples medios físicos, como Ethernet sobre par trenzado (10BaseT), ThickEthernet (10Base5), ThinEthernet (10Base2), TokenRing, fibra óptica, etc.

3.1.4 PUENTES (BRIDGES)

Son elementos inteligentes, constituidos como nodos de la red, que conectan entre sí dos subredes, transmitiendo de una a otra el tráfico generado no local. Al distinguir los tráficos locales y no locales, estos elementos disminuyen el mínimo total de

paquetes circulando por la red por lo que, en general, habrá menos colisiones y resultará más difícil llegar a la congestión de la red.

Operan en el Nivel de Enlace del modelo de referencia OSI, en el nivel de trama MAC (*Medium Access Control*, Control de Acceso al Medio) y se utilizan para conectar o extender redes similares, es decir redes que tienen protocolos idénticos en los dos niveles inferiores OSI, (como es TokenRing con TokenRing, Ethernet con Ethernet, etc) y conexiones a redes de área extensa.

Se encargan de filtrar el tráfico que pasa de una a otra red según la dirección de destino y una tabla que relaciona las direcciones y la red en que se encuentran las estaciones asignadas.

Las redes conectadas a través de *bridge* aparentan ser una única red, ya que realizan su función transparentemente; es decir, las estaciones no necesitan conocer la existencia de estos dispositivos, ni siquiera si una estación pertenece a uno u otro segmento.

Un *bridge* ejecuta tres **tareas básicas**:

Aprendizaje de las direcciones de nodos en cada red.

Filtrado de las tramas destinadas a la red local.

Envío de las tramas destinadas a la red remota.

Se distinguen dos **tipos** de *bridge*:

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.

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* está en soluciones de interconexión de LANs 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.

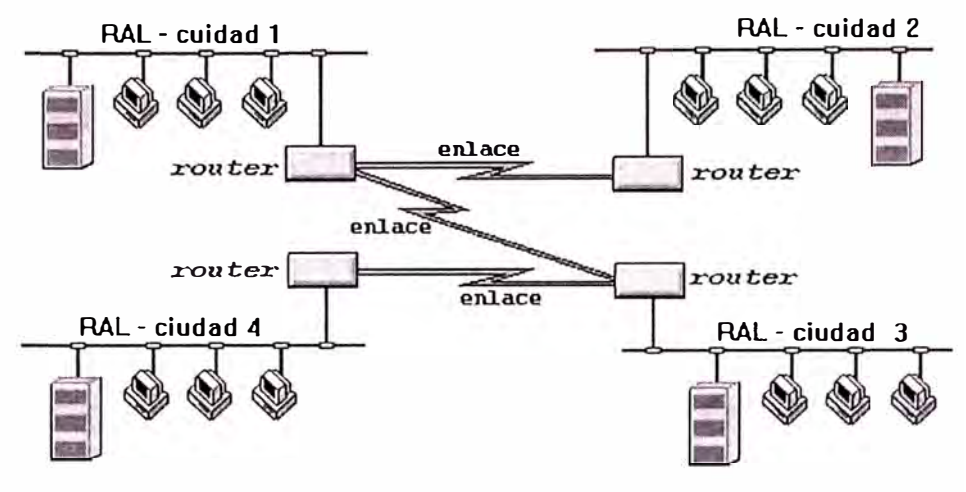
3.1.5 ENCAMINADORES (ROUTERS)

Son dispositivos inteligentes que trabajan en el Nivel de Red del modelo de referencia OSI, por lo que son dependientes del protocolo particular de cada red. Envían paquetes de datos de un protocolo común, desde una red a otra.

Convierten los paquetes de información de la red de área local, en paquetes capaces de ser enviados mediante redes de área extensa. Durante el envío, el encaminador examina el paquete buscando la dirección de destino y consultando su propia tabla de direcciones, la cual mantiene actualizada intercambiando direcciones con los demás *routers* para establecer rutas de enlace a través de las redes que los interconectan.

Este intercambio de información entre *routers* se realiza mediante protocolos de gestión propietarios.

Figura 3.4 : Routers o encaminadores



Los encaminadores se pueden clasificar dependiendo de varios criterios:

En función del **área**:

Locales: Sirven para interconectar dos redes por conexión directa de los medios físicos de ambas al *router*.

De área extensa: Enlazan redes distantes.

En función de la forma de actualizar las tablas de encaminamiento (***routing***):

Estáticos: La actualización de las tablas es manual.

Dinámicos: La actualización de las tablas las realiza el propio *router* automáticamente.

En función de los **protocolos** que soportan:

IPX, TCP/IP , DECnet, AppleTalk, XNS, OSI, X.25, etc.

En función del **protocolo de encaminamiento** que utilicen:

Routing Information Protocol **(RIP)**

Permite comunicar diferentes sistemas que pertenezcan a la misma red lógica. Tienen tablas de encaminamiento dinámicas y se intercambian información según la necesitan. Las tablas contienen por dónde ir hacia los diferentes destinos y el número de saltos que se tienen que realizar. Esta técnica permite 14 saltos como máximo.

Exterior Gateway Protocol (EGP)

Este protocolo permite conectar dos sistemas autónomos que intercambien mensajes de actualización. Se realiza un sondeo entre los diferentes *routers* para encontrar el destino solicitado. Este protocolo sólo se utiliza para establecer un camino origen-destino; no funciona como el RIP determinando el número de saltos.

***Open Shortest Path First Routing* (OSPF)**

Está diseñado para minimizar el tráfico de encaminamiento, permitiendo una total autentificación de los mensajes que se envían. Cada encaminador tiene una copia de la topología de la red y todas las copias son idénticas. Cada encaminador distribuye la información a su encaminador adyacente. Cada equipo construye un árbol de encaminamiento independientemente.

IS-IS

Encaminamiento OSI según las normativas: ISO 9575, ISO 9542 e ISO 10589. El concepto fundamental es la definición de encaminamiento en un dominio y entre diferentes dominios. Dentro de un mismo dominio el encaminamiento se realiza aplicando la técnica de menor coste. Entre diferentes dominios se consideran otros aspectos como puede ser la seguridad.

Otras variantes de los *routers* son:

***Router* Multiprotocolo**

Tienen la posibilidad de soportar tramas con diferentes protocolos de Nivel de Red de forma simultánea, encaminándolas dinámicamente al destino especificado, a través de la ruta de menor coste o más rápida. Son los *routers* de segunda generación. No es necesario, por tanto, tener un *router* por cada protocolo de alto nivel existente en el conjunto de redes interconectadas. Esto supone una reducción de gastos de equipamiento cuando son varios los protocolos en la red global.

Brouter (*bridging router*)

Son *routers* multiprotocolo con facilidad de *bridge*. Funcionan como *router* para protocolos encaminables y, para aquellos que no lo son se comportan como *bridge*, transfiriendo los paquetes de forma transparente según las tablas de asignación de direcciones.

Operan tanto en el Nivel de Enlace como en el Nivel de Red del modelo de referencia OSI. Por ejemplo, un Brouter puede soportar protocolos de encaminamiento además de ***source routing*** y ***spanning tree bridging***. El *Brouter* funciona como un *router* multiprotocolo, pero si encuentra un protocolo para el que no puede encaminar, entonces simplemente opera como *bridge*.

Las características y costes de los *Brouter*, hacen de estos la solución más apropiada para el problema de interconexión de redes complejas. Ofrecen la mayor flexibilidad en entornos de interconexión complejos, que requieran soporte multiprotocolo, ***source routing*** y ***spanning tree*** e incluso de

protocolos no encaminables. Son aconsejables en situaciones mixtas ***bridge/router***. Ofrecen la mayor flexibilidad en entornos de interconexión complejos, que requieran soporte multiprotocolo.

Trouter

Es una combinación entre un *router* y servidor de terminales. Permite a pequeños grupos de trabajo la posibilidad de conectarse a LANs, WANs, modems, impresoras, y otros ordenadores sin tener que comprar un servidor de terminales y un *router*. El problema que presenta este dispositivo es que al integrar las funcionalidades de *router* y de servidor de terminales puede ocasionar una degradación en el tiempo de respuesta.

Ventajas de los *routers*:

- **Seguridad**. Permiten el aislamiento de tráfico, y los mecanismos de encaminamiento facilitan el proceso de localización de fallos en la red.
- **Flexibilidad**. Las redes interconectadas con *router* no están limitadas en su topología, siendo estas redes de mayor extensión y más complejas que las redes enlazadas con *bridge*.
- **Soporte de Protocolos**. Son dependientes de los protocolos utilizados, aprovechando de una forma eficiente la información de cabecera de los paquetes de red.
- **Relación Precio / Eficiencia**. El coste es superior al de otros dispositivos, en términos de precio de compra, pero no en términos de explotación y mantenimiento para redes de una complejidad mayor.
- **Control de Flujo y Encaminamiento**. Utilizan algoritmos de encaminamiento adaptativos (RIP, OSPF, etc), que gestionan la congestión

del tráfico con un control de flujo que redirige hacia rutas alternativas menos congestionadas.

Desventajas de los *routers*:

- Lentitud de proceso de paquetes respecto a los bridges.
- Necesidad de gestionar el subdireccionamiento en el Nivel de Enlace.
- Precio superior a los *bridges*.

Por su posibilidad de segregar tráfico administrativo y determinar las rutas más eficientes para evitar congestión de red, son una excelente solución para una gran interconexión de redes con múltiples tipos de LANs, MANs, WANs y diferentes protocolos. Es una buena solución en redes de complejidad media, para separar diferentes redes lógicas, por razones de seguridad y optimización de las rutas.

3.1.6 PASARELAS (GATEWAYS)

Estos dispositivos están pensados para facilitar el acceso entre sistemas o entornos soportando diferentes protocolos. Operan en los niveles más altos del modelo de referencia OSI (Nivel de Transporte, Sesión, Presentación y Aplicación) y realizan conversión de protocolos para la interconexión de redes con protocolos de alto nivel diferentes.

Los *gateways* incluyen los 7 niveles del modelo de referencia OSI, y aunque son más caros que un *bridge* o un *router*, se pueden utilizar como dispositivos universales en una red corporativa compuesta por un gran número de redes de diferentes tipos.

Los *gateways* tienen mayores capacidades que los *routers* y los *bridges* porque no sólo conectan redes de diferentes tipos, sino que también aseguran que los datos de

una red que transportan son compatibles con los de la otra red. Conectan redes de diferentes arquitecturas procesando sus protocolos y permitiendo que los dispositivos de un tipo de red puedan comunicarse con otros dispositivos de otro tipo de red.

A continuación se describen algunos tipos de *gateways*:

***Gateway* asíncrono**

Sistema que permite a los usuarios de ordenadores personales acceder a grandes ordenadores (*mainframes*) asíncronos a través de un servidor de comunicaciones, utilizando líneas telefónicas conmutadas o punto a punto. Generalmente están diseñados para una infraestructura de transporte muy concreta, por lo que son dependientes de la red.

***Gateway* SNA**

Permite la conexión a grandes ordenadores con arquitectura de comunicaciones SNA *(System Network Architecture*, Arquitectura de Sistemas de Red), actuando como terminales y pudiendo transferir ficheros o listados de impresión.

***Gateway* TCP/IP**

Estos gateways proporcionan servicios de comunicaciones con el exterior vía LAN o WAN y también funcionan como interfaz de cliente proporcionando los servicios de aplicación estándares de TCP/IP.

***Gateway* PAD X.25**

Son similares a los asíncronos; la diferencia está en que se accede a los servicios a través de redes de conmutación de paquetes X.25.

***Gateway* FAX**

Los servidores de Fax proporcionan la posibilidad de enviar y recibir documentos de fax.

Ventajas:

- Simplifican la gestión de red.
- Permiten la conversión de protocolos.

Desventajas:

- Su gran capacidad se traduce en un alto precio de los equipos.
- La función de conversión de protocolos impone una sustancial sobrecarga en el Gateway, la cual se traduce en un relativo bajo rendimiento. Debido a esto, un *Gateway* puede ser un cuello de botella potencial si la red no está optimizada para mitigar esta posibilidad.

Su aplicación está en redes corporativas compuestas por un gran número de LANs de diferentes tipos.

3.1.7 CONMUTADORES (SWITCHES)

Los conmutadores tienen la funcionalidad de los concentradores a los que añaden la capacidad principal de dedicar todo el ancho de banda de forma exclusiva a cualquier comunicación entre sus puertos. Esto se consigue debido a que el conmutador no actúa como repetidor multipuerto, sino que únicamente envía paquetes de datos hacia aquella puerta a la que van dirigidos. Esto es posible debido a que los equipos configuran unas tablas de encaminamiento con las direcciones MAC (nivel 2 de OSI) asociadas a cada una de sus puertas.

Esta tecnología hace posible que cada una de las puertas disponga de la totalidad del ancho de banda para su utilización. Estos equipos habitualmente trabajan con anchos

de banda de 10 y 100 Mbps, pudiendo coexistir puertas con diferentes anchos de banda en el mismo equipo.

Las puertas de un conmutador pueden dar servicio tanto a puestos de trabajo personales como a segmentos de red (hubs), siendo por este motivo ampliamente utilizados como elementos de segmentación de redes y de encaminamiento de tráfico. De esta forma se consigue que el tráfico interno en los distintos segmentos de red conectados al conmutador afecte al resto de la red aumentando de esta manera la eficiencia de uso del ancho de banda.

Hay tres **tipos** de conmutadores o técnicas de conmutación:

- ***Almacenar - Transmitir***. Almacenan las tramas recibidas y una vez chequeadas se envían a su destinatario. La ventaja de este sistema es que previene del malgasto de ancho de banda sobre la red destinataria al no enviar tramas inválidas o incorrectas. La desventaja es que incrementa ligeramente el tiempo de respuesta del switch.
- ***Cortar - Continuar***. En este caso el envío de las tramas es inmediato una vez recibida la dirección de destino. Las ventajas y desventajas son cruzadas respecto a Almacenar -Transmitir. Este tipo de conmutadores es indicado para redes con poca latencia de errores.
- ***Híbridos***. Este conmutador normalmente opera como Cortar -Continuar, pero constantemente monitoriza la frecuencia a la que tramas inválidas o dañadas son enviadas. Si este valor supera un umbral prefijado el conmutador se comporta como un Almacenar -Transmitir. Si desciende este nivel se pasa al modo inicial.

En caso de diferencia de velocidades entre las subredes interconectadas el conmutador necesariamente ha de operar como Almacenar -Transmitir.

Esta tecnología permite una serie de **facilidades** tales como:

Filtrado inteligente. Posibilidad de hacer filtrado de tráfico no sólo basándose en direcciones MAC, sino considerando parámetros adicionales, tales como el tipo de protocolo o la congestión de tráfico dentro del switch o en otros switches de la red.

Soporte de redes virtuales. Posibilidad de crear grupos cerrados de usuarios, servidos por el mismo switch o por diferentes switches de la red, que constituyan dominios diferentes a efectos de difusión. De esta forma también se simplifican los procesos de movimientos y cambios, permitiendo a los usuarios ser ubicados o reubicados en red mediante software.

Integración de routing. Inclusión de módulos que realizan función de los routers (encaminamiento), de tal forma que se puede realizar la conexión entre varias redes diferentes mediante propios switches.

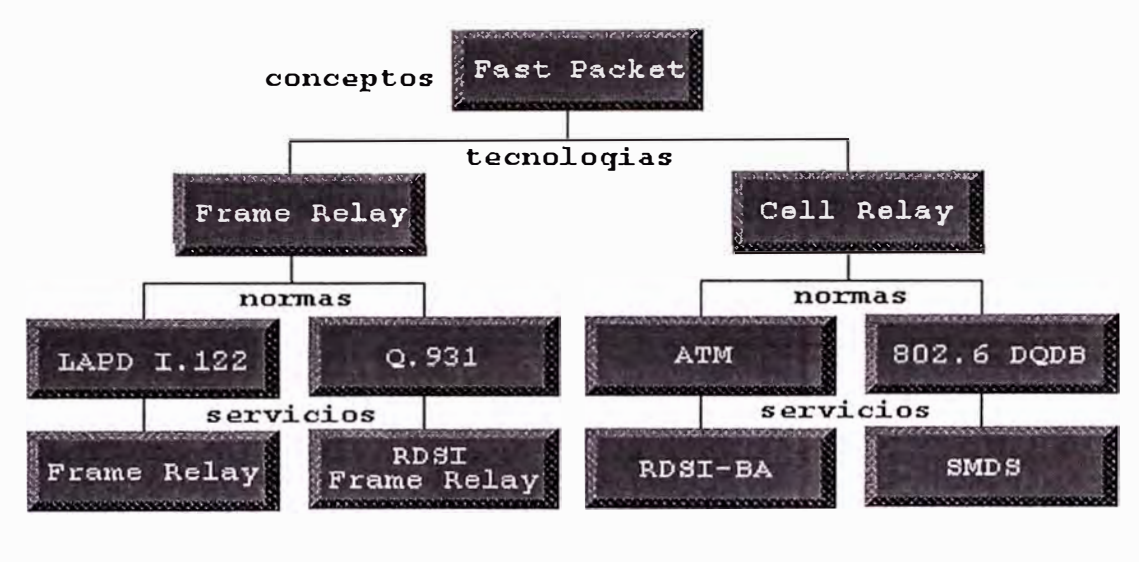
3.2 REDES DE CONMUTACIÓN DE PAQUETES

Las redes de conmutación de paquetes tradicionalmente han estado soportadas sobre tecnologías como X.25. Constituyen lo solución más adecuada para la transferencia de información entre puntos remotos dado se adecuan al tipo de tráfico generado por los terminales y equipos de comunicaciones siendo el coste de utilización es independiente de la distancia.

En la actualidad, las redes de conmutación de paquetes se soportan sobre tecnologías como Frame Relay o, más recientemente, ATM.

La figura 3.5 muestra una panorámica de las tendencias de las distintas tecnologías en el área de la conectividad entre redes remotas, en tecnologías, normas y servicios.

Figura 3.5 : Diagrama de las tendencias tecnológicas



3.2.1 FRAME RELAY

En el capítulo anterior se describió esta técnica de conmutación de paquetes que requiere menos proceso que X.25, lo que se traduce en velocidades de acceso mayores (2/1,5 Mbps frente a 64/56 kbps de X.25) y un coste de implementación menor.

El objetivo de diseño fue conseguir un servicio multiplexado que transportara tramas, minimizando los tiempos muertos y el *overhead* (sobrecarga) normalmente asociados a X.25, para lo cual, funcionalidades del tipo control de errores, de flujo, etc., se eliminan. *Frame Relay* nació en el seno de los comités encargados de la formulación

RDSI con el objetivo de sacar el mayor provecho posible de los accesos primarios (2 Mbps) para servicios portadores de paquetes. Actualmente la especificación permite alcanzar hasta 45 Mbps.

Opera sobre dos tipos de circuitos virtuales: Circuitos virtuales permanentes (PVC) y Circuitos virtuales conmutados (SVC).

Para cada circuito virtual se debe definir un CIR (Caudal Mínimo Comprometido) en cada sentido de la comunicación. Este CIR representa el ancho de banda que garantiza la red en caso de congestión o saturación de la misma, sin embargo, debido a que Frame Relay se basa en el concepto de *multiplexación estadística*, se podrá superar esta velocidad de transmisión comprometida hasta la *velocidad de acceso* al servicio (ancho de banda de la conexión entre el equipo terminal de comunicaciones y el nodo de red Frame Relay). La diferencia entre el ancho de banda de conexión a la red y el CIR se denomina EIR (Ráfaga en Exceso).

Para un mismo acceso Frame Relay será necesario definir tantos circuitos virtuales (caso de PVCs) como puntos de red con los que se desee conexión, siempre que la suma de los CIRs de cada uno de estos circuitos no supere en dos veces (teóricamente) la velocidad de acceso a la red, en otro caso será necesario aumentar el ancho de banda de conexión. (Para asegurar la concurrencia de comunicaciones por todos los PVCs la suma de los CIRs deberá ser como máximo equivalente a la velocidad de acceso a la red Frame Relay).

La técnica *Frame Relay* presenta un conjunto de ventajas que la hacen idónea para la definición de redes de área extensa; no representa cambios substanciales a nivel de equipamiento físico, las modificaciones en el equipamiento lógico a nivel de enlace son mínimas, presenta una eficiencia óptima para tráfico de datos y un

comportamiento excelente hasta 45 Mbps, lo que se considera suficiente para la interconexión de redes locales a medio y largo plazo. *Frame Relay* no conoce las redes de área local que interconecta, por ello es un protocolo transparente y adecuado en aplicaciones que intercambian grandes volúmenes de datos a grandes velocidades. Está especialmente indicado para transmisión asíncrona de datos.

3.2.2 ATM

La tecnología ATM (*Asynchronous Transfer Mode*, Modo de Transferencia Asíncrono) ha surgido como parte de un conjunto de investigaciones realizadas por los operadores públicos de telecomunicaciones para desarrollar la Red Digital de Servicios Integrados de banda ancha (RDSI-BA). En 1991, los trabajos de la UIT-T en el campo RDSI-BA dieron lugar a la definición de un estándar global de interfaces de usuario para redes ATM (recomendación UIT-T.I.121), con una capacidad de transferencia de información de 155,52 Mbps y 622,08 Mbps.

ATM fue diseñada para el transporte de datos sobre fibra óptica, de forma que el ancho de banda se reparte en bloques de tamaño idéntico denominados células (*cells*). Es una técnica del tipo *Cell Relay* orientada a la conmutación de células de tamaño constante a alta velocidad. El objetivo de ATM es realizar el *routing* y la multiplexación de las células. Es similar a Frame Relay diferenciándose, fundamentalmente, en que en esta última el tamaño de la célula (o *frame*) es variable.

Las redes ATM son transparentes a todos los tipos de información de usuario transportados mediante los servicios proporcionados por la red: voz, datos y vídeo. Soporta la transmisión de tráfico de diferente naturaleza de forma integrada.

La flexibilidad del ancho de banda es prácticamente ilimitada: es posible establecer cualquier ancho de banda hasta la capacidad máxima del enlace de transmisión utilizado.

Es una técnica eficiente para el tráfico de datos interactivo. Para aplicaciones del tipo de transferencia masiva de información o conexión entre redes de alta velocidad es la técnica idónea.

Una red ATM está formada por un conjunto de elementos de conmutación ATM interconectados entre sí por enlaces o interfaces punto a punto. Los conmutadores ATM soportan dos tipos de interfaces distintos: interfaz de red de usuario e interfaz de red de nodo. Los interfaces de red de usuario conectan dispositivos ATM finales (host, router, PBX, vídeo, ..) a un conmutador ATM. Los interfaces de red de nodo conectan dos conmutadores ATM entre sí.

Las redes ATM están orientadas a conexión, es decir se requiere el establecimiento de un circuito virtual antes de la transferencia de información entre dos extremos. Los circuitos que establece ATM son de dos tipos: caminos virtuales y circuitos virtuales, que son la agrupación de un conjunto de caminos virtuales.

El funcionamiento básico de un conmutador ATM es el siguiente: una vez recibida una celda a través de un camino o circuito virtual asigna un puerto de salida y un número de camino o circuito a la celda en función del valor almacenado en una tabla dinámica interna. Posteriormente retransmite la celda por el enlace de salida y con el identificador de camino o circuito correspondiente.

Existen principalmente dos tipos de conexiones en ATM:

Conexiones virtuales permanentes

La conexión se efectúa por mecanismos externos, principalmente a través del gestor de red, por medio del cual se programan los elementos de conmutación entre fuente y destino.

Conexiones virtuales conmutadas

La conexión se efectúa por medio de un protocolo de señalización de manera automática. Este tipo de conexión es la utilizada habitualmente por los protocolos de nivel superior cuando operan con ATM.

Dentro de estas conexiones se pueden establecer dos configuraciones distintas:

- Conexión punto a punto

  Se conectan dos sistemas finales ATM entre sí, con una comunicación uni- o bidireccional.

- Conexión punto multipunto

  Conecta un dispositivo final como fuente con múltiples destinos finales, en una comunicación unidireccional.

Los conmutadores ATM intercambian cada cierto número de celdas de información otras denominadas RM (Resource Management). Estas viajan en un sentido y en el conmutador final son reescritas y devueltas al origen con la indicación de retransmitir más despacio o de que todo va bien y que se puede continuar la transmisión del mismo modo. Este es un mecanismo de control de congestión.

Otra ventaja de la tecnología ATM es la utilización eficiente del ancho de banda: por el mismo "canal" circulan celdas que pueden llevar información de voz, datos o imagen y todas reciben el mismo tratamiento en los conmutadores. Cuando una comunicación finaliza, el ancho de banda que ocupaba queda liberado para otra comunicación. Para establecer una comunicación, se negocia el ancho de banda y la

calidad de servicio con el conmutador ATM, que puede aceptar la petición o limitar sus pretensiones de acuerdo con el ancho de banda disponible (este proceso de negociación forma parte de las especificaciones UNI, User-Network Interface).

En la actualidad el servicio ATM ofrecido por los operadores dominantes está disponible en todo el territorio nacional ofreciendo servicios de transporte de datos, conmutación de voz, etc. interoperando con otras redes de comunicaciones como Frame Relay de mayor penetración en el mercado.

ATM pretende ser una solución multimedia totalmente integrada para la interconexión de edificios ofreciéndose por parte de los operadores de comunicaciones la posibilidad de alquiler o compra del equipamiento de acceso al servicio, e infraestructura de líneas en caso de establecimiento de redes privadas.

ATM es la apuesta de las empresas de equipos de comunicaciones condicionada por la demanda de servicios multimedia y la liberalización del mercado de las comunicaciones, ya que es una tecnología que permite a los nuevos operadores de comunicaciones ser rápidamente competitivos. Un ejemplo de esta tendencia la presentan los operadores de cable que ofrecen multiservicios por una única infraestructura (televisión de alta definición, transporte de datos de gran ancho de banda, telefonía, etc.)

3.2.3 SONET/SDH

SONET (*Synchronous Optical Network*, Red Optica Síncrona) y SDH (*Synchronous Digital Hierarchy*, Jerarquía Digital Síncrona) en terminología UIT-T, es un estándar

internacional, desarrollado por el Working Group T1X1 de ANSI para líneas de telecomunicación de alta velocidad sobre fibra óptica (desde 51,84 Mbps a 2,488 Gbps). SONET es su nombre en EE.UU. y SDH es su nombre europeo. Son normas que definen señales ópticas estandarizadas, una estructura de trama síncrona para el tráfico digital multiplexado, y los procedimientos de operación para permitir la interconexión de terminales mediante fibras ópticas, especificando para ello el tipo monomodo.

Para entender el funcionamiento de SDH es conveniente hacer una introducción previa a PDH *(Plesiochronous Digital Hierachy)*.

- **PDH**

PDH surgió como una tecnología basada en el transporte de canales digitales sobre un mismo enlace. Los canales a multiplexar denominados módulos de transporte o contenedores virtuales se unen formando tramas o módulos de nivel superior a velocidades estandarizadas 2 Mbps, 8 Mbps, 34 Mbps, 140 Mbps y 565 Mbps.

Es una jerarquía de concepción sencilla, sin embargo contiene algunas complicaciones, que han llevado al desarrollo de otras jerarquías más flexibles a partir del nivel jerárquico más bajo de PDH (2 Mbps) equivalente a una trama MIC de RDSI (30B+D).

La principal problemática de la jerarquía PDH es la falta de sincronismo entre equipos. Cuando se quiere pasar a un nivel superior jerárquico se combinan señales provenientes de distintos equipos. Cada equipo puede tener alguna pequeña diferencia en la tasa de bit. Es por ello necesario ajustar los canales entrantes a una

misma tasa de bit, para lo que se añaden bits de relleno. Sólo cuando las tasas de bit son iguales puede procederse a una multiplexación bit a bit como se define en PDH. El demultiplexor debe posteriormente reconocer los bits de relleno y eliminarlos de la señal. Este modo de operación recibe el nombre de plesiócrono, que en griego significa cuasi síncrono.

Los problemas de sincronización ocurren a todos los niveles de la jerarquía, por lo que este proceso ha de ser repetido en cada etapa de multiplexación.

Este hecho genera un gran problema de falta de flexibilidad en una red con diversos niveles jerárquicos. Si a un punto de la red se le quieren añadir canales de 64 Kbps, y el enlace existente es de 8 Mbps o superior, debe pasarse por todas las etapas de demultiplexación hasta acceder a un canal de 2 Mbps y luego volver a multiplexar todas las señales de nuevo.

La falta de flexibilidad dificulta la provisión de nuevos servicios en cualquier punto de la red. Adicionalmente se requiere siempre el equipamiento correspondiente a todas las jerarquías comprendidas entre el canal de acceso y la velocidad del enlace, lo que encarece en extremo los equipos.

Otro problema adicional de los sistemas basados en PDH es la insuficiente capacidad de gestión de red a nivel de tramas. La multiplexación bit a bit para pasar a un nivel de jerarquía superior y con bits de relleno convierte en tarea muy compleja seguir un canal de tráfico a través de la red.

- **JERARQUIA DIGITAL SINCRONA (SDH)**

Una red síncrona es capaz de incrementar sensiblemente el ancho de banda disponible y reducir el número de equipos de red sobre el mismo soporte físico que otro tipo de tecnologías. Además la posibilidad de gestión de red dota a ésta de mayor flexibilidad.

El desarrollo de equipos de transmisión síncronos se ha visto reforzada por su capacidad de interoperar con los sistemas plesiócronos (PDH) existentes destinados principalmente al transporte de telefonía vocal. SDH define una estructura que permite combinar señales plesiócronas y encapsularlas en una señal SDH estándar.

Las facilidades de gestión avanzada que incorpora una red basada en SDH permiten un control de las redes de transmisión. La restauración de la red y las facilidades de reconfiguración mejoran la incorporación y prestación de nuevos servicios.

Este estándar de transmisión síncrona se recoge en las recomendaciones G.707,G.708, y G.709 del ITU (Unión Internacional de Telecomunicaciones) bajo el epígrafe SDH (Synchronous Digital Hierachy).

Las recomendaciones del ITU definen un número de velocidades de transmisión básicas en SDH:

- 155 Mbps, STM - 1 ('Synchronous Transport Module')
- 622 Mbps, STM - 4
- 2,4 Gbps, STM - 16
- 10 Gbps, STM - 64 (en desarrollo)

Estas recomendaciones definen también una estructura de multiplexación, donde una señal STM-1 puede portar señales de menor tráfico, permitiendo el transporte de señales PDH entre 1,5 Mbps y 140 Mbps.

SDH define un número de contenedores, cada uno de ellos correspondiente a una velocidad de transmisión PDH. La información de la señal PDH se introduce en su contenedor correspondiente y se añade una cabecera al contenedor, que permite monitorizar estas señales. Cabecera y contenedor forman un denominado contenedor virtual.

En una red síncrona todo el equipamiento se sincroniza con un mismo reloj de red. Variaciones de retardo asociadas a un enlace de transmisión inciden en una posición variable de los contenedores virtuales, lo que se resuelve asociándoles un puntero en la trama STM -1.

Ventajas de una red SDH:

- Simplificación de red

  Uno de los mayores beneficios de la jerarquía SDH es la simplificación de red frente a redes basadas exclusivamente en PDH. Un multiplexor SDH puede incorporar tráficos básicos (2 Mbps en SDH) en cualquier nivel de la jerarquía, sin necesidad de utilizar una cascada de multiplexores, reduciendo las necesidades de equipamiento.

- Fiabilidad

  En una red SDH los elementos de red se monitorizan extremo a extremo y se gestiona el mantenimiento de la integridad de la misma. La gestión de red permite la inmediata identificación de fallo en un enlace o nodo de la red.

Utilizando topologías con caminos redundantes la red se reconfigura automáticamente y reencamina el tráfico instantáneamente hasta la reparación del equipo defectuoso.

Es por esto que los fallos en la red de transporte son transparentes desde el punto de vista de una comunicación extremo a extremo, garantizando la continuidad de los servicios.

- Software de control

  La inclusión de canales de control dentro de una trama SDH posibilita un control software total de la red. Los sistemas de gestión de red no sólo incorporan funcionalidades típicas como gestión de alarmas, sino otras más avanzadas como monitorización del rendimiento, gestión de la configuración, gestión de recursos, seguridad de red, gestión del inventario, planificación y diseño de red.

  La posibilidad de control remoto y mantenimiento centralizado permite disminuir el tiempo de respuesta ante fallos y el ahorro de tiempo de desplazamiento a emplazamientos remotos.

- Estandarización

  Los estándares SDH permiten la interconexión de equipos de distintos fabricantes en el mismo enlace. La definición de nivel físico fija los parámetros del interfaz, como la velocidad de línea óptica, longitud de onda, niveles de potencia, y formas y codificación de pulsos. Asimismo se definen la estructura de trama, cabeceras y contenedores.

Esta estandarización permite a los usuarios libertad de elección de suministradores, evitando los problemas asociados a estar cautivo de una solución propietaria de un único fabricante.

Las redes de transmisión de telecomunicaciones que se desarrollan e implantan en la actualidad se basan principalmente en soluciones técnicas de jerarquía digital síncrona (SDH). Tanto las operadoras o PTT's en sus redes públicas, como empresas y organismos oficiales en sus redes privadas, están implantando SDH, que permite una integración de todos los servicios de voz, datos y vídeo a nivel de transmisión, lo que facilita la gestión de las redes y las beneficia de los niveles de protección y seguridad intrínsecos a SDH. Otra ventaja adicional de esta tecnología es que sobre ella se pueden desarrollar otras soluciones del tipo Frame Relay o ATM.

En conclusión cabe decir que actualmente SDH es la alternativa tecnológica de más futuro para la transmisión en las redes de comunicaciones. La tecnología PDH juega un papel todavía importante en la transmisión, al permitir segregar el tráfico en canales de comunicación de baja velocidad (menores de 64 Kbps). Es por ello que los equipos PDH se integran en el denominado acceso de usuario a las redes de transmisión en su jerarquía más baja (PDH a 2 Mbps). No obstante el resto de niveles de jerarquía superior en PDH (8, 34, 140 Mbps) están siendo desplazados por equipos de tecnología SDH, compatibles con PDH, pero más versátiles y económicos.

CAPÍTULO IV

CONFIGURACIÓN DE EQUIPOS ROUTER

General

Los Routers son los aparatos encargados de encaminar los paquetes que circulan por una red, en definitiva son ellos los que forman el núcleo de Internet. Un Router recoge el paquete que le llega, lo analiza y decide cual es el camino que debe seguir para llegar a su destino, haciendo de puente entre los distintos medios de transmisión (Frame Relay, X.25, RDSI, etc..) y los distintos protocolos. Físicamente un Router no es mas que un ordenador dedicado, es decir tiene su Microprocesador, su memoria y hasta su Sistema Operativo.

La empresa CISCO acapara el 70% del mercado de los routers, es algo así como Microsoft en el software. Para comprender el funcionamiento práctico de estos aparatos lo mejor es conocer el Sistema Operativo de Cisco: CISCO IOS.

Primero vamos a ver algunos conceptos de router, en particular del fabricante Cisco, tanto a nivel de hardware como software. También nos familiarizaremos con el manejo en modo consola de los routers.

4.1 ROUTER

Un router lo podemos definir como un dispositivo hardware, o bien un software corriendo sobre una computadora, que se encarga principalmente de tomar decisiones de encaminamiento de paquetes basándose en unas tablas almacenadas.

De otro modo: el router decide por donde enviar determinado paquete en función de la dirección destino. Normalmente un router tendrá al menos 2 interfaces de red LAN y/o WAN.

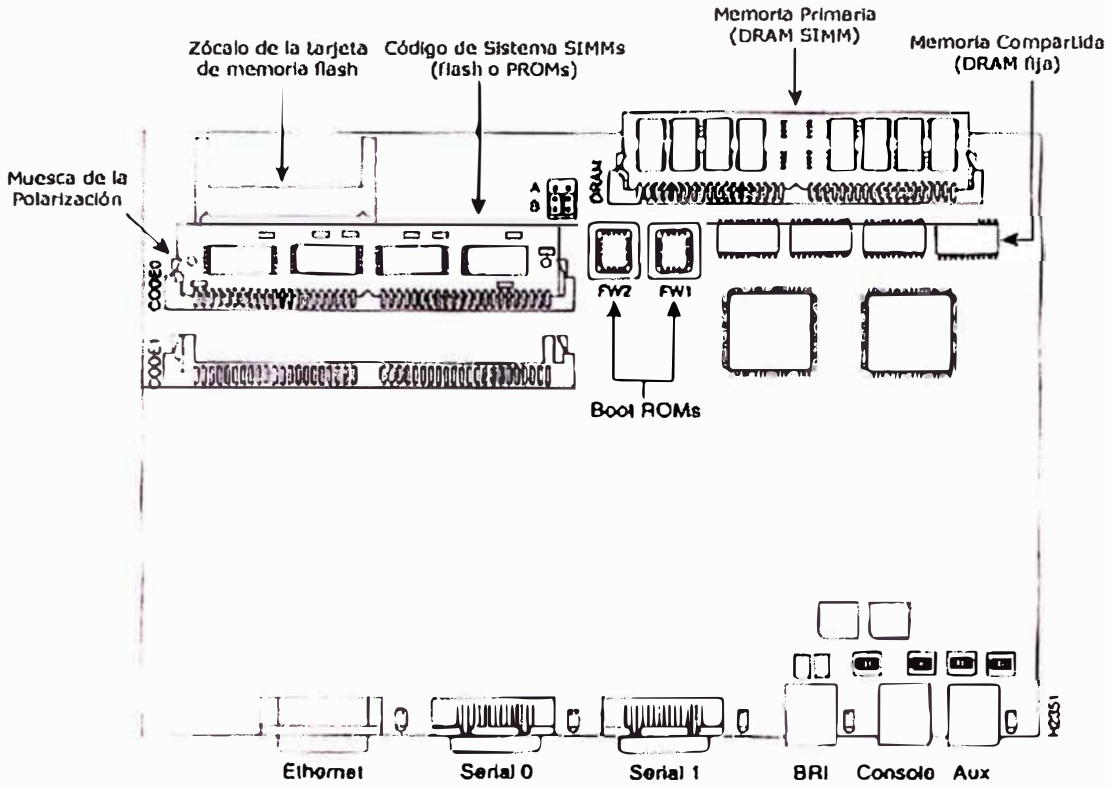
En el caso de Cisco, los routers son dispositivos hardware con un sistema operativo propietario llamado IOS, aunque no todos los routers Cisco tienen IOS (Por ejemplo: Cisco 7XX).

Los routers Cisco, aparte de su función fundamental, son capaces de hacer filtrado de paquetes, firewalling, traducción de direcciones, priorización de tráfico, etc. Las funcionalidades que tiene el router vienen determinadas en gran medida por la versión y el feature set (conjunto de características), que tenga la IOS (no es lo mismo un software IP que un IP/FW o un IP Plus).

4.1.1 CARACTERÍSTICAS DEL HARDWARE

Un router cisco, es muy parecido a un PC sólo que sin ningún tipo de periférico. Internamente se componen de una placa base que alberga la CPU, la memoria RAM, la memoria ROM, la memoria Flash (EEPROM) y la NVRAM, sin contar con las conexiones a los interfaces.

Figura 4.1 : Distribución de memorias en la tarjeta principal (Router Cisco 2501)



La memoria RAM se encarga de ejecutar la IOS, y de ejecutar todos los procesos que intervienen en cada una de las funciones del router, así como almacenar los buffers de E/S hacia y desde las interfaces y almacenar la configuración del router en cada momento.

La memoria ROM almacena una versión reducida de IOS y un interprete de comandos básico para casos de catástrofe.

La memoria Flash almacena una o mas imágenes, normalmente comprimidas, de la IOS, que se ejecutará sobre la RAM.

La memoria NVRAM (Non-Volatile RAM) se encarga de almacenar el archivo de configuración del router. Esta configuración se almacena en la RAM al arrancar el router.

Después de los componentes internos, pasemos a ver lo que nos ofrecen los routers al exterior: las interfaces. Todos los routers Cisco tienen un puerto de consola, con interfaz RJ45, que sirve para acceder al interprete de comandos de la IOS. Es la manera básica de acceder a configurar el router. A partir de los modelos 17XX, además tienen un puerto auxiliar, que es similar al de consola. Ambos puertos se pueden configurar para gestionar conexiones asincronas de baja velocidad.

El resto de interfaces son para conexiones de red, ya sea LAN o WAN. Hay routers que tienen interfaces fijos (Por ejemplo: Cisco 8XX, Cisco 25XX), y otros a los que se les pueden añadir tarjetas (modulares; por ejemplo: Cisco 36XX). También hay routers que incluyen interfaces fijos y algunos módulos para añadir tarjetas. (por ejemplo: Cisco 16XX, 26XX).

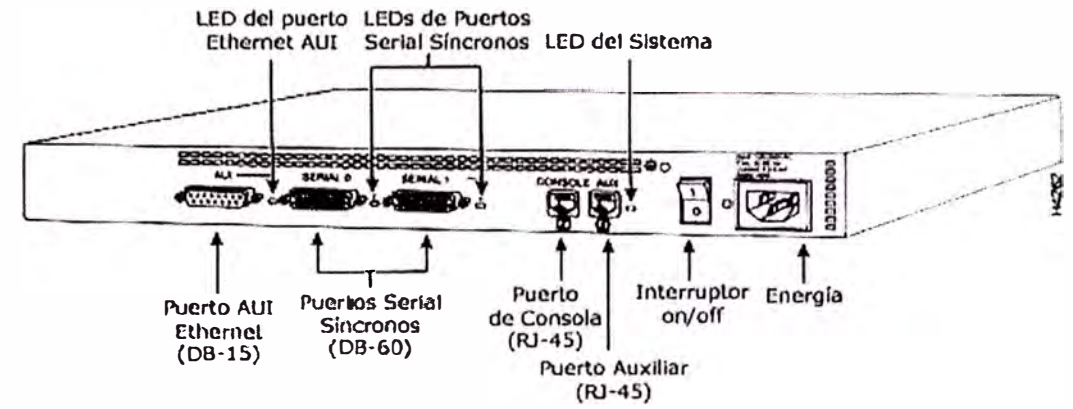
Existen por lo menos 2 tipos de tarjetas: las WIC's (Wan Interface Cards), y las VIC's (Voice Interface Cards), utilizadas para conexiones de datos de redes WAN y para enlaces o conexiones de voz, respectivamente, tal y como sus nombres indican.

Dentro de las tarjetas WIC podemos encontrar interfaces Serial, HSSI(High Speed Serial Interface), RDSI Basico, RDSI primario, E1, ATM, etc

Dentro de las VIC's, interfaces E&M, FXS, FXO, Primarios, etc.

Aparte de las tarjetas, existen Network Modules (NM), que pueden englobar varios slots para tarjetas WIC o VIC, interfaces LAN, interfaces WAN, y sus combinaciones (1 int Lan + 2 slots Wan, 2 Int Lan + 2 slots Wan, etc.)

Figura 4.2 : Vista posterior del Router Cisco 2501



4.1.2 CARACTERÍSTICAS DEL SOFTWARE (IOS)

Lo primero que debemos conocer sobre la IOS (Internetworking Operating System) es como poder acceder a su interprete de comandos. Tenemos varios métodos: por el puerto de consola (CONSOLE), por el auxiliar (AUX), o por una sesión telnet a través de un interfaz (VTY 0-4). Si tenemos el router en vacío, lo mas fácil es entrar por consola. Para ello, debemos usar cualquier software de emulación de terminal (Hyperterminal, Reflection, minicom, etc.) y conectar un cable desde el puerto serial de la PC al puerto de consola del router. Luego conectamos a 9600 baud, 8 bits y 1 bit de parada, y veremos que, si ya estaba encendido el router, aparece el siguiente prompt:

Router>

La IOS tiene varios modos de funcionamiento: dentro de los modos normales, empezamos por el EXEC, que se identifica con el promt ">", tal y como esta arriba. En este modo no tenemos privilegios y no podemos modificar, ni siquiera leer, la

configuración del router, aunque hay muchos comandos que se pueden usar (show, ping, telnet, enable, traceroute, etc.).

Si escribimos el comando enable, pasamos a modo EXEC Privilegiado, en el cual tendremos completos privilegios para cambiar la configuración y ejecutar todos los comandos.

Router> **enable**

Router#

Una vez en modo privilegiado, podemos entrar en modo configuración global:

Router# **configure terminal** (o en forma abreviada: **conf t**)

Router(config)#

Luego podemos pasar al modo de configuración de la interface:

Router(config)# **interface Serial0**

Router(config-if)#

Podemos salir de los modos con "exit", y del modo configuración en general con "end" o CTRL+Z. Otros modos dentro de la configuración son el modo router y el modo line:

Router(config)# **router**

Router(config-router)# (Para configuración de ruteo básicamente)

Router(config)# **line con 0**

Router(config-line)# (Para la configuración de la consola, puerto auxiliar y terminales virtuales (VTY)).

Resumiendo, tenemos 6 modos normales:

- EXEC
- EXEC Privilegiado (enable)

- Configuración global
- Configuración de interfaz
- Configuración de router (routing)
- Configuración de line

Existen otros 2 modos que sólo se usan en situaciones excepcionales:

- El modo rommon, se ejecuta un interprete de comandos distinto de la IOS que se ha cargado desde la ROM debido a que hemos interrumpido el arranque o a que no se ha podido cargar una IOS correctamente de la flash.
- El modo boot, es una versión de IOS reducida que almacena la ROM, debido a que no existe ninguna imagen de IOS valida en la flash (o esta en blanco). En este modo, el router es capaz de procesar paquetes, es decir, de hacer su función básica: el routing o encaminamiento.

4.2 REGISTROS DE CONFIGURACIÓN

El registro de configuración es un número de 2 bytes que se almacena en la NVRAM y define el modo en el que arranca el router. Normalmente, el router intenta arrancar una imagen de IOS de la memoria flash. Pero esto podemos cambiarlo, y también podemos arrancar el router sin que lea la NVRAM. Los valores que nos interesan del registro de configuración son los que pueden tomar los 4 bits menos significativos (bits 0, 1, 2 y 3), y el valor del bit 6:

Valor de lo 4 BMS	Significado
0x0	Arranca en modo rommon
0x1	Arranca en modo boot

0x2 a 0xF	Examina la NVRAM en busca de algún comando "boot system" si no existe, carga la primera imagen de la flash

Valor del bit 6	Significado
0 (0x00)	Arranca leyendo la NVRAM
1 (0x40)	Arranca si leer la NVRAM

De este modo, podemos hacer combinaciones (el valor 21h en el primer byte viene por defecto en Cisco, no influye):

Valor del registro	Significado
0x2102	Se carga la IOS de la flash y se lee la NVRAM (por defecto)
0x2142	Se carga el IOS de la flash y no se lee la NVRAM
0x2101	Modo boot leyendo la NVRAM
0x2141	Modo boot sin leer la NVRAM

Nota: no se incluyen las combinaciones en modo rommon porque a ese modo se accede mas fácilmente interrumpiendo la secuencia de inicio con CTRL + Break, y además no tiene sentido lo de leer o no la NVRAM ya que en modo rommon nunca se lee.

Para cambiar el valor del registro de configuración podemos usar el comando (en modo configuración global):

Router(config)# **config-register 0x21XX**

Realizamos una recarga de la configuración (reload), y si nos pregunta si queremos guardar la configuración, debemos responder que NO.

Para ver el valor actual del registro, usamos el comando "**show version**", que nos muestra también datos sobre el hardware y el software del router.

4.3 GESTIÓN DE LA IMAGEN DEL IOS

Hay veces que para determinadas funciones no nos valdrá la imagen de IOS que tenemos en nuestra flash. En este caso, habrá que cargar una nueva ya sea borrando la antigua o añadiéndola a ésta. Para ver el contenido de la flash usamos el comando:

Router# **show flash**

System flash directory:

File Lenght Name/Status

1 5403260 c2600-i-mz.112-17.bin

[5403324 bytes used, 2985284 available, 8388608 total]

8192K bytes of processor board System flash (Read ONLY)

Si no cabe la nueva imagen, se debe borrar la actual; debemos asegurarnos también de que la cantidad de RAM que tengamos en el router sirva para cargar nuestra nueva imagen. Esto lo podemos comprobar en la web de Cisco.

La nueva imagen la podemos descargar a través del protocolo xmodem o a través de un interfaz con un Server tftp. Lo mas cómodo es lo segundo.

Para el ejemplo, se ha supuesto que la dirección de nuestra interfaz Ethernet es la 192.168.1.1/24 y el Server tftp está en 192.168.1.2

Router(config)# **copy tftp flash**

IP address of remote host [255.255.255.255]? **192.168.1.2**

Name of tftp filename to copy into flash? **c2600-i-mz.120-1.bin**

copy c2600-i-mz.120-1.bin from 192.168.1.2 into flash memory? **[confirm]**

2678394 bytes available for writing without erasure.

Erase flash before writing? **[confirm]**

Clearing and initializing flash memory (please wait) #####.....###

Loading from 192.168.1.2: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Verifying checksum

VVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV

Flash verification successful. Lenght = 3804637, checksum = 0xD7A4

También podemos hacer lo contrario: cargar una imagen en un server tftp, con el comando "**copy flash tftp**".

Hay un caso especial al descargar una imagen a una flash de este modo: hay algunos modelos que no cargan toda la IOS en RAM, y hay parte de esta que se lee sobre la flash (por ejemplo, los Cisco 25XX). En ese caso la flash esta en modo lectura cuando el router arranca normalmente, para que en ningun caso se pueda modificar el código del software que se esta ejecutando, como en el ejemplo de arriba de "**show flash**" aparece que la flash esta en modo "Read ONLY". En este caso, tendremos que usar el modo boot:

Router(config)# **config-register 0x2101** (Arrancamos sin leer la flash)

Router(config)# **end**

Router# **reload**

System configuration has been modified. Save? [yes/no] **no**

Proceed with reload? **[confirm]**

El router comienza a rearrancar, pero en modo boot, de manera que ahora la flash está en modo escritura/lectura, y aparece el prompt:

Router(boot)> **enable**

password: ******

Router(boot)# **copy tftp flash**

....

.... (Cuando termine la descarga)

Router(boot)# **conf t**

Router(boot)(config)# **config-register 0x2102**

Router(boot)(config)# **end**

Router(boot)# **reload**

....

....

- **Particularidades del Interprete de Comandos**

El interprete de comandos de la IOS, aunque parezca poco amigable, puede llegar a ser muy rápido y cómodo para configurar el equipo, ya que tiene algunas funciones interesantes, en el interprete de comandos, nos devuelve un listado de posibles comandos y posibles parámetros de comandos:

Router# **conf t**

Router(config)# **interface ?**

Serial

Ethernet

Tokenring

Router(config)# **interface Serial ?**

Serial interface number

etc....

También nos da los posibles comandos que empiezan por los caracteres escritos:

Router# **debug i?**

interface ip

Router# **debug ip p?**

packet peer pim policy

Pulsamos, si el router reconoce el comando unívocamente con los caracteres que hayamos escritos, lo completa automáticamente. Aun así, si no completamos el comando y no es ambiguo, lo acepta igualmente:

Router# **sh**

Router# **show run**

Router# **show running-config** (equivalente a **sh run**)

Cisco ejecuta casi todos sus comandos en tiempo real, esto es, cuando escribes un comando, este hace efecto instantáneamente, sin tener que rearrancar el equipo.

Visualizamos la configuración que corre en el equipo con el comando **sh run**, la copiamos y la pegamos en otro router similar, se configura igual que el primero (con la salvedad de que habría que levantar manualmente las interfaces). Otros fabricantes funcionan con menús o con resúmenes de configuraciones, por lo que tendríamos que apuntar los parámetros y configurarlos en otro equipo.

Con la flecha de direcciones del teclado hacia arriba repetimos los comandos anteriores y con la flecha hacia abajo avanzamos los comandos.

4.4 COMANDOS DE CONFIGURACIÓN BÁSICA

A continuación se muestran los comandos para la configuración a nivel muy básico el router, como configuración del nombre del router, y los passwords de acceso y enable. Cabe recordar que todo los cambios de configuración que se realizará se encuentran en la configuración que está corriendo (running-config), por lo que si apagamos y encendemos el router, dichos cambios se perderán, para evitar esto debemos grabarlo en la NVRAM (startup-config) con el siguiente comando:

MiRouter# **copy** running-config startup-config

Otra manera de grabar, luego de cada configuración que realicemos, es usar el comando "**write memory**" o "**write**".

- Configurando el nombre del router

  Router# **config term** (o tambien **conf t**)

  Router(config)# **hostname** MiRouter

  MiRouter(config)#

- Configuración del password del modo enable

  MiRouter(config)# **enable password** mipass

- Habilitación del password para acceder al router por cualquier interfaz o por consola/auxiliar

  MiRouter(config)# **line con 0**

  MiRouter(config-line)# **password** mipass

  MiRouter(config-line)# **login** (Para hacer login por consola)

  MiRouter(config-line)# **line aux 0**

MiRouter(config-line)# **pass** mipass

MiRouter(config-line)# **login**

MiRouter(config-line)# **line vty 0 4** (Este comando configura a los 5 terminales virtuales a la vez con las mismas características, si se desea configurarlos independientemente, usar "**line vty X**", donde X: 0,1,2,3,4)

MiRouter(config-line)# **pass** mipass

MiRouter(config-line)# **login** (Si se desea bloquear el acceso por alguna interfaz del router, colocar el comando "**no login**")

MiRouter(config-line)# **exec-timeout [segundos]** (Define el tiempo máximo de inactividad en las sesiones telnet, luego del cual la sesión es cerrada)

A nivel global existen los siguientes comandos útiles:

show version	Muestra información general sobre el hardware, la IOS, memoria y el valor del registro de configuración.
show running-config	Muestra la configuración actual
show startup-config	Muestra la configuración con la que arranca el router
show interfaces	Muestra todas las interfaces y sus parámetros
show protocols	Muestra los protocolos que maneja el router
show process cpu	Muestra los procesos que están corriendo en la CPU y el porcentaje de consumo de cada uno. No es recomendable que la CPU este a más de 1/3 de su capacidad total.
show memory	Muestra detalles sobre la memoria RAM

Al visualizar la configuración, se puede observar que los passwords aparecen en texto claro, para evitar que sean de fácil lectura, podemos encriptarlos:

MiRouter(config)# **service password-encryption**

Pero ésta encriptación es débil y reversible (llamada tipo 7 en Cisco), pues existen programas que la desencriptan (por ejemplo, getpass), así que mejor es usar la encriptación 5 (MD5):

MiRouter(config)# **enable secret** mipass (para el enable password)

Para los de line, usar el siguiente comando: **password 5** mipass

Con estos cambios, al ver nuevamente la configuración (**sh run**) se verán algo así:

enable secret 5 1h7dd$VTNs4.BAfQMUU0Lrvmw6570

password $2n<jnjdwJ478Hl&sdkj

Este algoritmo es irreversible, por lo que el único ataque a estas claves es por fuerza bruta o por diccionario.

- **Descripción de un archivo de configuración**

router# **show configuration**

version 10.3 /* version del Cisco IOS */

service udp-small-servers /* servicios activos */

service tcp-small-servers

!

hostname router /* nombre del router */

!

enable secret 5 $7$5fr3$Lblju33t7NjnSUThFgxy34 /* clave encriptada */

enable password holahola /* clave para acceso por el puerto serial */

```
!
!
interface Ethernet0                    /* Configuración de la Tarjeta de Red */
 ip address 197.111.1.2 255.255.255.0
!
interface Serial0                      /* configuración de Frame Relay */
 no ip address
 encapsulation frame-relay IETF
 frame-relay lmi-type ansi
!
interface Serial0.1 point-to-point     /* configuración de los PVC Frame Relay */
 ip address 10.1.1.1 255.255.255.252
 frame-relay interface-dlci 510
!
interface Serial0.2 point-to-point
 ip address 10.1.1.2 255.255.255.252
 frame-relay interface-dlci 512
!
ip host otro1 10.1.1.1
ip host otro2 10.1.1.2
snmp-server community public RO
!
line con 0                             /* configuración para acceso por consola */
 exec-timeout 40 0
```

line vty 0 5 /* configuración para acceso remoto */

password hola

login

!

end

- **Aplicación del router como Firewall**

Un router Cisco pueden funcionar como un Firewall a nivel de red permitiendo o denegando el acceso a determinadas IPs. Esto se consigue con las listas de acceso:

access-list nn [permit/deny] ip IP-in Mask-in IP-out Mask-out

- Para permitir el acceso a las maquinas 147.22.x.x

  acces-list 101 permit ip 147.22.0.0 0.0.255.255 0.0.0.0 255.255.255.255
- Para denegar el acceso a conexiones udp a las maquinas de la red 156.23.22.0

  access-list 101 deny udp 156.23.22.0 0.0.0.255 0.0.0.0 255.255.255.255

También se puede filtrar por puertos, especificando un puerto concreto (eq x) o un rango (gt x, mas grande que x)

Para permitir tráfico Domain Name System (DNS) y Network Time Protocol (NTP) usamos lo siguiente:

access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 53

access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 123

Para denegar el acceso al Network File System (NFS) usando el puerto UDP

access-list 101 deny udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 2049

Después de definir la lista de acceso es necesario guardarla en la memoria no volátil (NVRAM) y luego aplicarla a un interface específica, por ejemplo

interface ethernet 0

ip access-group 101

CONCLUSIONES

La interconexión de redes LAN, hoy en día más que una necesidad, es el modo de trabajo, pues en estos tiempos de globalización, las zonas de trabajo ya no se encuentran limitadas por las áreas físicas de las oficinas o departamentos de la empresa donde se labore, actualmente el área de trabajo es a nivel mundial.

Frame Relay, contribuye grandemente a la interconexión de redes, pues sus características estudiadas demuestran que posee mayor rapidez para el traslado de los datos y más aún abarató los costos de conexión, al permitir a los usuarios y empresas poder conectarse con velocidades intermedias, a las grandes redes de datos ATM y SDH.

Por otro lado los equipos que permiten la interconexión de las redes, como es el caso del Router, con su constante evolución nos permite añadir mayores servicios, pues ya no solo se habla de interconexión de redes de Datos, si no también de la interconexión de los servicios de Voz y Videos, de tal manera que las empresas se sientan tan cerca y unidas al estar distribuidas en diferentes puntos de planeta.

ANEXO A : ACRONIMOS

ANSI	American National Standard Institute
ATM	Modo de Transferencia Asíncrono
AUI	Attachment Unit Interface
BECN	Backward-Explicit Congestion Notification
BW	Ancho de Banda
CAD	Diseño Asistido por Computadora
CAM	Manufactura Asistida por Computadora
CBR	Tasa de Bit Constante
CCITT	Comité Consultatif International Telégraphique et Teléphonique
CDE	Data circuit-terminating equipment
CDMA	Code Division Multiple Access
CIR	Caudal Mínimo Comprometido
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DE	Discard Eligibility
DLCI	Data-link Connection Identifier
DTE	Data terminal equipment
E&M	Ear and Mouth

EA	Extended Address
EIR	Ráfaga en exceso
FCS	Frame Check Sequence
FDMA	Frequency Division Multiple Access
FDDI	Fiber Distributed Data Interface
FECN	Forward-Explicit Congestion Notification
FTP	Protocolo de Transferencia de Archivo
FXS	Foreign Exchange Station
FXO	Foreign Exchange Office
HDLC	Control de Enlace de Datos de Alto Nivel
IEEE	Institute of Electric and Electronic Engineers
IP	Protocolo de Internet
IPX	Internetwork Packet Exchange
ISDN	Integrated Services Digital Network
ISO	International Standard Organization
LAN	Local Area Networks
LMI	Local Management Interface
MAC	Medium Access Control
OSI	Open Systems Interconnection
PABX	Private Automatic Branch exchange
PBX	Private Branch exchange
FDDI	Fiber Distributed Data Interface
PDH	Plesiochronous Digital Hierarchy
PDX	Private Digital exchanges

PSN	Packet-switched network
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuits
RAM	Random Access Memory
RISN	Reduced Instructions Set Computer
ROM	Read Only Memory
SDH	Synchronous Digital Hierarchy
SIMM	Single In-line Memory Module
SNA	System Network Architecture
SONET	Synchronous Optical Network
STM	Synchronous Transport Module
SVC	Switched Virtual Circuits
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
UTP	Unshielded Twisted Pair
WAN	Wide Area Networks
WIC	Wan Interface Card
XNS	Xerox Network Systems

BIBLIOGRAFÍA

- Fred Halsall, "Comunicación de datos, redes de computadores y sistemas abiertos", Cuarta Edición – Editorial Addison Wesley Longman de México, S.A. 1998
- Andrew Tanenbaum, "Redes de Ordenadores", Segunda Edición - Editorial Prentice-Hall Hispanoamericana S.A. México, 1991
- Cisco System, "Frame Relay", 2002. En http://www.cisco.com
- Steve Spanier, "Tecnologías de Interconectividad de Redes", Editorial Prince Hall – Cisco Press
- Philip Smith, "Frame Relay Principles and Applications", Editorial Addison-Wensley Publishers 1993, Data Communications and Networks Series
- W. Stallings, "ISDN and Broadband ISDN with Frame Relay and ATM", 3Th Edition – Prentice Hall International editions.
- Interconexión de Redes, http://www.map.es/csi/silice/Red.html
- Configuración de Router, http://www.ircayuda.net/manuales/routers.htm
- Guía de configuración de router Cisco, http://go.to/guiacisco%20