UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
"ARAGÓN"

PROYECTO DE MODERNIZACIÓN DE LA RED IMSS VPN IP/MPLS

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO MECÁNICO ELECTRICISTA
P R E S E N T A :
RAFAEL TAMAYO SALAZAR

ASESOR:
ING. RAÚL BARRÓN VERA

MÉXICO **2003**

LA IGNORANCIA MATA A LOS PUEBLOS,
POR ELLO ES PRECISO MATAR LA
IGNORANCIA.

José Martí

TRIUNFAR ES LA BASE DE MI LEMA,
Y DE LA VICTORIA SOY EL HIJO
PREDILECTO.

Anónimo

**********AGRADECIMIENTOS **********

Agradezco a todas aquellas personas que aportaron e incentivaron mi camino para que se haya concluido uno de los pasajes más importantes en mi vida, por ello expreso mi más sincero reconocimiento y a su vez hago extensa mi deuda de gratitud hacia todos ustedes:

- **A mi padre y a mi madre que han aguantado y tolerado todas mis locuras.**
- **A mi hermano Eduardo por su apoyo.**
- **A mi esposa Susana y mi hijo Said Yaroo por su paciencia y su confianza.**
- **Al Ing. David Estopier Bermúdez por amistad y su tiempo para dirigir y asesorar mi proyecto de tesis.**
- **A mis compañeros y amigos de trabajo IMSS sub 4 Gro:**
  - **Mario Escalante H.**
  - **Manuel Sandoval M.**
  - **Miguel Santillán T.**
  - **Juana Coronel G.**
  - **Melania Barreto M.**
- **A mis compañeros y amigos de escuela:**
  - **Juan Gabriel Quillo H.**
  - **Víctor Hernández M.**
  - **Oscar Ramírez H.**
  - **Eduardo Uribe R.**
  - **Rafael Martínez M.**
  - **Gildardo Apaez G.**
  - **Julio Pastelin A.**
  - **Valentín Santos C.**
  - **Juan C. Luna K.**
  - **Edgar Moreno N.**
  - **Emilio Cuellar H.**
  - **Alejandro I. Vigueras G.**
  - **José A. Chávez G.**
  - **Elizabeth Reyes B.**
  - **Mauricio Téllez A.**
  - **Leonardo Granados J.**
  - **L. Héctor Manríquez S.**
- **A mis compañeros y amigos del área de telecomunicaciones IMSS nivel central:**
  - **Ing. Alfonso Chopin S.**
  - **Ing. G. Eloy Vargas E.**
  - **Ing. Antonio Camacho U.**
  - **Ing. Arnulfo Macías H.**
  - **Ing. Adrián Jiménez H.**
  - **Ing. Luis Camargo D.**
  - **Ing. Mauricio Pastrana H.**
  - **Ing. Francisco Parada G.**
  - **Yolanda Cuevas H.**

PROYECTO DE MODERNIZACIÓN DE LA RED IMSS VPN IP/MPLS

ÍNDICE

Pagina No

********** OBJETIVO GENERAL **********

El objetivo de este proyecto es desarrollar un nuevo esquema de comunicaciones que sea innovador de acuerdo a los nuevos requerimientos de crecimiento y expansión de la institución. Que se acople a los retos que tendrá el IMSS, y que además sea capaz de poner a esta institución en un panorama de vanguardia tecnológica para que pueda seguir sustentando el crecimiento y la evolución de todas sus áreas, así como todos los escenarios de la institución en el corto y mediano plazo, con el fin de seguirse transformando como una institución, que es patrimonio de todos los mexicanos y que sea capaz de llegar a satisfacer los índices de calidad que todos los derechohabientes y la seguridad social de este país exigen.

Las redes de computadoras nacen como evolución de los sistemas de acceso y transmisión a la información y cumplen fundamentalmente el objetivo de facilitar el acceso a información remota, comunicación entre personas y entretenimiento interactivo. Hoy en día la conversión de las líneas telefónicas en redes de telecomunicaciones integradas es producto del desarrollo tecnológico, es por ello que podemos mencionar que la transmisión de información tiene sus inicios con la aparición del telégrafo, y una cantidad de inventos y descubrimientos que han sustentado en avance tecnológico de nuestros días. Ahora bien, con el objeto de no hacer una reseña extensa y tediosa del concierto de las telecomunicaciones solo nos avocaremos a mencionar una pequeña serie de aportaciones y descubrimientos científicos que fueron esenciales para el desarrollo de la transmisión de información. De lo anterior se desprende que solo se hace mención de algunos o los más importantes que sirvieron de fundamento en el desarrollo de la evolución tecnológica en la transmisión de datos (información) en las redes modernas.

El primero elemento que consideramos fue el telégrafo que fue inventado por el norteamericano Samuel F. B. Morse en 1837, el código Morse, transmitía mensajes mediante impulsos eléctricos que circulaban por un único cable. Posteriormente años más tarde aparece la Invención del teléfono por Alexander Graham Bell en 1876. Y ya para los años 1920-1928 Se desarrolla la "Teoría de transmisión señal a ruido" por J.R. Carson, H. Nyquist, J.B. Johnson, y R. V. Hartley. En 1930 surge el concepto de ARQ. Consiste en una técnica de telecomunicaciones en la cual el dispositivo receptor detecta errores y realiza una verificación de señal (*request*) al dispositivo emisor. ARQ significa Repetición Automática de Verificación (*Automatic Repeat Request*). En 1940 aparece la Primer computadora, llamada Z2 por Konrad Zuse (Alemán). Y para el año de 1948 Quizás el mayor evento en las comunicaciones del mundo ocurre, cuando Claude Shannon desarrolló su *"Teoria matemática de las comunicaciones"* Shannon desarrolla el concepto "Teoría de la Información". En los años 1948-1951 Es inventado el transistor por Bardeen, Brattain, y Shockley; con este descubrimiento se reduce significativamente el tamaño y la potencia de los equipos de comunicaciones. Pero es en el año 1969 Enero 2, cuando nace el precedente de la redes de computadoras, el gobierno de los Estados Unidos le da vida a INTERNET cuando un equipo de científicos empiezan a hacer investigaciones en redes de computadoras. La investigación fue fundada por la *Advanced Research Projects Agency -ARPA*, una organización del Departamento de Defensa de los E.U., mejor conocida como ARPANET. Ya para estos años se tenían elementos técnicos y otros medios de comunicaciones eficientes que habían sido probados y bastante desarrollados como lo eran la comunicación inalámbrica por ondas de radio, la red telefónica e incluso la comunicación satelital, pero el desarrollo de los sistemas informáticos estaba en sus inicios. Estas investigaciones arrojaron como resultado el protocolo de comunicaciones TCP/IP (Trasmission Control Protocol/Internet Protocol) un sistema de comunicaciones muy sólido y robusto en el cual se integran todas las redes que conforman lo que se conoce actualmente como Internet. Las primeras redes construidas permitieron la comunicación entre una computadora central y terminales remotas bajo el uso de las líneas telefónicas. Ya hemos mencionado que en los años 70 surgieron las primeras redes de transmisión de datos, y la literatura informática nos dice que la primera red comercial fue la TRANSCANADA TELEPHONE SYSTEMS DATAROUTE a la que posteriormente surgió el Digital Data System de AT&T. Desde el nacimiento de internet y hasta nuestros días han surgido enormes cantidades de redes, servicios, estándares de normatividad y tecnologías para redes en todo el mundo, así como también se ha incrementado notablemente el número de redes locales de agencias gubernamentales, consorcios empresariales y de universidades en todo el planeta. En México los primeras referencias que se tienen acerca de las comunicaciones aparecen a fines del siglo XIX a pocos años de después de los primeros descubrimientos.

En 1878, se realizó en México la primera prueba telefónica exitosa entre la ciudad de México y la entonces remota población de Tlalpan, que hoy constituye una de las delegaciones políticas del Distrito Federal. El Departamento del Distrito Federal (DDF) y la empresa Alfredo Westrup y Compañía firmaron un contrato para comunicar a las seis comisarías de policía con que entonces contaba la ciudad, con las oficinas del Inspector General y del Ministro de Gobernación.

Entre 1879 y 1880 se tendieron las primeras redes privadas, y el 19 de julio de 1881, se otorgó permiso al estadounidense M.L. Greenwood para instalar una red de servicio público en la Ciudad de México, y en 1882 se fundó la Compañía Telefónica Mexicana, subsidiaria de Telefónica de Boston que posteriormente, en 1905, cambió su razón social a Compañía Telefónica y Telegráfica Mexicana, S.A. Fue así como nació la primera empresa de telefonía en el país.

En 1888 se editó el primer directorio telefónico del país, el cual incluía los datos de poco más de 800 suscriptores, y tres años después contaban con servicio telefónico las ciudades de México, Guadalajara, Puebla, Mérida y Veracruz. Hasta este momento, el servicio telefónico era considerado un lujo al que sólo tenían acceso las clases más favorecidas, y En 1892 y 1893, la Compañía Telefónica Mexicana se expandió gracias a la compra que realizó de otras empresas que operaban en diversas regiones del país. En 1896 comenzó a prestar el servicio en Monterrey y otras doce ciudades, y en 1897 procedió a la instalación de los primeros teléfonos públicos de larga distancia en el Distrito Federal.

En 1904, la International Telephone and Telegraph Company (ITT) de los Estados Unidos adquirió las instalaciones de la Compañía Telefónica Mexicana. El sueco Axel Bostrom, por su parte, solicitó ese mismo año el registro de la compañía L.M. Ericsson para prestar servicios de telefonía. Al año siguiente, Bostrom traspasó su concesión a la L.M. Ericsson, que en 1909 efectuó una nueva transacción acompañada de una reestructuración de la empresa para constituirse como Teléfonos Ericsson.

En 1924 se inauguró en México la primera central automática, que si bien reducía la necesidad de conectar manualmente las líneas en un tablero, conservaba el gran tamaño, alto costo y bajo rendimiento de los sistemas telefónicos de la época. En 1926, Teléfonos Ericsson inició el servicio de larga distancia, y al año siguiente la Compañía Telefónica y Telegráfica de México inauguró el servicio de larga distancia a Estados Unidos y Canadá. En 1928, extendió el servicio de larga distancia internacional a Europa. Así, la primera mitad del siglo XX estuvo dominada por las compañías Ericsson y Mexicana, con el grave inconveniente de que los aparatos de una y otra no podían dialogar entre sí. Debido a que no contaban con interconexión entre sus redes, quien tenía contrato con Mexicana no podía comunicarse con un cliente Ericsson, y viceversa. Tras un largo cortejo, Ericsson y Mexicana se "casaron" en 1941, año en que enlazaron sus líneas en todo el territorio mexicano, con excepción del Distrito Federal.

En 1947 fue constituido Teléfonos de México, S.A., y en 1948 quedaron completamente enlazadas las líneas de todo el país. Dos años más tarde, Teléfonos de México adquirió los bienes de la Compañía Telefónica y Telegráfica Mexicana.

En 1958 un grupo de inversionistas mexicanos adquirió la mayoría de las acciones de Teléfonos de México, que décadas más tarde, el 31 de octubre de 1972, se convirtió en empresa de participación estatal mayoritaria. Con el estatus de empresa gubernamental, Teléfonos de México continuó prestando nacionalmente servicios telefónicos en forma exclusiva hasta 1990, y desde entonces conserva este derecho a pesar de haberse transformado en una empresa privada. No obstante, la modificación (en 1990) del título de concesión que le fue otorgado el 10 de marzo de 1976 a Teléfonos de México inició el proceso de apertura del mercado nacional de telecomunicaciones y el fin de un servicio prestado monopólicamente por casi 50 años.

En su devenir, Teléfonos de México consiguió resultados importantes en términos de ampliación de la cobertura geográfica del servicio telefónico y generación de nuevos servicios. Cuando Teléfonos de México se privatizó en 1990, las modificaciones efectuadas al título de concesión entregado al grupo encabezado por Grupo Carso fijaron una serie de compromisos cuyo cumplimiento por la empresa le permitiría disfrutar, entre otros derechos, de la exclusividad sobre el servicio de larga distancia hasta enero de 1997. Estos compromisos incluyen la universalización del servicio telefónico con énfasis en las zonas rurales del país y la inversión en tecnología. Actualmente, Teléfonos de México (Telmex) presta servicio telefónico en más de 20,500 localidades y próximamente tendrá cobertura en todas las poblaciones del país con más de 500 habitantes. Desde 1990, Telmex ha ejercido inversiones superiores a los $10,000 millones de dólares en la actualización de su infraestructura, de los cuales una parte ha servido para digitalizar la totalidad de las líneas instaladas en el Distrito Federal y otras grandes poblaciones. Conformada actualmente por más de 45,000 empleados, Telmex es además la compañía más grande del país después de Petróleos Mexicanos y cuenta con la mayor participación extranjera entre todas las empresas de telecomunicaciones de América Latina

En 1995, Teléfonos de México fue además la empresa de telecomunicaciones más rentable del mundo en términos de utilidad por acción y utilidad neta, y de hecho fue la compañía más rentable del listado anual Fortune 500 después de una compañía de seguros británica. El Grupo Carso, que bajo la presidencia del empresario mexicano Carlos Slim detenta el control accionario sobre Telmex, anunció en 1996 su división en dos grandes grupos, de los cuales Global Carso Telecom representa a Telmex en empresas que incluyen a

Telcel (telefonía celular con cobertura nacional), Red Uno (redes de datos), Telecorp (servicios empresariales de comunicación y valor agregado) y Cablevisión (televisión por cable).

CONCEPTOS GENERALES DE REDES

PAGINACIÓN DISCONTINUA

1.1 DEFINICIÓN DE RED

Derivado del análisis hecho y tomando en consideración diferentes perspectivas, definiremos el concepto de red del modo siguiente: ¿Que es una red? por lo que podemos citar en ese contexto la siguiente definición.

Una red se denomina como un sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario. La infraestructura o instalación que establece una red de canales o circuitos para conducir señales de voz, sonidos, datos, textos, imágenes u otras señales de cualquier naturaleza, entre dos o más puntos definidos por medio de un conjunto de líneas físicas, enlaces radioeléctricos, ópticos o de cualquier otro tipo, así como por los dispositivos o equipos de conmutación asociados para tal efecto.

En términos de tecnologías de información, una red es una serie de puntos ó nodos interconectados por vías de comunicación. Las redes pueden interconectarse con otras redes y contener subredes.

Ahora para dar una explicación más detallada podemos citar que una red es un sistema de comunicaciones que permite a los usuarios de computadoras compartir los recursos de una computadora, y sus datos, la voz, imágenes y las transmisiones de vídeo. Las redes pueden conectar a usuarios que están situados en la misma oficina o en países diferentes. La información de la red se transmite por cable, a través de comunicaciones por fibra óptica o a través de ondas de radio como las microondas.

Existen varias razones para tener una red. La primera es para que el propietario de la red ahorre recursos, ya que se comparten el software y los equipos. Toda una oficina puede compartir una impresora, ahorrando el costo de incorporar una impresora a cada computadora. El almacenamiento en discos y en CD-ROM también puede compartirse, para ahorrar la compra de un disco duro y una unidad de CD-ROM por cada computadora. La figura (1.1a) muestra 10 computadoras en red, que comparten un único banco de 14 unidades de CD-ROM.

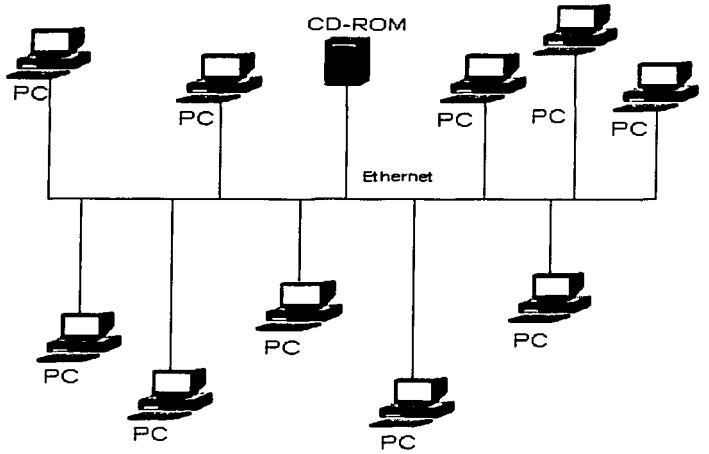


Figura (1.1a)

La segunda razón es que las redes hacen que las personas sean más productivas por que pueden compartir la información sin dejar sus oficinas o sus casas. Otra razón para tener una red es la posibilidad que proporciona de abrir vías de información. Bibliotecas, organizaciones de investigación, universidades, empresas, e individuos privados confeccionan todo tipo de información disponible a través de redes conectadas a la red Internet.

1.2 TIPOS DE RED POR COBERTURA

a) REDES LAN

Redes de área local (LAN, Local Area Network). Una de las redes locales más conocidas y populares es la red Ethernet, desarrollada por Xerox Corporation en los laboratorios de investigación de Palo Alto, en California. La red fue diseñada para enlazar un grupo de microordenadores que Xerox tenía distribuidos por todo el centro, con el fin de intercambiar programas, datos, y tener acceso a diversos periféricos.

Este tipo de redes se extiende a lo largo de áreas relativamente pequeñas, tales como un campus universitario, o una planta de manufactura. Las distancias que cubren estas redes pueden variar entre algunos metros y varios kilómetros. Al principio, las redes conectaban a usuarios que estaban próximos, por ejemplo en la misma oficina o en la misma planta de un edificio. En realidad, estaban formando redes de área local (LAN, Local Area Network), con un área limitada de servicio. Cuando las LAN llegaron a ser habituales, el siguiente paso fue encontrar la forma de conectar una LAN con otra. Por ejemplo, conectar una red LAN que se encuentra en un edificio con una red LAN que esta situada en un edificio contiguo o incluso en un edificio que se encuentra en el otro extremo de la ciudad.

Al igual que las redes de área amplia, una red de área local es una red de comunicaciones que interconecta a varios dispositivos y proporciona un medio para el intercambio de información entre ellos. No obstante hay algunas diferencias entre las LAN y las WAN que se enumeran a continuación:

- La cobertura de una LAN es pequeña, típicamente de un edificio o como mucho un conjunto de edificios próximos y la cobertura geográfica, condicionara la solución técnica finalmente adoptada.
- Es común que la LAN sea propiedad de la misma entidad que es propietaria de los dispositivos conectados a la red. En WAN, esto no es tan corriente, o al menos una fracción significativa de recursos de la red son ajenos. Esto implica. Primero se debe cuidar mucho la elección de la LAN, ya que evidentemente, lleva acarreado una inversión substancial de capital (comparado con los gastos de conexión o alquiler de líneas en redes de área amplia) tanto en la adquisición como en el mantenimiento. Segundo, la responsabilidad de la gestión de la red local solamente en usuario. Tercero, las velocidades internas de transmisión en una LAN son mucho mayores.

Tradicionalmente, en LAN se utiliza la difusión en lugar de utilizar técnicas de conmutación. En una red de difusión, no hay nodos intermedios. En cada estación hay un transmisor/ receptor que se comunica con la otras estaciones a través de un medio compartido. Una transmisión desde cualquier estación se recibirá por todas las otras estaciones. Los datos se transmiten en forma de paquetes. Debido a que el se recibirá por todas las otras estaciones. Los datos se transmiten en forma de paquetes. Debido a que el medio es compartido, una y sólo una estación en cada instante de tiempo podrá transmitir el paquete. Recientemente, la conmutación también se esta utilizando en LAN. Ahora daremos una descripción sobre el formato de la trama Ethernet IEEE 802.3, cuando se transmiten datos sobre redes Ethernet estos se encapsulan en tramas como la que se muestra en el grafico de la figura (1.2a). El primer campo es el preámbulo con longitud de 56 bits y se encarga de sincronizar la transmisión de la trama y consta de un patrón de 0's y 1's alternados, el siguiente campo es el delimitador de inicio de trama (SDF, Start Frame Delimiter), compuesto por 8 bits. El patrón de bits del delimitador (SDF) es 10101011. Las direcciones del destino y el origen se encuentran situados en dos campos que hay a continuación del delimitador (SDF). Según las especificaciones IEEE 802.3, los campos de dirección pueden ser de 16 o 48 bits. A continuación, un campo de 16 bits especifica la longitud de la trama, después aparece el campo de datos encapsulados con longitud de 576 a 12,208 bits y han de ser múltiplos de 8. Y en el caso de que la longitud de los datos sea menor de 512 bits hay que incluir un campo de relleno. Por ultimo la parte final de la trama esta compuesta por una secuencia de comprobación (FCS, Frame Check Sequence) de 32 bits, el cual utiliza un código de redundancia cíclica (CRC) para detectar se han producidos errores.

Preámbulo	SDF	Dirección Destino	Dirección Origen	Indicador de longitud	Datos	Relleno	FCS
56	8	16 - 48	16	16	0 - 12,0000		32

Figura (1.2a)

b) REDES MAN

Una red de área metropolitana (MAN, Metropolitan Area Network) es una red de ordenadores de tamaño superior a una LAN, soliendo abarcar el tamaño de una ciudad. Es típica de empresas y organizaciones que poseen distintas oficinas repartidas en una misma área metropolitana, por lo que en su tamaño comprenden un área desde unos kilómetros.

Una red de área metropolitana MAN, se consigue conectando varias redes LAN dentro de una ciudad o zona urbana. Un ejemplo claro es la universidad estatal de alguna ciudad, es una red MAN cuando se conecta a varios centros de investigación y a otros recursos a lo largo de la ciudad. Otro caso muy común es un gran complejo empresarial podría tener redes LAN utilizadas para el procesamiento administrativo que a su vez estuvieran conectadas a otras redes LAN utilizadas para la investigación científica.

Las redes de área metropolitana (MAN). Son redes públicas de alta velocidad, operando a 100 Mbps, capaces de transmitir voz y datos sobre áreas de hasta 50 millas (80 kms). Ejemplo: una red que conecta varios edificios de una organización dentro de una ciudad.

c) REDES WAN

El alcance de las redes ha crecido hasta expandirse a lo largo de continentes y de océanos. Una red de área amplia (WAN, Wire Area Network) es un sistema de redes de largo alcance. Las redes WAN pueden extenderse a lo largo de países y continentes. En la realidad la tecnología de red esta omnipresente y no tiene claras las decisiones entre redes LAN y redes WAN.

Generalmente, se considera como redes de área amplia a todas aquellas que cubren una extensa área geográfica, requieren atravesar rutas de acceso público, y utilizan parcialmente circuitos proporcionados por una entidad proveedora de servicios de telecomunicación. Típicamente, una WAN consiste en una serie de dispositivos de conmutación interconectados. La transmisión generada por cualquier dispositivo se encaminara a través de estos nodos internos hasta alcanzar el destino. A estos nodos (incluyendo a los situados en los entornos) no les concierne el contenido de los datos, al contrario, su función es proporcionar el servicio de conmutación, necesario para transmitir los datos de nodo en nodo hasta alcanzar su destino final.

Una WAN que se extiende sobre un área geográfica amplia, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar programas de usuario (aplicaciones), estas maquinas se llaman Hosts. Los hosts están conectados por una subred de comunicación. El trabajo de una subred es conducir mensajes de un host a otro. La separación entre los aspectos exclusivamente de comunicación de la red (la subred) y los aspectos de aplicación (hosts), simplifica enormemente el diseño total de la red.

En muchas redes de área amplia, la subred tiene dos componentes distintos: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión (también llamadas circuitos o canales) mueven los bits de una máquina a otra.

Los elementos de conmutación son computadoras especializadas que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación debe escoger una línea de salida para enviarlos. Como término genérico para las computadoras de conmutación, les llamaremos enrutadores.

En redes de área amplia (WAN). Los usuarios y los procesadores están distantes cientos ó miles de kilómetros. Ejemplo: las sucursales regionales de un banco con la matriz.

CONSTITUCIÓN DE UNA RED DE ÁREA AMPLIA (WAN)

La red consiste en ECD (computadoras de conmutación) interconectados por canales alquilados de alta velocidad (por ejemplo, líneas de 56 kbit / s). Cada ECD utiliza un protocolo responsable de encaminar correctamente los datos y de proporcionar soporte a las computadoras y terminales de los usuarios finales

conectados a los mismos. La función de soporte ETD (Terminales / computadoras de usuario). La función soporte del ETD se denomina a veces PAD (Packet Assembly / Disasembly – ensamblador / desensamblador de paquetes). Para los ETD, el ECD es un dispositivo que los aísla de la red. El centro de control de red (CCR) es el responsable de la eficiencia y fiabilidad de las operaciones de la red.

CARACTERISTICAS DE UNA RED DE COBERTURA AMPLIA

Los canales suelen proporcionarlos las compañías telefónicas, con un determinado costo mensual si las líneas son alquiladas.

- Los enlaces son relativamente lentos (de 64 Kbps a 2.048 Mbps).
- Las conexiones de los ETD con los ECD son generalmente más lentas (150 bit / s a 19.2 kbit / s).
- LOS ETD y los ECD están separados por distancias que varían desde algunos kilómetros hasta cientos de kilómetros.

Las líneas son relativamente propensas a errores (si se utilizan circuitos telefónicos convencionales).

Debido a las diferencias entre las redes de área local y las redes de cobertura amplia, sus topologías pueden tomar formas muy diferentes.

La estructura de las WAN tiende a ser más irregular, debido a la necesidad de conectar múltiples terminales, computadoras y centros de conmutación. Como los canales están alquilados mensualmente (a un precio considerable), las empresas y organizaciones que los utilizan tienden a mantenerlos lo más ocupados posible. Para ello, a menudo los canales "serpentean" por una determinada zona geográfica para conectarse a los ETD allí donde estén. Debido a eso la topología de las WAN suele ser más irregular.

Por el contrario el propietario de una LAN no tiene que preocuparse de utilizar al máximo los canales, ya que son baratos en comparación con su capacidad de transmisión (los cuellos de botella en las LAN suelen estar en el Software). Por tanto, no es crítica la necesidad de esquemas muy eficientes de multiplexado y multidistribución. Además, en las redes de área local que residen en un mismo edificio, la topología tiende a ser más ordenada y estructurada, con configuraciones en forma de bus, anillo o estrella.

Ahora bien hacemos mención en este capitulo de conceptos que tienen que ver con las formas más habituales con las que operan las WAN, tradicionalmente, las WAN se han implementado usando alguna de las tecnologías ó técnicas de conmutación siguientes: conmutación de circuitos y conmutación de paquetes. Aunque últimamente, se esta empleando como solución la técnica de retransmisión de tramas (Frame Relay), así como las redes ATM.

CONMUTACIÓN DE CIRCUITOS

En las redes de conmutación de circuitos se establece a través de los nodos de la red un camino dedicado a la interconexión de dos estaciones. El camino es una secuencia conectada de enlaces físicos entre nodos. En cada enlace, se dedica un canal lógico a cada conexión. Los datos generados por la estación fuente se transmiten por el camino dedicado tan rápido como se pueda. En cada nodo, los datos de entrada se encaminan o conmutan por el canal apropiado de salida sin retardos. El ejemplo más ilustrativo de la conmutación de circuitos es la red telefónica.

CONMUTACIÓN DE PAQUETES

Un enfoque diferente al anterior es el adoptado en redes de conmutación de paquetes. En este caso, no es necesario hacer una reserva a priori de recursos (capacidad de transmisión) en el camino (o sucesión de nodos). Por el contrario, los datos se envían en secuencias de pequeñas unidades llamadas paquetes. Cada paquete se pasa de nodo a nodo en la red siguiendo algún camino entre la estación origen y la destino. En cada nodo, el paquete se recibe completamente, se almacena durante un intervalo breve y posteriormente se transmite al siguiente nodo. Las redes de conmutación de paquetes se usan fundamentalmente para comunicaciones terminal-computador y computador-computador.

CLASIFICACIÓN LÍNEAS DE CONMUTACIÓN

Líneas Conmutadas: Líneas que requieren de marcar un código para establecer comunicación con el otro extremo de la conexión.

Líneas Dedicadas: Líneas de comunicación que mantienen una permanente conexión entre dos o más puntos. Estas pueden ser de dos o cuatro hilos.

Líneas Punto a Punto: Enlazan dos DTE

Líneas Multipunto: Enlazan tres o más DTE

Líneas Digitales: En este tipo de línea, los bits son transmitidos en forma de señales digitales. Cada bit se representa por una variación de voltaje y esta se realiza mediante codificación digital en la cual los códigos más empleados son: Manchester, Manchester Diferencial, TTL, NRZ, etc.

Las tecnologías de WAN más habituales son: HDLC, PPP, X25, Frame Relay, ATM, RDSI, MPLS.

d) REDES SAN y BACKEND

SAN (Storage Area Network) es una red independiente de almacenamiento de altas prestaciones basada en tecnología Fibre Channel. Su función es centralizar el almacenamiento de los ficheros en una red de alta velocidad y máxima seguridad. Es una solución global donde se comparte toda el área de almacenamiento corporativo. Fibre Channel: Es un estándar de conexión de alto rendimiento diseñado para realizar comunicaciones bidireccionales de datos en serie entre servidores, subsistemas de almacenamiento masivo y periféricos, a través de concentradores, conmutadores y conexiones punto a punto. Fibre Channel proporciona conectividad de larga distancia y el ancho de banda necesario para transferir de forma eficaz grandes archivos de datos entre el servidor y los sistemas de almacenamiento. Desaparecen las limitaciones de SCSI (Small Computer System Interface). Resulta ideal para redes SAN, grupos de ordenadores y otras configuraciones informáticas en las que existe un flujo de datos intensivo. El Fibre Channel puede ir tanto sobre cable de cobre como en fibra óptica.

Una SAN es una red independiente para gestionar las necesidades de almacenamiento. La SAN despliega las tareas de almacenamiento de servidores específicos y crea un servicio de almacenamiento compartido a través de una red de alta velocidad. Entre el conjunto de dispositivos de almacenamiento de la red se pueden encontrar discos duros, unidades de cinta y dispositivos CD. La mayor parte de las SAN hacen uso de canales de fibra.

Las redes de almacenamiento pueden ser grandes, complejas y costosas. Uno de los grandes retos al construir una red de ese tipo es decidir qué tecnología usar. SCSI tiene limitaciones de distancia y carece de rutas redundantes de datos. El canal de fibra (fibre channel) posee canales redundantes de datos (en un formato conmutado) y maneja distancias mucho más grandes, de hasta 10 kilómetros. La implementación y mantenimiento de ambas tecnologías, pero sobre todo el canal de fibra, requiere conocimientos especializados. La promesa de las SAN (redes de área de almacenamiento) es que el almacenamiento se usará de forma más eficaz y será más fácil reasignarlo. No obstante, la realidad es que una SAN requiere gran cantidad de tiempo, recursos y capacitación. La SAN se creó porque las primeras redes ethernet/IP no podían manejar volúmenes elevados de tráfico. El canal de fibra nació de la necesidad de una red rápida, dedicada y robusta para almacenamiento. En fechas más recientes, los avances en tecnología ethernet, junto con el deseo de simplificar la capacitación, el hardware y el soporte, han hecho posible iSCSI (Internet SCSI). Lo que se busca es incluir todo en un solo tipo de plataforma de red. Esto no necesariamente implica que el tráfico de almacenamiento viajará por la misma red que el tráfico general de datos. Lo más común es que una SAN empresarial exista como entidad aparte de la red general de datos. De hecho, desde el punto de vista de la implementación, cabe esperar que la red de almacenamiento basada en iSCSI siga siendo una entidad aparte. Por otra parte el uso de la misma tecnología en las redes generales de datos y en las SAN reduciría los costos sobre la contratación y capacitación de personal, y la amplia base instalada de ethernet deberá bajar los costos de precio-desempeño. La ventaja más importante es que se puede aprovechar la infraestructura TCP/IP existente, que es fácil de entender, para construir redes SAN. Con los adelantos en calidad de servicio (QoS) y seguridad, la oportunidad de compartir almacenamiento con la infraestructura existente representa un ahorro importante en los costos por concepto de hardware, capacitación e implementación.

Las redes de respaldo (Backend) se utilizan para interconectar grandes sistemas tales como computadoras centrales, supercomputadoras, y dispositivos de almacenamiento masivo. El requisito principal en este caso es la transferencia elevada de datos entre un numero limitado de dispositivos en un área reducida, siendo también necesaria generalmente una alta fiabilidad. Entre sus características típicas se encuentran las siguientes:

- Alta velocidad: se precisan velocidades de 100 Mbps o más para satisfacer la demanda de alto volumen de tráfico.

- Interfaz de alta velocidad: las operaciones de transferencia de datos entre un gran sistema anfitrión y un dispositivo de almacenamiento masivo se realizan generalmente a través de interfaces de entrada/salida paralelo de alta velocidad en lugar de a través de interfaces de comunicaciones más lentas. Por lo tanto, el enlace físico entre la estación y la red debe ser de alta velocidad.
- Acceso distribuido: se necesita una técnica de control distribuido de acceso al medio (MAC) para permitir que varios dispositivos compartan el medio mediante un acceso eficiente y fiable.
- Distancia limitada: generalmente las redes de soporte se emplean en salas de computadoras o en un número reducido de habitaciones contiguas.
- Número limitado de dispositivos: el número de computadoras principales y dispositivos de almacenamiento masivo caros existentes en una sala de computadoras es generalmente del orden de las docenas.

Generalmente, las redes de respaldo se encuentran en grandes compañías o en instalaciones de investigación con alto presupuesto en procesamiento de datos.

Consideremos un lugar donde se hace uso de una computadora principal dedicada, lo que implica una aplicación grande o un conjunto de aplicaciones. Si la carga crece la computadora principal puede reemplazarse por una más potente, quizá por un sistema multiprocesador. En algunos lugares no basta con colocar un solo sistema dado que el crecimiento de la demanda supera el aumento de las prestaciones del equipamiento, por lo que se precisaran eventualmente varias computadoras independientes. De nuevo, existen razones que fuerzan la interconexión de estos sistemas. El costo de la interrupción del sistema es alto, de modo que sería posible, fácil y rápido, trasladar las aplicaciones a sistemas de respaldo. Debe ser posible testar nuevo procedimientos y aplicaciones sin degradar el sistema de producción. Los ficheros de gran tamaño deben ser accesibles por parte de más de una computadora. El equilibrado de la carga posibilitaría la maximización de la utilización de las prestaciones.

Se pueden observar que algunos de los requisitos principales para redes de salas de computadoras son los contrarios a los de las LAN de computadoras personales. Se requieren altas velocidades para trabajar adecuadamente, lo que implica generalmente la transferencia de bloques de datos de gran tamaño. Afortunadamente, aunque el costo del equipamiento para conseguir altas velocidades es alto, este es razonable debido al costo mucho mayor de los dispositivos conectados.

Un concepto relacionado con el de la red de respaldo es el de la red de almacenamiento (SAN, Storage Área Network), ya antes mencionada.

e) RED GAN

Redes de área global (GAN, Global Area Network), son redes que cubren todo el mundo y une todas las redes, el ejemplo más claro de una red de este tipo lo tenemos en la Red Global Internet ó internets La red Internet es aquella que se ha derivado de un proyecto del departamento de defensa de Estados Unidos y que ahora es accesible desde más de 2 millones de nodos en todo el mundo, y cuyos servicios típicos son las conexiones con emulación de terminal telnet, la transferencia de archivos ftp, el W W W, el correo electrónico, los foros de información globales NetNEWS. Por otro lado, se consideran como internets (con la letra "i" minúscula) a aquellas redes públicas o privadas que se expanden por todo el mundo. El asunto interesante es que estas internets pueden valerse del Internet en algunos tramos para cubrir el mundo. La restricción mayor para que una red privada se expanda en el mundo usando Internet es que puede verse atacada por usuarios del Internet. Un esquema de seguridad para este caso puede ser que, para las LANs que conforman la internet privada, cada una de ellas encripte su información antes de introducirla a Internet y se decodifique en las LANs destinos, previo intercambio de las claves o llaves de decodificación, este tipo de esquemas se pueden lograr con el uso de firewalls.

El Internet es una gigantesca colección de millones de computadoras que están unidas mediante una Red Computacional, también llamada red global (GAN, Global Area Network). Esta red permite que todas las computadoras se comuniquen entre sí. Una manera de conectarse a la GAN es con una computadora casera conectada usualmente a Internet utilizando una línea telefónica normal y un módem que se comunica con un ISP (Internet Service Provider, o proveedor de servicios de Internet). Una computadora de alguna empresa ó universidad que posea una tarjeta **NIC** (Network Interface Card, o tarjeta para interfase en red) que se conecta

directamente a una LAN (Local Area Network, o red de área local) dentro de la empresa puede tener un acceso mediante un servidor dedicado a darles salida las computadoras de la LAN hacia Internet. Toda la entidad conecta su LAN a un ISP utilizando una línea telefónica de alta velocidad como por ejemplo una línea T1 (una línea T1 puede manejar aproximadamente 1.5 millones de bits por segundo, mientras que una línea telefónica normal usando un módem debe ser capaz de manejar de 30000 a 50000 bits por segundo).

1.3 TIPOS DE REDES POR APLICACIÓN

a) REDES DE VOZ

Para hacer una pequeña descripción de las redes no podemos omitir que para que las redes de todos tipos existieran necesariamente tuvo que haber algo que sentara la idea y un precedente del origen de todas la tecnologías, conceptos y desarrollo de las redes existentes.

Bajo esas circunstancias en este punto tratamos de manera breve el contexto que ocupan la redes de voz, llamadas también redes de telefonía. Estas recordemos que nacen con la aparición del telégrafo y teléfono como primeros inventos que vienen a revolucionar y facilitar el esquemas de las comunicaciones existentes hasta esos días. Las primeras redes de telecomunicaciones aparecen en el siguiente orden cronológico y la figura (1.3a) muestra la cronología de desarrollo telefónico.

➢ 1793 Claude Chappe introduce en Francia el telégrafo óptico con una línea de 190 Km que unía París con Lille a través de 15 estaciones. Y para 1852 la red contaba con 556 estaciones, se extendía mas de 4800 Km y cubría casi toda Francia, la velocidad promedio de los telégrafos ópticos era de 0.5 bps.
➢ 1839 entra en operación en Inglaterra, el telégrafo eléctrico desarrollado por William Cook y Charles Whcatstone.
➢ 1844 se usa el uso del teléfono eléctrico, desarrollado por Samuel Morse, Joseph Henry y Alfred Vail, en Estados Unidos.
➢ 1851 se fundan las primeras compañías telegráficas.
➢ 1858 primer cable telegráfico submarino transatlántico.
➢ 1875 s encuentra en operación mas de 300,000 Km de líneas de telégrafos y el telégrafo eléctrico es capaz de transmitir a 30 bps.
➢ 1876 Alexander Grahambell patenta el teléfono.
➢ 1878 se establece el primer sistema comercial telefónico con 21 usuarios en New Haven, C.T.
➢ 1881 la primera llamada de larga distancia para el publico
➢ 1891 el primer sistema de marcado automático
➢ 1897 Guillermo Marconi hace posible la telegrafía inalámbrica.
➢ 1900 se desarrollo un dispositivo para la amplificación de líneas telefónicas.
➢ 1901 primera transmisión telegráfica inalámbrica transatlántica.
➢ Las redes de telex surgen de la idea de conectar teletipos e impresoras directamente a las líneas telegráficas.
➢ 1915 New York - San Francisco línea telefónicas abiertas.
➢ 1925 se encuentran en operación redes completas de telex (telegraph exchange) y la red mundial conmutada de telex es un sistema de teleimpresión que opera a 50 bps, aunque en algunos países funciona a 200.
➢ 1927 New York - London se abren líneas telefónicas comerciales
➢ 1927 primer circuito radiotelefónico trasatlántico.
➢ 1956 primer cable telefónico submarino transatlántico.
➢ 1958 los laboratorios Bell desarrollan los modems.
➢ A principios de la década de 1960 se introducen enlaces digitales.
➢ 1965 se introducen los satélites de comunicación comerciales y son más rutinarias las conversaciones transoceánicas.
➢ 1965 sistema electrónico de conmutación con la primer central eléctrica
➢ A mediados de la década de 1970 se introducen sistemas de conmutación digital.
➢ La introducción de los modems hizo posible el uso de líneas telefónicas para enlazar terminales a computadoras, sin embargo la técnica de conmutación de circuitos no es la adecuada para la transmisión de tráfico de ráfagas.
➢ 1988 el primer cable submarino de fibra óptica.
➢ 1994 utilización de la telefonía utilizando a Internet
➢ En la actualidad estamos viviendo la transición a redes telefónicas completamente digitales.

Figura (1.3a)

Y es la infraestructura telefónica de hecho la que marca el nacimiento de las redes de datos ya que sobre los recursos y la plataforma de las redes telefónicas descansan innumerables servicios que a su vez soportan gran parte de los esquemas de red existentes.

En los inicios de la telefonía, la voz sobre las líneas telefónicas era casi inaudible. Las tarifas de las llamadas de larga distancia eran muy costosas, lo cual hacia prácticamente accesible la telefonía solo para las grandes empresas. El teléfono rápidamente paso a ser una extensión mas del cuerpo humano.

Hoy en día las redes de paquetes de la siguiente o nueva generación pueden transportar voz, datos y vídeo sobre una infraestructura común. Los proveedores de servicios y los operadores (Carriers), tienen un gran potencial en la entrega de la nueva generación de servicios de voz y telefonía con la integración de tecnologías como WEB e IP. El Reto se encuentra en la rápida integración de estos servicios. Una de las sorprendentes innovaciones para la comunicación en los tiempos recientes es VoIP, Voz sobre el protocolo de Internet, el cual permite a los usuarios de Internet tener conversaciones telefónicas a través de plataformas y continentes.

Se predice que el tráfico IP de todo el mundo sobrepasara el tráfico de las redes de telefonía pública conmutada (PSTN) dentro de unos cuantos años, y nuevas redes están siendo construidas solo para manejar tráfico IP. Al mismo tiempo, el tráfico de datos está comenzando a ser un auténtico rival del tráfico de voz en términos de la demanda de la red.

El sistema mundial de redes conmutadas interconectadas entre sí, representan una gran inversión de equipamiento, sistemas de soporte y recursos técnicos. Es muy probable que en los próximos años, todo el tráfico IP sea transportado sobre redes conmutadas y la mayoría de las redes serán híbridas, construidas por IP y hardware conmutado.

Mientras que los estándares para desarrollar servicios basados en IP se están formulando, la naturaleza subdesarrollada de las operaciones convergentes de la red, implica que muchas áreas claves sean necesitadas para construir servicios y las cuales están comenzando a ser tratadas. Los estándares para la interoperabilidad son generalmente los primeros que se adoptarán en cualquier segmento de telecomunicaciones, y mientras que están emergiendo los productos basados en H.323, justo ahora comienzan a ser probados. Dentro de la red IP, las terminales, los Gateways, y las enrutadores utilizan el protocolo H.323.

H.323 es un estándar que se ha sido adoptado para la telefonía IP; es la especificación de la unión de telecomunicaciones internacional (ITU) para las comunicaciones de multimedia sobre redes de datos que no asignan un nivel de calidad de servicio (QoS). H.323 proporciona los estándares para la disposición y negociación de llamadas entre los
Gateways usando cualquier tipo de computadora en Internet.

El Gateway es el puente entre la red de teléfono regular y el mundo IP H.323. El Gateway asocia señales de llamada, control de llamada, y asocia los medios entre los circuitos y las redes de paquetes.

El siguiente nivel de la jerarquía es el portero (gatekeeper), quien controla muchas terminales y Gateways, además que proporciona una función de enrutamiento según el nivel de Calidad de Servicio (QoS) u otras características indicadas en el encabezado de los paquetes

b) REDES DE DATOS

Las primeras redes construidas permitieron la comunicación entre una computadora central y terminales remotas. Se utilizaron líneas telefónicas, ya que estas permitían un traslado rápido y económico de los datos. Se utilizaron procedimientos y protocolos ya existentes para establecer la comunicación y se incorporaron moduladores y demoduladores para que, una vez establecido el canal físico, fuera posible transformar las señales digitales en analógicas adecuadas para la transmisión por medio de un módem.

Posteriormente, se introdujeron equipos de respuesta automática que hicieron posible el uso de redes telefónicas públicas conmutadas para realizar las conexiones entre las terminales y la computadora. A principios de los años 70 surgieron las primeras redes de transmisión de datos destinadas exclusivamente a este propósito, como respuesta al aumento de la demanda del acceso a redes a través de terminales para poder satisfacer las necesidades de funcionalidad, flexibilidad y economía. Se comenzaron a considerar las ventajas de permitir la comunicación entre computadoras y entre grupos de terminales, ya que dependiendo del grado de similitud entre computadoras es posible permitir que compartan recursos en mayor o menor grado.

La primera red comercial fue la *TransCanada Telephone System's Dataroute*, a la que posteriormente siguió el *Digital Data System* de AT&T. Estas dos redes, para beneficio de sus usuarios, redujeron el costo y aumentaron la flexibilidad y funcionalidad. Durante los años 60 las necesidades de teleproceso dieron un enfoque de redes privadas compuesto de líneas (leased lines) y concentradores locales o remotos que usan una topología de estrella. El concepto de redes de datos públicas emergió simultáneamente. Algunas razones para favorecer el desarrollo de redes de datos públicas es que el enfoque de redes privadas es muchas veces insuficiente para satisfacer las necesidades de comunicación de un usuario dado. La falta de interconectividad entre redes privadas y la demanda potencial de información entre ellas en un futuro cercano favorecieron el desarrollo de las redes públicas.

c) RAS

(Remote Access Server, RAS) Hace mucho años, la forma mas común de acceder a una red de forma remota era llamando a una estación de trabajo de la red que tuviese un software de acceso remoto, por ejemplo pcANYWHERE o Carbon Copy. Esta estación de trabajo, la mayoría de las veces, solo dejaba trabajar a un único usuario que llamaba desde la computadora de su casa. El acceso era frustrante por que los módems eran lentos, en algunas veces la computadora que estaba conectada a la red se apagaba accidentalmente y, para colmo, no había forma de utilizar el ratón en la conexión remota. A principios de los años 90, la empresa Novell mejoro la tecnología introduciendo el servidor de acceso NetWare (NAS, NetWare Access Server). El objetivo original de NAS fue realizar un nodo que estuviese conectado a la red y que hiciese la función de varias estaciones de trabajo. Por ejemplo, una computadora de red funcionando como NAS podría contener cinco tarjetas de MODEM, permitiendo que el número de usuarios que pudiesen estar conectados a la red fuese cinco, uno por cada tarjeta de MODEM. Cada usuario podría utilizar una parte concreta de la computadora, incluida la CPU y espacio en el disco duro. El NAS funcionaria como si cinco estaciones de trabajo estuviesen en su interior. Microsoft ha desarrollado el acceso remoto al hacer que un servidor de red Windows NT(o una estación de trabajo) se pueda convertir en un servidor RAS capaz de manejar cientos de conexiones simultáneas. instalando los servicios de acceso remoto (Remote Access Server, RAS). Windows NT Server realiza sus funciones normales como servidor pero al mismo tiempo realiza las funciones de servidor de acceso remoto. Un usuario puede acceder a un servidor RAS con su nombre de cuenta y contraseña. Si esta instalado NWLink en la estación de trabajo del usuario, y el servidor RAS tiene configurado IPX, el usuario puede proporcionarle una contraseña para conectarse al mismo tiempo a un servidor NetWare. Los servicios de acceso remoto RAS son servicios de software que permiten a las estaciones de trabajo que no pertenecen a la red poder acceder al servidor Windows NT a través de una línea telefónica analógica o digital (RDSI).

Lo servidores de acceso remoto ofrecen de modo consistente y altamente seguro al usuario remoto un acceso transparente a la red LAN a través de la red telefónica conmutada (RTC). Respecto a los servidores de acceso remoto, los usuarios pueden acceder telefónicamente utilizando conexiones normales de la RTC vía módems analógicos con velocidades de transmisor de hasta 33.6 Kbps y 56 Kbps (el uso de módems 56 Kbps-V.90 también es posible). Un servidor de acceso remoto normalmente soportara entre 2 y 16 usuarios y suele tener puertos fijos, lo que significa que no es escalable. Este método de acceso remoto se utiliza con más frecuencia en la pymes o para aplicaciones especificas de departamentos y grupos de trabajo.

Los servidores de acceso remoto apoyan un mayor número de llamadas entrantes simultáneas. Lo consiguen utilizando canales T1/E1/PR1 de alta capacidad o conexiones RDSI BRI y la tecnología de telefonía conmutada. La mayor densidad de puertos proporcionada por los servidores de acceso remoto simplifica los problemas relacionados con la seguridad y la administración ya que el administrador de red tiene que encargarse de un solo punto de acceso a los recursos de sistemas abiertos para todos los usuarios remotos. Los servidores de acceso remoto generalmente son escalables de modo que puedan adaptarse al futuro crecimiento y soportaran llamadas RDSI de igual modo que las analógicas a través de la misma línea T1/E1/PR1 o BRI (incluyendo el soporte de módems digitales V.34 Y 56Kbps-V.90).

d) REDES ISP

Los ISP se conectan a otros ISP más grandes, y éstos mantienen conexiones de fibra óptica llamados "backbones" (backbone significa columna vertebral) para una nación o región. Los backbones están conectados alrededor del mundo mediante cables submarinos o conexiones satelitales. De esta forma cada computador en Internet está conectado con los demás. La figura (1.3b) muestra la conexión de varios proveedores ISP conectados al backbone.

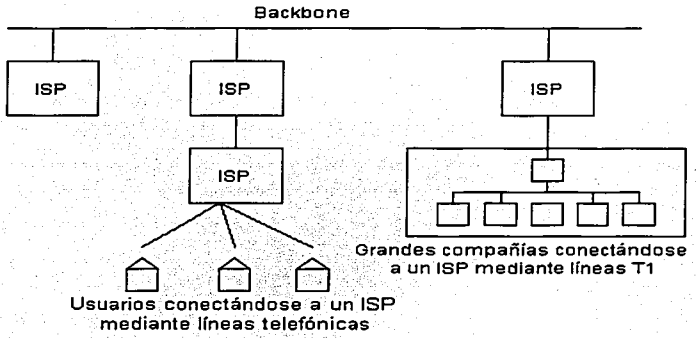


Figura (1.3b)

e) REDES ASP

Un Proveedor de Servicios de Aplicaciónes (ASP, Application Services Provider), ofrece el servicio externo de aplicaciones orientadas a la web (servidor web, hosting de webs,...), así como de aplicaciones de e-business para pequeñas, medianas o grandes empresas.

El ASP Industry Consortium amplía esta definición en los siguientes términos:

Los Proveedores de Servicios de Aplicaciones (ASPs), hospedan, despliegan y gestionan aplicaciones y servicios informáticos desde centros de datos remotos a múltiples usuarios a través de Internet o de una red privada. Las aplicaciones se entregan sobre las redes mediante suscripción. Para una pequeña, mediana o gran compañía, el obtener estas aplicaciones de un suministrador externo es una solución de bajo costo para satisfacer las necesidades de propiedad de sistemas que exigen anticipación del gasto, retos de implantación y una necesidad continua de mantenimiento, migración y personalización. Un ASP puede ser tanto una entidad comercial, o una organización oficial o sin ánimo de lucro que proporcione soporte a los usuarios. Muchos ASP son también ISP u operadores de telecomunicaciones.

Los ASP Proporcionan un acceso a información y a soluciones generadas por el uso de algún servicio ó tecnología en cualquier momento y en cualquier lugar.

f) REDES DE VIDEO

Se pueden realizar videoconferencias a través de líneas telefónicas tradicionales (analógicas), a través de equipos que cuentan con el protocolo H.324 es posible, sin embargo no es muy recomendable para uso profesional ya que al utilizar las líneas analógicas con un ancho de banda de solamente 64 kbps (kilobits por segundo) la calidad es muy pobre. La sugerencia es utilizar al menos 128 kbps. Con la que alcanzamos 15 cuadros por segundo (fps). Y ésta se logra solamente con líneas digitales. Nos referimos con líneas digitales a diferencia de las analógicas, aquellas que fueron creadas originalmente para la voz, y éstas nacieron para poder transmitir datos y voz, con la diferencia de que en lugar de enviar frecuencias se envían bits de información, por lo que si se envía voz, esta se digitaliza y se envía, y además es posible recuperarla del otro lado prácticamente sin ruido, por lo tanto con una excelente calidad, los datos se envían desde su origen como bits, por lo que no hay problemas con pérdida de información. Cuando surge la necesidad de enviar imágenes y vídeo utilizando éstas líneas, surge la videoconferencia, que es la tecnología que hace posible aprovechar ésta infraestructura pero ahora dedicada a voz,datos y vídeo. Las líneas digitales pueden ser:

- Enlaces dedicados; que se contratan de 64 kbps. (DS0's ó E0's) ó líneas de 2,048 kbps. (E1's). Con interfaces V.35, G.703, RS-449, X.25, utilizando el protocolo de videoconferencia H.320.

- Líneas telefónicas digitales conmutadas (ISDN). Que se contratan de 128 kbps. (BRI's) ó líneas de 2,048 kbps. (PRI's), utilizando el protocolo de videoconferencia H.320.

Redes de Area Local (LAN=Local Area Network) ó Redes de área Extendida (WAN=Wide Area Network), utilizando el protocolo de videoconferencia H.323 (IP).

1.4 MEDIOS DE TRANSMISIÓN EN REDES

NOMENCLATURA DE LOS MEDIOS DE TRANSMISIÓN

La denominación de estas especificaciones es la siguiente:

- 10 indica la velocidad de transmisión del cable.
- La nomenclatura BASE significa que la transmisión se realiza en **banda base** en lugar de **banda ancha**.
- El 5 y el 2 indican que el cable será 5 ó 2 X 100 mts en cable coaxial.

- Cable de par trenzado apantallado (STP, Shielded Twisted Pair).
- Cable de par trenzado sin apantallar (UTP, Unshielded Twisted Pair). Por lo que al UTP se le conoce popularmente como 10BASE-T; con velocidades de Tx desde 10 hasta 100 Mbps según la categoría del cable.

Ya se menciono que Ethernet es una red de bus CSMA/CD, que por lo regular se implementa como una red de cable coaxial de banda base 10Mbps o bien como una red de par trenzado de 10 Mbps, aunque en los documentos normativos podemos contemplar otro tipo de medios de transmisión:

- 10BASE5: cable coaxial grueso (0.5 pulgadas de diámetro) con una longitud máxima de 500m.
- 10BASE2: cable coaxial delgado (0.25 pulgadas de diámetro) con una longitud máxima de 200m.
- 10BASE-T: topología de concentrador con cables de extensión de par trenzado.
- 10ANCHA36: especificación de banda ancha.
- 10BASE-F: topología de concentrador con cables de extensión de fibra óptica.

Aunque se usan diferentes medios todos utilizan el mismo método de control de acceso al medio.

10BASE5

La especificación 10BASE5 emplea cable coaxial de 50 ohmios, así como señalización digital Manchester. La longitud máxima entre varios repetidores es de 500m, siendo la longitud máxima entre dos estaciones de 2,5 km (por tanto, son necesarios 4 repetidores).

Al emplear cable coaxial grueso los circuitos del transceptor se colocan en el punto de derivación del cable, a lo que se le denomina unidad integrada de derivación y transceptor.
El transceptor contiene los circuitos electrónicos que nos permiten:

- Enviar datos al cable y recibirlos.
- Detectar colisiones en el medio del cable

Además, el transceptor debe proporcionar un aislamiento eléctrico entre el cable y los circuitos de la interfaz, así como proteger al cable de los posibles fallos en la estación. A esta función se le denomina control de parloteo, ya que si no existe tal protección puede introducirse en el canal un flujo aleatorio de bits (parloteo) que alteran el resto de las transmisiones. El control de parloteo aísla la línea de transmisión, del cable transceptor si se violan ciertos límites de tiempo definidos.
La unidad transceptora se conecta con la estación por medio de un cable blindado que contiene cinco cables de par trenzado (para alimentación, dos para datos, dos para funciones de control).
La estación puede estar a una distancia de hasta 50m de la unidad transceptora, esto es, del punto de derivación.

10BASE2

La especificación 10BASE2 nos proporciona una red local con un costo menor que el 10BASE5, así como una instalación más sencilla (debido a la menor rigidez del cable). A las redes de cable coaxial delgado de bus CSMA/CD también se les denomina Cheapernets. El tipo de cable que emplean es coaxial de una impedancia de 50 ohmios, y de un diámetro de 0.25 pulgadas. Emplean señalización Manchester.

A pesar de la menor calidad del cable la velocidad de transmisión de una Cheapernet es la misma que una Ethernet de cable grueso. Sin embargo, el número de conexiones, así como la longitud máxima de la red es menor.
Otra de las principales diferencias radica en la unidad transceptora.

10BASE-T

Sacrificando distancia, se puede desarrollar una red local a 10 Mbps haciendo uso de un par trenzado no apantallado. La topología de este tipo de especificación es en estrella. Es un sistema sencillo que consiste en varias estaciones conectadas a un punto central denominado repetidor multipuerto. El punto central acepta la entrada y la repite en todas las direcciones.
Debido a la alta velocidad y pobre calidad de transmisión del par trenzado, la longitud del enlace es bastante limitada (100 m).
Como alternativa, puede utilizarse un enlace de fibra óptica (500 m).

10ANCHA36

Esta es la única especificación para banda ancha, donde el medio empleado es un cable coaxial de impedancia 75 ohmios.
La técnica de modulación más empleada, es por desplazamiento de fase PSK, en la cual un 0 binario se representa por una portadora con una determinada fase, y un 1 binario, por la portadora en oposición de fase.
También existe otra técnica: DPSK, que hace uso de una codificación diferencial (cuando se produce un cambio de fase aparece un 0, en caso contrario, tenemos un 1. Esto simplifica el receptor).

10BASE-F

Con la presente especificación, se permite aprovechar las características en cuanto a distancia y velocidad de transmisión de la fibra óptica. Existen tres normalizaciones, pero todas ellas utilizan un par de fibras ópticas para cada enlace de transmisión (para cada dirección).
Generalmente, suele usarse codificación Manchester, de manera que la presencia de luz se interpreta como estado alto y la ausencia como estado bajo.

ETEHERNET DE ALTA VELOCIDAD

Ethernet de alta velocidad son un conjunto de especificaciones, cuyo fin es proporcionar una red local de bajo costo compatible con ethernet y de alta velocidad (100Mbps). El conjunto de todas las normalizaciones es 100 BASE-T, de tal modo que podemos encontrar diferentes variantes en función del medio de transmisión.
El principal problema con la Ethernet rápida es cómo lograr una tasa de transferencia de datos de 100 Mbps por 100 m 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 tres; y la otra, para cables de par trenzado blindado STP de categoría cinco, o bien con fibras ópticas. La primera norma se denomina 100BASE4T y la segunda, 100BASEX.

100BASE4T

100BASE 4T, está pensado para ofrecer una velocidad de 100Mbps mediante un cable UTP de categoría tres, que contiene cuatro pares de hilos trenzados independientes. Así, los datos se transmiten haciendo uso de tres pares y se reciben a través de otros tres, de manera que la tasa de transmisión efectiva en cada uno, es de 33.3 Mbps.

En esta especificación no se emplea un esquema de codificación en NRZ (no proporciona sincronización). En general, se emplea un código ternario (de tres niveles) en lugar de una codificación binaria (de dos niveles) simple. Al código se le denomina 8B6T, porque antes de ser transmitido, cada conjunto de 8 bits binarios se convierte en 6 símbolos ternarios. Los tres niveles de señal empleados son: +, 0, -.

100BASEX

Está diseñado para cables de más alta calidad, que son los que actualmente se instalan en la mayor parte de las redes (cable de categoría cinco). Además, está pensado para emplearse con cables de STP y fibra óptica. La X se debe a que se puede aplicar en diversos medios de transmisión.
Cada tipo de medio de transmisión requiere una subcapa PMD distinta. La primera en elaborarse fue la de cable de fibra óptica multimodal apropiada para las redes FDDI. En éstas, el esquema de codificación se realiza mediante 4B5B, en la que cada grupo de 4 bits de datos se codifica como un símbolo binario de 5 bits. Los símbolos se eligen de modo que se garantice una transición de señal, por lo menos cada dos bits, para poder mantener la sincronización de reloj.
Por ejemplo, la especificación 100BASEFX, utiliza dos fibras ópticas: una para transmitir y otra para recibir. En ésta es necesario algún método para convertir la secuencia de grupos de código (4B5B) en señales ópticas, conociéndose la técnica usada como modulación de intensidad. Un 1 binario se representa por una ráfaga o pulso de luz, mientras que un 0 binario, por la ausencia de pulso de luz, o en su defecto, por una de muy baja intensidad.

GIGABIT ETHERNET

La solución Gigabit Ethernet es la misma que la adoptada por la Fast Ethernet, en Gigabit Ethernet se sigue adoptando tanto el protocolo CSMA/CD, como el formato de sus predecesores Ethernet a 10 Mbps y 100 Mbps. Es compatible con 100BASET y 10BASET, facilitando la migración. La demanda de la tecnología Gigabit Ethernet ha crecido debido a que cada vez más organizaciones están adoptando 100BASET lo que implica cantidades enormes de tráfico en las líneas troncales.

MEDIOS INALÁMBRICOS

En virtud de que en este punto los medios y las posibilidades de conectividad, así como los dispositivos son todo un tema amplio solo nos concretamos a mencionar las características más relevantes de dichos medios de Transmisión, ya que el abordar cada uno de ellos de manera más amplia y particular sale fuera de los alcances de esta tesis.

Existen varios medios de transmisión inalámbricos para transmitir paquetes por la red: ondas de radio, infrarrojos, microondas y transmisiones satelitales. Todas estas tecnologías transmiten a través del aire o de la atmósfera y una característica que las hace ser una buena alternativa es en aquellas situaciones donde nos es difícil o imposible la utilización de cable.

En Radio las transmisiones en una red utilizan un ámbito de frecuencias que va de 902 a 928 Mhz, y su transmisión puede ser orientada de manera unidireccional como omnidireccional. Su transmisión más adecuada es con línea de vista para distancias largas ya que la ondas tienen longitud corta.

Para los rayos infrarrojos el intervalo de frecuencias oscila entre los 100 Ghz y 1000 Thz, el tipo onda es unidireccional y omnidireccional, tienen la desventaja de no poder atravesar paredes o medios sólidos, otra desventaja es que solo llegan hasta 16 Mbs en enlaces unidireccionales y 1 Mbps en comunicaciones omnidireccionales.

En un sistema de microondas la señal se transmiten mediante antenas parabólicas y la transmisión se realiza en los intervalos de frecuencia del espectro electromagnético de .3 a 300 Mhz. Pero con el inconveniente de los costos elevados por las transmisiones satelitales y además tienen el infortunio de ser muy sensibles en climas extremosos por lo que la atenuación de la señal es bastante grande.

Los satélites de comunicaciones tienen algunas propiedades interesantes que los hacen atractivos para muchas aplicaciones, ya que se les puede ver como una gran repetidora de microondas en el cielo. Un satélite contiene varios transponders, cada uno de los cuales capta alguna porción del espectro, amplifica la señal de entrada y después la redifunde a otra frecuencia para evitar la interferencia con la señal original. Los haces retransmitidos pueden ser amplios y cubrir una fracción sustancial de la superficie de la Tierra, o estrechos y cubrir un área de sólo cientos de kilómetros de diámetro.

Los sistemas tradicionales de comunicaciones vía satélite se basan en la idea de A. Clarke, las señales se transmiten entre las diferentes estaciones terrestres mediante un satélite situado en una determinada órbita de la Tierra. Estas señales viajan sobre una onda portadora en el margen de microondas y permiten transportar grandes cantidades de información al mismo tiempo que pueden focalizarse en haces extremadamente estrechos, lo que las hace especialmente apropiadas para las comunicaciones.

Esta focalización se realiza, mediante una antena, en un haz muy estrecho que se dirige al satélite. Cuando el satélite recibe el haz, las señales son extremadamente débiles debido al camino recorrido, por lo que debe amplificarlas para compensar la pérdida de potencia sufrida durante la transmisión por el espacio; tras amplificar el haz lo retransmite a la Tierra, en concreto, a las estaciones receptoras que deben recibir la señal. En este sentido, el satélite actúa como una estación repetidora en el espacio.

Cuando el satélite está diseñado únicamente para esta función de repetidor, es decir, para acoger la señal y retransmitirla otra vez a la tierra, se dice que el satélite es transparente. Los avances en la tecnología han permitido agregar a esta función básica inherente funciones de valor añadido en términos de control y comando de los circuitos de microondas del satélite, así como de procesamiento on-board, entre otros.

En el contexto de la transmisión se utilizan dos conceptos fundamentales: el enlace ascendente o uplink y el enlace descendente o downlink. El modo en que se utilizan estos enlaces es el siguiente. En la estación terrestre, la señal se superpone a la portadora a una determinada frecuencia y se envía al satélite (enlace ascendente); en el satélite, una vez que se ha amplificado la señal, se superpone a una portadora a una frecuencia diferente de la anterior y se envía a la Tierra (enlace descendente).

Bandas de frecuencia

El espectro electromagnético es un problema con el que todos nos enfrentamos. Los nombres más comunes para ciertas bandas frecuencia les datan de antes de la Segunda Guerra Mundial.

Aunque el IEEE intente imponer una convención de nombres estándares fáciles de usar, lo cierto es que la mayoría de las personas del sector se refieren a los segmentos del espectro de radio por una clasificación de bandas basadas en letras (que en general son imprecisas). En la Segunda Guerra Mundial, los desarrolladores de radares de los Estados Unidos y Gran Bretaña nombraron partes del espectro con letras, tales como la Banda L, Banda C, Banda Ku o Banda Ka. Las letras fueron escogidas de forma aleatoria, para que el enemigo no pudiera saber sobre lo que estaban hablando. Durante los siguientes años hubo discrepancias sobre los nombres y sus inconsistencias.

La **banda C** fue la primera en destinarse al tráfico comercial por satélite; en ella se asignan dos intervalos de frecuencia, el más bajo para tráfico de enlaces descendentes (desde el satélite) y el superior para tráfico de enlaces ascendentes (hacia el satélite). Para una conexión dúplex se requiere un canal en cada sentido. Estas bandas ya están sobre pobladas porque también las usan las portadoras comunes para enlaces terrestres de microondas.

La **banda Ku** es la banda más alta disponible para las portadoras de telecomunicaciones comerciales. Esta banda no está congestionada aún y a estas frecuencias los satélites pueden estar espaciados tan cerca como 1 grado. Esta banda proporciona más potencia que la C y, en consecuencia, el plato de la antena receptora puede ser más pequeño, del orden de 1.22 metros de diámetro, aunque la cobertura es mayor. A la banda Ku, no le afectan las interferencias terrestres, pero sí las turbaciones meteorológicas, por ejemplo, la lluvia, que produce distorsiones y ruido en la transmisión. Las tormentas fuertes casi nunca abarcan áreas extensas, de modo que con usar varias estaciones terrestres ampliamente separadas en lugar de una sola se puede resolver el problema, a expensas de gastar más en antenas, cables y circuitos electrónicos para conmutar con rapidez entre estaciones. Con la **banda Ka** se espera paliar la creciente saturación de las bandas C y Ku.

FIBRA ÓPTICA

El conductor de fibra óptica está compuesto por dos elementos básicos:

El núcleo (core) y el recubrimiento (cladding), cada uno de ellos formado por material conductor de las ondas luminosas. Así cuando hablamos de fibras de 50/125, 62.5/125 o 10/125 mm, nos estamos refiriendo a la relación entre el diámetro del núcleo y el recubrimiento.

Otro parámetro importante en una fibra es su apertura numérica. En los conductores de fibra óptica se utiliza el efecto de la reflexión total para conducir el rayo luminoso por su interior. El ángulo necesario para acoplar al núcleo un rayo luminoso desde el exterior recibe el nombre de ángulo de aceptación. Pues bien, el seno de este ángulo se denomina apertura numérica.

Un parámetro extrínseco a la fibra óptica es la ventana de trabajo. Cuando hablamos de ventanas de trabajo nos referimos a la longitud de onda central de la fuente luminosa que utilizamos para transmitir la información a lo largo de la fibra. La utilización de una ventana u otra determinará parámetros tan importantes como la atenuación que sufrirá la señal transmitida por kilómetro.

Las ventanas de trabajo más corrientes son: Primera ventana a 850 nm, segunda ventana a 1300 nm y tercera ventana a 1550 nm. La atenuación es mayor si trabajamos en primera ventana y menor si lo hacemos en tercera. El hecho de que se suela utilizar la primera ventana en la transmisión de una señal es debido al menor coste de las fuentes luminosas utilizadas, al ser tecnológicamente más simple su fabricación.

Por último hablaremos de la atenuación en las fibras como parámetro importante a destacar. Es producida por tres causas: Dispersión, debida a defectos microscópicos de la fibra; absorción, debida a materiales no deseados de la fibra y flexión debida a las curvaturas.

Tipos de fibra óptica

Se pueden realizar diferentes clasificaciones acerca de las fibras ópticas, pero básicamente existen dos tipos: fibra multimodo y monomodo.

Fibras multimodo. El término multimodo indica que pueden ser guiados muchos modos o rayos luminosos, cada uno de los cuales sigue un camino diferente dentro de la fibra óptica. Este efecto hace que su ancho de banda sea inferior al de las fibras monomodo. Por el contrario los dispositivos utilizados con las multimodo tienen un costo inferior (LED). Este tipo de fibras son las preferidas para comunicaciones en pequeñas distancias, hasta 10 kms. Originalmente usada para largas distancias y sistema trunking interoficinas, La fibra multimodo fue rápidamente desplazada por la fibra de modo simple (Single-Mode) para aplicaciones de telecomunicación, porque este tipo presenta una baja atenuación óptica y una gran capacidad de transmisión de información.

Fibras monomodo. El diámetro del núcleo de la fibra es muy pequeño y sólo permite la propagación de un único modo o rayo (fundamental), el cual se propaga directamente sin reflexión. Este efecto causa que su ancho de banda sea muy elevado, por lo que su utilización se suele reservar a grandes distancias, superiores a 10 kms, junto con dispositivos de elevado costo (LASER).

1.5 ARQUITECTURAS DE RED

MODELO DE REFERENCIA OSI

El modelo de referencia OSI (Open System Interconection) es un principio de la interconexión de redes, y este modelo es un modelo de arquitectónico de siete capas desarrollado por la Organización Internacional para la normalización (Internacional Organitation for Standarization, ISO) y la Unión Internacional de las Telecomunicaciones (Internacional Telecomunications Union-Telecomunications, ITU-T). Se utiliza en todo el mundo para facilitar el conocimiento de las funciones de las redes. El modelo de referencia OSI aporta una estructura a las numerosas complejidades implicadas en el desarrollo de software de comunicaciones.

El modelo de referencia OSI se divide en siete capas diferenciadas. Cada una de ellas realiza una función única y especifica que facilitan el funcionamiento de los sistemas de comunicaciones. La capa funciona de acuerdo con un conjunto de reglas, que se llaman protocolo. Además de seguir las reglas del protocolo, cada capa proporciona un conjunto de servicios a las otras capas del modelo. Las siete capas del modelo del modelo de referencia OSI son las capas de aplicación, de presentación, de sesión, de transporte, de red, de enlace de datos y la capa física. En la figura (1.5a) se muestra la disposición de las capas en el modelo OSI.

Figura (1.5a) Modelo OSI de siete capas

LA CAPA DE APLICACIÓN

La capa de aplicación proporciona la interfaz al sistema de comunicaciones que ve el usuario. Actualmente, en los entornos de red se utilizan muchas aplicaciones habituales, como navegadores web, clientes del protocolo de transferencia de archivos (File Transfer Protocol, FTP) y correo electrónico. Un ejemplo de comunicación de capa de aplicación es un navegador web que descarga un documento de un servidor web. El navegador y el servidor web son aplicaciones iguales (peer) de la capa de aplicación que se comunican directamente entre si para la recuperación del documento. No conocen la existencia de las seis capas inferiores del modelo de referencia OSI, que funcionan para establecer las comunicaciones necesarias.

LA CAPA DE PRESENTACIÓN

La capa de presentación se encarga de la sintaxis de los datos mientras estos se transfieren entre dos aplicaciones que se comunican. También proporcionan un mecanismo para transmitir la presentación de los datos deseada entre las aplicaciones. Muchos usuarios infieren que el aspecto y el comportamiento del entorno de escritorio de una computadora, como el aspecto y el modo de interacción uniformes que tienen las aplicaciones de

una computadora Apple Computer, Inc. Es un ejemplo de la capa de presentación. De hecho no es una capa de presentación, sino una serie de aplicaciones que utilizan una interfaz común de programador. Actualmente, una de las capas de presentación común es ASN.1 (Abstract Syntax Notation One), que se utiliza en protocolos como el protocolo simple de administración de redes SNMP (Simple Network Management Protocol) para representar la estructura de las bases de datos de administración de redes.

LA CAPA DE SESIÓN

La capa de sesión permite que dos aplicaciones sincronicen sus comunicaciones e intercambien datos. Esta capa divide la comunicación entre dos sistemas en unidades de dialogo y proporciona puntos de sincronización principales y secundarios durante dicha comunicación. Por ejemplo, una gran transacción de bases de datos distribuidas entre varios sistemas puede utilizar protocolos de capa de sesión para garantizar que la transferencia progrese a la misma velocidad en ambos sistemas.

LA CAPA DE TRANSPORTE

La capa de transporte, capa 4, es la responsable de la transferencia de datos entre dos entidades de la capa de sesión. Existen muchos protocolos de capa de transporte, desde los que proporcionan los mecanismos básicos de transferencia (como los servicios poco fiables), hasta los que garantizan que la secuencia de datos que llega al destino está en el orden correcto, multiplexan varios flujos de datos, proporcionan un mecanismo de control de flujos y aseguran la fiabilidad.

Algunos protocolos de capa de red, llamados protocolos sin conexión, no garantizan que los datos lleguen a su destino en el orden en el que los envió el origen. En este caso algunas capas de transporte resuelven este problema secuenciando los datos correctamente antes de pasarlos a la capa de sesión. La multiplexión de datos significa que la capa de transporte puede manejar los flujos de datos simultáneos (que pueden proceder de diferentes aplicaciones) entre dos sistemas. El control de flujo es un mecanismo que puede utilizar la capa de transporte para regular la cantidad de datos enviados desde el origen al destino. A menudo, los protocolos de capa de transporte añaden fiabilidad al hacer que el sistema de destino envíe acuses de recibo al sistema de origen a medida que va recibiendo los datos. Los tres protocolos de transporte mas utilizados son: el protocolo para el control de la transmisión (Transmission Control Protocol, TCP) que se utiliza en Internet, el protocolo de intercambio de paquetes secuencial /Streams Packet Exchange, SPX) de Novell, y el protocolo de transporte AppleTalk (AppleTalk Transport Protocol, ATP) de Apple.

LA CAPA DE RED

La capa de red, que enruta los datos de un sistema a otro, proporcionan direcciones para su utilización en la red. El protocolo Internet (Internet Protocol, IP) define el direccionamiento mundial para Internet; Novell define la direcciones globales para intercambio de paquetes entre redes (Internet Packet Exchange, IPX) y su arquitectura cliente-servidor; y AppleTalk de Apple utiliza el protocolo de entrega de datagramas (Datagram Delivery Protocol, DDP) y las direcciones patentadas para la comunicación entre sus maquinas en la capa de red.

Los protocolos en la capa red enrutan datos desde el origen hasta el destino y pertenecen a una de estas dos categorías: orientados a conexión y sin conexión. Las capas de red orientadas a conexión enrutan los datos de forma similar a uso de un teléfono. Comienzan la comunicación realizando una llamada o estableciendo una ruta desde el origen hasta el destino. Envían los datos secuencialmente por la ruta determinada y finalizan la llamada o cierran la comunicación. Los protocolos de red sin conexión, que envían datos con toda la información en cada paquete, funcionan como el sistema postal. Cada carta, o paquete tiene una dirección de origen y otro destino. Cada oficina de correos intermedia, o dispositivo de red, lee estas direcciones y toma una decisión independiente sobre el enrutamiento de los datos. La carta, o datos, pasa de un dispositivo intermedio a otro hasta alcanzar su destino. Los protocolos de red sin conexión no garantizan la llegada de los paquetes al destino en el orden en que fueron enviados. Los protocolos de transporte son los responsables de la secuenciación de los datos en el orden correcto en los protocolos de red sin conexión.

LA CAPA DE ENLACE DE DATOS

La capa de enlace de datos, capa 2, proporciona la conexión entre la red física y la capa de red, lo que facilita el flujo fiable de datos en la red. Los protocolos de capa 2 mas utilizados comúnmente en la actualidad son Ethernet, Fast Ethernet, Token Ring, Frame Relay y modo de transferencia asíncrona (Asynchrnous Transfer Mode, ATM). Las direcciones de capa de enlace de datos son diferente de la direcciones de capa de red. Las direcciones de la capa de enlace de datos son únicas para cada segmento lógico de enlace de datos, mientras que las direcciones de la capa de red se utilizan en toda la red

LA CAPA FÍSICA

La primera capa del modelo de referencia OSI es la capa física. La capa física se ocupa de las interfaces física, eléctrica y mecánica entre dos sistemas.

La capa física define las propiedades de los medios de la red, como fibra, cobre de par trenzado, cobre coaxial, satelital, etcétera. Los tipos de interfaz de red estándares que se encuentran en la capa física incluyen conectores V.35, RS-232, RJ-, RJ-45, AUI y BNC. En la figura (1.5b) se observa el modelo de referencia OSI con la representación de datos que viajan desde un host de origen a un host destino a través de un switch y un router.

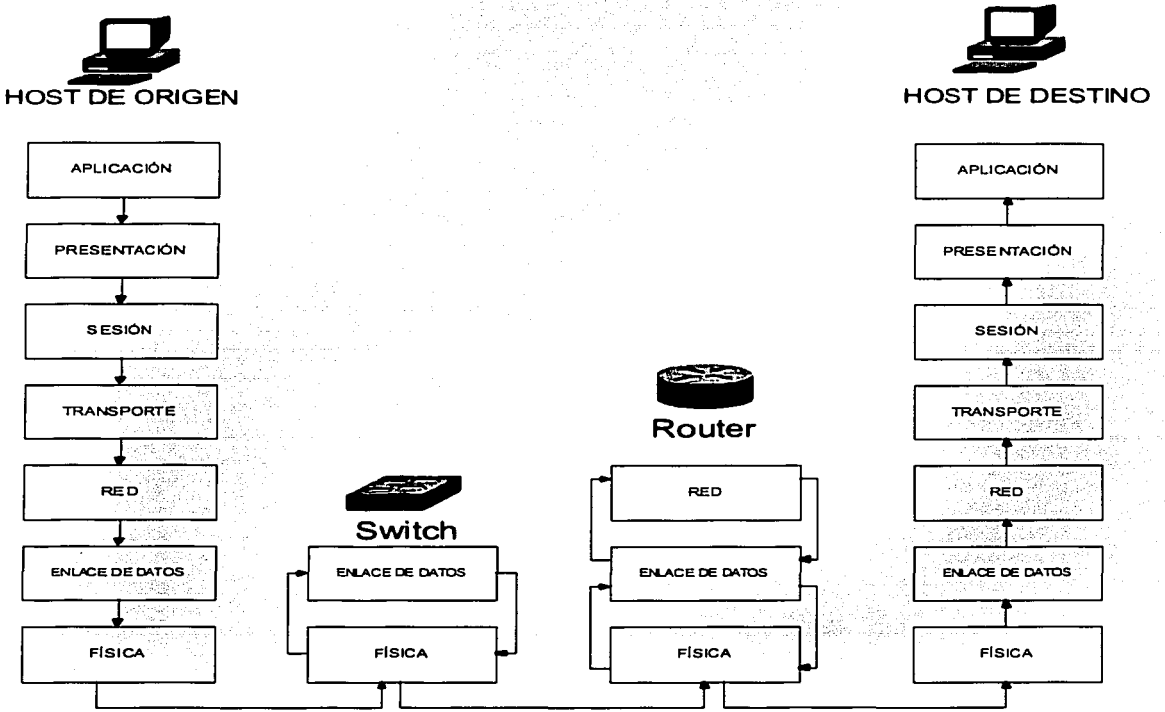


Figura (1.5b)

Los siguientes esquemas (1.5c), (1.5d), (1.5e), (1.5f) nos muestran la relación que guardan algunas de las diversas arquitecturas de red, así como también se observa cada una de ellas con sus respectiva suite de protocolos de red comparadas en función del modelo de referencia OSI.

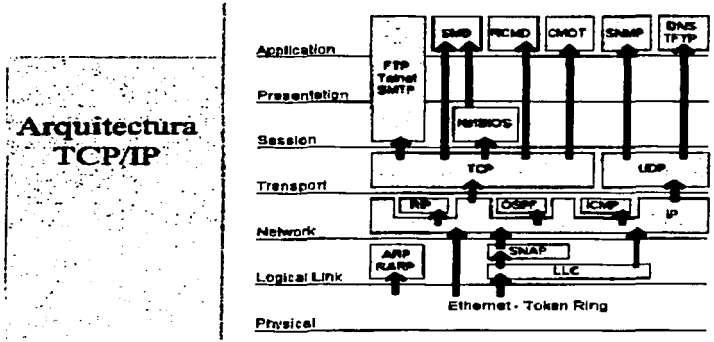


Figura (1.5c)

Arquitectura Novell IPX

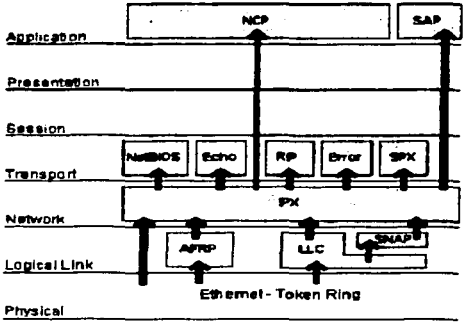


Figura (1.5d)

Arquitectura IBM & Microsoft

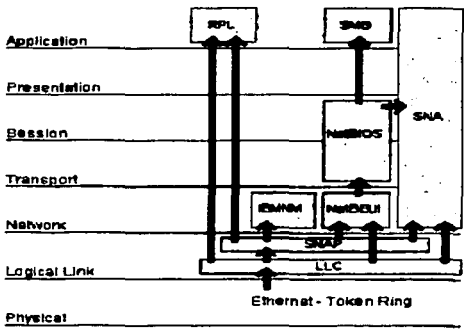


Figura (1.5e)

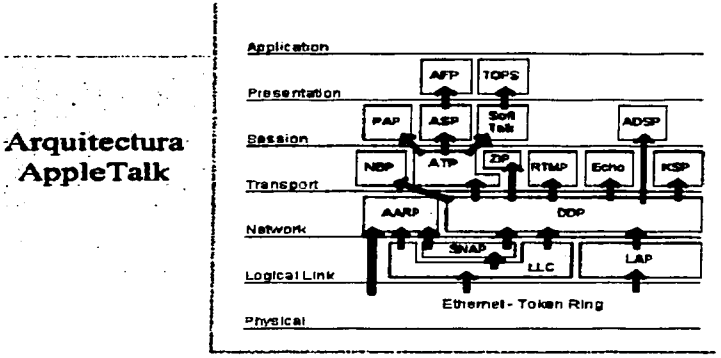


Figura (1.5f)

Ahora por otra parte debido al surgimiento del modelo OSI, se ha realizado un continuo desarrollo asociado a protocolos estándares. Estos protocolos describen la utopía de interconectividad, pero como aún predominan las arquitecturas de red propietarias como SNA de IBM y DECNet, la evolución hacía una arquitectura de red equivalente entre sistemas (como la de OSI) ha sido lenta.

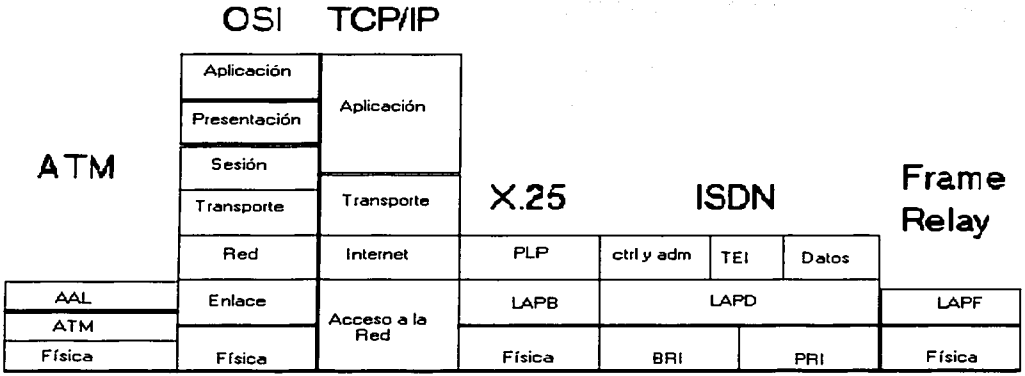


Figura (1.5g)

En la figura (1.5g) se muestra la relación de diferentes protocolos los cuales actúan sobre determinadas capas que van desde la uno a la capa siete según sea el tipo de tecnología WAN implementada tomando de nueva cuenta el modelo de referencia OSI. Así de esta manera el modelo de referencia OSI puede ser dividido en dos

grupos funcionales, el subconjunto de comunicaciones que forman las primeras tres capas y el subconjunto de procedimientos que operan utilizando las capas de la 4 a la 7.

EVOLUCIÓN DE LA TECNOLOGÍA DE REDES TELEMÁTICAS

2.1 FRAME RELAY

Frame Relay, o "transmisión de tramas", ha sido citado, en numerosos ámbitos, como la primera tecnología normalizada que realmente funciona, con enlaces activos entre ciudades Norteamericanas, Europeas y Asiáticas.

Frame Relay es igual que SMDS, un servicio público para interconexión de redes de alta velocidad y bajo retraso. La diferencia entre ambos es que SMDS (Servicios de Datos Multimegabit conmutado) es un servicio sin conexión ("connection less"), mientras que Frame Relay esta orientado a conexión ("connection oriented"). SMDS se utiliza normalmente en MAN, el ancho de banda máximo es de 44,736 Mbps aunque y usualmente los medios de transmisión son el cable de par trenzado y la fibra óptica; pero su uso no esta muy extendido y su costo es relativamente alto.

Ahora bien Frame Relay se define, oficialmente, como un servicio portador RDSI de banda estrecha en modo de paquetes, y ha sido especialmente adaptado para velocidades de hasta 2 Mbps, aunque nada le impide superarlas.

Frame Relay es un protocolo de switching de paquetes de WAN que se desarrollo inicialmente para su paso a través de RDSI (ISDN), las propuestas iniciales para los estándares de Frame Relay se presentaron en el CCITT en 1984. Aunque el estándar existía, había problemas con la interoperatividad entre los fabricantes, por que la tecnología recibió poco apoyo por parte de la industria hasta finales de los ochenta. Normalmente, Frame Relay se considera una versión mucho mas rápida y pulida de X.25; no tiene definido ningún protocolo de capa 3, ni es fiable. Sin embargo esta orientado a la conexión, los servicios de circuito conmutado utilizan TDM y son sincronizo (utilizan STM), de modo que se dice que la conmutación de paquetes utiliza TDM estadístico y, en ocasiones, se dice que es asíncrono.

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

Al igual que X.25, Frame Relay es un Protocolo de switching de paquetes que tiene PVC (Circuitos Virtuales Permanentes) y SVC (Circuitos Virtuales Conmutados). La mayoría de las redes Frame Relay actuales usan PVC, ya que los SVC están tan solo empezando a implementarse.

Un circuito virtual (Virtual Circuit), VC) es un mecanismo de comunicación en el que se establece la ruta para el traslado de información antes de que se envíen los datos, proceso conocido como colocar una llamada. Todos los paquetes de datos relacionados con la llamada siguen la misma ruta a través de la red, con lo que nos aseguramos que los datos lleguen al destino en el mismo orden que se enviaron. Al terminar la transferencia de datos, se finaliza la llamada. Los circuitos virtuales conmutados (Switched Virtual Circuits, SVC) son los que se pueden establecer y suprimir según lo requiera la red. Los circuitos virtuales permanentes (Permanent Virtual Circuits, PVC) los establece la red de forma permanente y nunca se suprimen.

Un sistema que es análogo a un circuito virtual (VC) es el sistema de teléfono, cada llamada que hacemos puede considerarse como un circuito virtual. Casi todas las llamadas que hacemos son análogas a los SVC. Pero si realizáramos una llamada de un teléfono una vez y no colgáramos nunca, seria un CVP(Permanent Virtual Circuits, PVC).

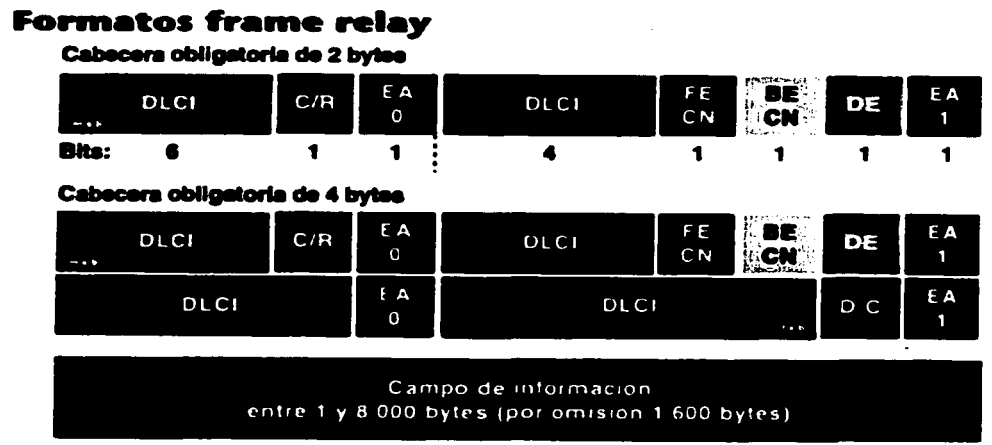
Frame Relay utiliza la configuración de llamadas, la transferencia de datos y el proceso de terminación de llamadas como en X.25. Los dispositivos finales como los routers, realizan llamadas a través de la red Frame Relay. Una vez establecida la llamada, el router traslada los datos y luego da por finalizada la llamada. En el caso de un PVC, la llamada esta siempre activa lo que permite que el router envíe datos sin tener que realizar la llamada.

De la misma manera que X.25 utiliza direcciones X.121, Frame Relay usa direcciones llamadas identificadores de conexión de enlace de datos (Data-Link Connection Identifiers, DLCI). Cada DLCI puede tener importancia local o global a través de la red Frame Relay.

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

Este equipo se denomina FRAD o "Ensamblador/Desensamblador Frame Relay" (Frame Relay Assembler/Disassembler) y el nodo de red se denomina FRND o "Dispositivo de Red Frame Relay" (Frame Relay Network Device). Las tramas y cabeceras de Frame Relay pueden tener diferentes longitudes, ya que hay una gran variedad de opciones disponibles en la implementación, conocidos como anexos a las definiciones del estándar básico. La información transmitida en una trama Frame Relay puede oscilar entre 1 y 8.000 bytes, aunque por defecto es de 1.600 bytes. En la figura (2.1a) se muestran los formatos de las tramas Frame relay.

Figura (2.1a)



Frame Relay a demostrado que funciona perfectamente, y ha demostrado un muy alto grado de interoperatibilidad entre diferentes fabricantes de equipos y redes. Esto de debe a que, cualquiera que sean las opciones empleadas por una determinada implementación de red o equipamiento, siempre existe la posibilidad de "convertir" los formatos de Frame Relay a uno común, intercambiando así las tramas en dicho formato.

Las redes Frame Relay son orientadas a conexión, como X.25, SNA e incluso ATM. El identificador de conexión es la concatenación de dos campos de HDLC (High level Data Link Control), en cuyas especificaciones originales de unidad de datos (protocolo de la capa 2), se basa Frame Relay. Por ello, el "identificador de conexión de enlace de datos" o DLCI (Data Link Connection Identifier), esta interrumpido por algunos bits de control.

Otros bits de la cabecera tienen funciones muy especiales en las redes Frame Relay. Dado que los nodos conmutadores Frame Relay carecen de una estructura de paquetes en la capa 3, que por lo general es empleada para implementar funciones como el control de flujo y de la congestión de la red, y que estas funciones son imprescindibles para el adecuado funcionamiento de cualquier red, se decidió emplear, para ello, algunos bits de la cabecera.

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

Es importante destacar que, en estos aspectos, Frame Relay es incluso más avanzado que ATM, que carece de capacidades explícitas FECN y BECN. Por otro lado, el bit CLP de ATM puede ser fácilmente empleado para proporcionar la funcionalidad del bit DE.

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

Frame Relay también ha sido denominado "tecnología de paquetes rápidos" (fast packet technology) o "X.25 para los 90'", y esto es cierto en gran medida.

El protocolo X.25 opera en la capa 3 e inferiores del modelo OSI, y mediante la conmutación de paquetes, a través de una red de conmutadores, entre identificadores de conexión. En cada salto de la red X.25 se verifica la integridad de los paquetes y cada conmutador proporciona una función de control de flujo. La función de control de flujo impide que un conmutador X.25 no envíe paquetes a mayor velocidad de la que el receptor de los mismos sea capaz de procesarlos. Para ello, el conmutador X.25 receptor no envía inmediatamente la señal de reconocimiento de los datos remitidos, con lo que el emisor de los mismos no envía más que un determinado número de paquetes a la red en un momento dado.

Frame Relay realiza la misma función, pero partiendo de la capa 2 e inferiores. Para ello, descarta todas las funciones de la capa 3 que realizaría un conmutador de paquetes X.25, y las combina con las funciones de trama. La trama contiene así al identificador de conexión, y es transmitida a través de los nodos de la red en lugar de realizar una "conmutación de paquetes". Lógicamente, todo el control de errores en el contenido de la trama, y el control de flujo, debe de ser realizado en los extremos de la comunicación (nodo origen y nodo destino). La conmutación de paquetes en X.25, un proceso de 10 pasos, se convierte en uno de 2 pasos, a través de la transmisión de tramas.

El procedimiento de control de errores y de flujo empleado en Frame Relay, implica que los mismos se realizan para el beneficio de la red misma, y no para el de los usuarios. Si se hallan errores, la trama es rechazada. Es un claro cambio de prioridades comparado con X.25.

Actualmente, y como consecuencia de trabajos del "Frame Relay Forum", se ha logrado definir unas especificaciones de "interfaz de nodo de red" o NNI (Network Node Interface). Una vez más, se demuestra que el uso de la tecnología va siempre por delante de las propias especificaciones y normalizaciones de la misma, como en el caso de ATM. En la figura (2.1b) se muestra la diferencia entre X.25 y Frame Relay para hacer la conmutación de paquetes en diferente capa del modelo OSI.

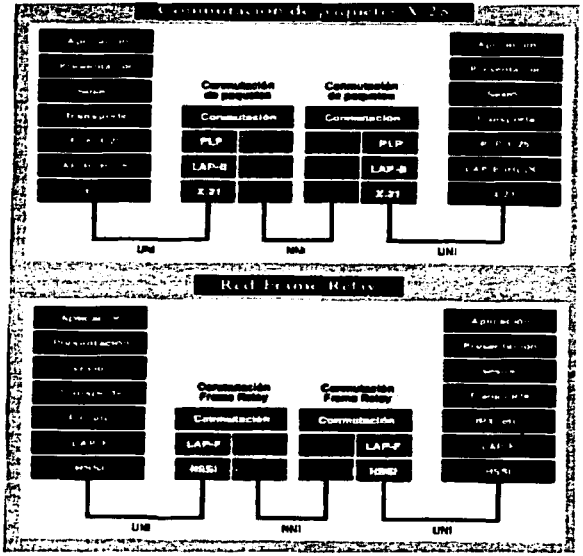
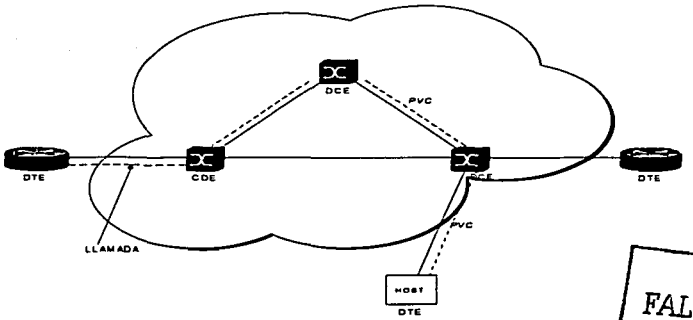


Figura (2.1b)

La figura (2.1c) ilustra un ejemplo de una red Frame Relay.

Figura (2.1c)



Estructura y transmisión de tramas, parámetros de dimensionamiento de CVP (Circuito Virtual Permanente, en ingles siglas PVC) (CIR, Bc, Be), señalización de líneas y CVP, gestión y prevención de la congestión.

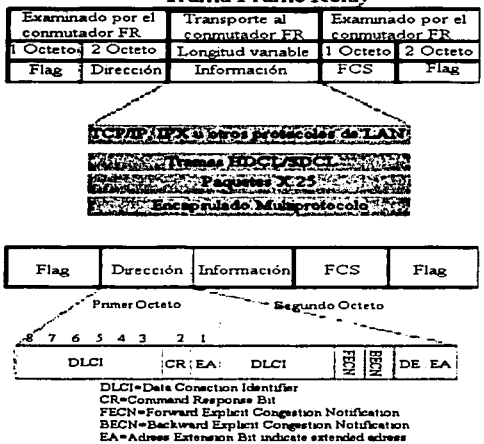
Frame Relay como tecnología de WAN es extremadamente popular, Frame Relay es mas eficiente que X.25, pero ofrece servicios similares, el ancho de banda máximo es de 44,736 Mbps; en Estados Unidos son extremadamente populares 56 Kbps y 384 Kbps. Su uso esta extendido; el costo es de moderado a bajo, los medios mas comunes son el cable de cobre de par trenzado y la fibra óptica.

Estructura y transmisión de tramas

La red Frame Relay obtiene datos de los usuarios en las tramas recibidas, comprueba que sean válidas, y las enruta hacia el destino, indicado en el DLCI del campo "dirección". Si la red detecta errores en las tramas entrantes, o si el DLCI no es válido, la trama se descarta. En la figura (2.1d) se muestra a detalle la estructura de la trama Frame Relay.

Figura(2.1d)

Trama Frame Relay



El "flag" es la secuencia de comienzo y fin de trama. El campo de "dirección" contiene el DLCI y otros bits de congestión. Los datos de los usuarios se meten en el campo "Información", de longitud variable que permite transmitir un paquete entero de protocolos LAN.

El siguiente gráfico (2.1e) representa cómo se transmite la información de dos usuarios. Lo primero es conectar a los usuarios mediante un acceso Frame Relay (puerto en el nodo de la red más línea de acceso). Después hay que definir en la red un CVP entre los accesos, que es el camino lógico para la transmisión de información. Un usuario puede definir más de un CVP hasta distintos destinos a través de un único acceso Frame Relay. Este concepto se llama multiplexación estadística.

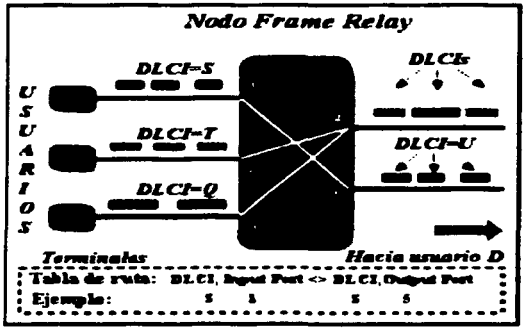


Figura (2.1e)

Los parámetros de dimensionamiento de CVP (CIR, Bc, Be).

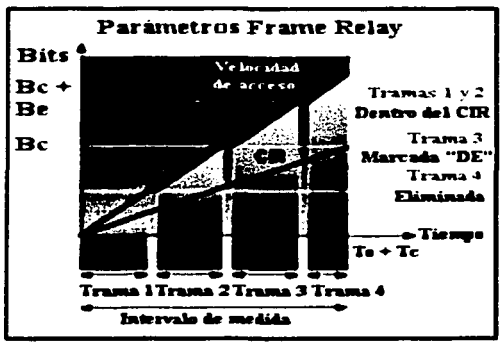
CIR: (Committed Information Rate, o tasa de información comprometida). Tasa a la cual la red se compromete, en condiciones normales de operación, a aceptar datos desde el usuario y transmitirlos hasta el destino. Puede ser distinto en cada sentido. Son las tramas 1 y 2 del ejemplo.

Bc: (Committed Burst Size o ráfaga comprometida). Es la cantidad de bits transmitidos en el periodo T a la tasa CIR (CIR=Bc/T). En las redes Frame Relay se permite al usuario enviar picos de tráfico a la red por encima de CIR, durante intervalos de tiempo muy pequeños, incluidos en el periodo T.

Be: (Excess Burst Size, o ráfaga en exceso): es la cantidad de bits transmitidos en el periodo T por encima de la tasa CIR. Si la red tiene capacidad libre suficiente admitirá la entrada de este tipo de tráfico en exceso (trama 3 del ejemplo), marcándolo con DE activo.

El tráfico entrante en la red, por encima de Bc + Be, es el descartado directamente en el nodo de entrada, (trama 4 del ejemplo); esto se observa en la figura (2.1f).

Figura (2.1f)



Señalización de estado de líneas de acceso y CVP

Es el conjunto de mensajes de señalización transmitidos entre la red y el equipo de acceso acerca del estado del acceso y de todos los CVP definidos.

Gestión y prevención de la congestión

En la trama, y dentro del campo de "Dirección" está el DLCI y otros bits que se utilizan para la gestión de la congestión.

Los FECN y BECN son activados por la red cuando empieza a detectar que el tráfico aumenta y debe evitar congestionarse. Así, todas las tramas que pasan por el nodo, hacia el destino (forward), hacia el origen (backward), con FECN y BECN activados, se entregan a cada equipo de acceso del usuario.

El equipo de acceso que recibe tramas con BECN activo puede reducir la cantidad de información enviada a la red hasta que ya no reciba más. El equipo de acceso conectado en el destino, que recibe tramas con el FECN activo, puede controlar al equipo de acceso conectado en el origen, utilizando mecanismos de control de flujo y ventana de transmisión de niveles superiores. Las tramas con DE activo pueden ser descartadas por la red si sigue habiendo congestión.

2.2 ATM

Modo de Transferencia Asíncrona (ATM, Asynchrnous Transfer Mode) hoy en día es una de las tecnologías WAN(e incluso LAN) más importantes. A grandes rasgos podemos describir ATM como una tecnología que utiliza pequeñas tramas o celdas de longitud fija (53 bytes) para transportar los datos, su ancho de banda máximo es actualmente de 622 Mbps, aunque se esta desarrollando para velocidades mas altas y los medios comunes de esta tecnología son el cable de par trenzado y la fibra óptica; pero esta descripción no nos aporta mucho sobre como funciona realmente esta tecnología y por esta razón nos vemos en la necesidad de abundar más sobre su funcionamiento y estructura

Ahora bien podemos mencionar que la función principal de una red digital de banda ancha es ofrecer servicios de transporte para diferentes tipos de tráfico a diferentes velocidades usando, como soporte, un limitado número de enlaces de comunicaciones de elevado ancho de banda.

La metodología tradicional de las redes de transporte digital se basaba en la multiplexación estática en el tiempo (TDM) de los diferentes servicios sobre los escasos troncales de comunicación. Esta tecnología de multiplexación es tanto utilizada a velocidades pleisócronas, como en JDS (Jerarquía Digital Síncrona).

Los nuevos tipos de datos, aplicaciones y requerimientos de los usuarios de este tipo de servicios obligó al desarrollo de una nueva tecnología que permitiera ofrecer este nuevo nivel de servicio. La nueva tecnología debería ser, además, lo suficientemente flexible como para asegurar un crecimiento rápido hacia las nuevas demandas que aparecerían en el futuro.

Después de un largo periodo de investigación y de diversas propuestas por parte de diferentes comités tecnológicos se define la nueva generación de tecnología para red de transporte digital de banda ancha: ATM

En este punto analizaremos tanto las causas de su aparición, como sus características particulares, lo que nos permitirá situar las diferencias entre Redes ATM y Redes TDM, sus puntos en común (transporte SDH) y sus aplicaciones concretas.

Y es que fueron diversos los motivos que forzaron una revolución tecnológica en el área del transporte digital de banda ancha. Entre ellos, la aparición de nuevas aplicaciones, la necesidad de incorporar el tráfico de LAN directamente en la red de transporte digital, las previsiones de crecimiento desmesurado, la necesidad de consolidar todos los tipos de tráfico, etc.

En este apartado explican, en detalle, los principales motivos que motivaron el desarrollo de ATM. Pero para continuar tendremos que preguntarnos ¿Qué tiene que ver la gestión del ancho de banda?

La técnica de división en el tiempo que usan las redes de transporte digital "tradicionales" (por ejem. redes basadas en multiplexores PDH, SDH) no es válida para el transporte del tráfico LAN, que es uno de los tipos de datos que más ha crecido en los últimos años y que más insistentemente pide un lugar en las redes de banda ancha.

El tráfico de datos se caracteriza por una necesidad muy grande de ancho de banda pero en momentos muy puntuales. El uso de técnicas TDM para la multiplexación del tráfico de LAN sobre los troncales de comunicaciones lleva a un compromiso demasiado duro. Por un lado, si se le asigna un *time-slot* de poco ancho de banda, el rendimiento de las comunicaciones no será aceptable. Por otro lado, si se le asigna un *time-slot* de gran ancho de banda, se malgastará demasiado espacio del canal cuando no se efectúen transferencias.

ATM, como nueva tecnología de transporte digital de banda ancha, dispone de mecanismos de control dinámico del ancho de banda. De este modo, cuando una fuente de datos deja de emitir, el ancho de banda que resulta liberado del canal de comunicación se reasigna a otra fuente.

La gestión dinámica del ancho de banda va acompañada de unos complejos mecanismos de control de congestión que aseguran que el tráfico sensible (voz, vídeo) siempre dispondrá de la calidad de servicio requerida (QoS).

La evolución de las aplicaciones que requieren transporte digital muestra, desde hace tiempo, un claro cambio de rumbo de entornos punto a punto a entornos punto a multipunto. Aplicaciones como videoconferencias, tráfico LAN, broadcasting de vídeo, etc. requieren de soporte broadcast en la capa de transporte.

Antes de ATM, las tecnologías de transporte digital, se basaban en la multiplexación sobre canales punto a punto y, por lo tanto, no podían enfrentarse a este nuevo requerimiento de servicio.

ATM, aunque es una tecnología orientada a la conexión, contempla el uso de circuitos punto-multipunto que permiten ofrecer funciones de broadcasting de información. Los datos se replican en el interior de la red allí donde se divide el circuito punto-multipunto. Esta aproximación minimiza el ancho de banda asociado a tráfico broadcast y permite la extensión y crecimiento de estos servicios hasta niveles muy elevados.

Otro requerimiento que se le pidió a ATM fue que dispusiera de mecanismos para el establecimiento de circuitos conmutados bajo demanda del DTE. Estas funcionalidades que, hasta la fecha, solo se exigían a las redes de banda estrecha (RTC, RDSI, X.25, FrameRelay,) se hacen, cada vez más, necesarias en la capa de banda ancha (Cable-TV, Videoconfencia). ATM define un protocolo de señalización entre el DTE y la red, llamado UNI, que permite a este segundo, la negociación de canales conmutados bajo demanda. El protocolo, basado en el Q.931 de RDSI, permite al DTE la creación de un canal (punto a punto o multipunto) con una determinada calidad de servicio (ancho de banda, retardo).

Otro protocolo (NNI) se encarga de la propagación de la petición de llamada dentro del interior de la red hacia el destino para su aceptación. El NNI es un protocolo no orientado a la conexión que permite la propagación de llamadas por múltiples caminos alternativos.

En el momento de definición de ATM se optó por un sistema de numeración de 20 bytes (basado en la numeración actual de la red telefónica básica) para los puntos terminales.

ATM se diseñó como una red "inteligente". Por lo que el objetivo debía ser que los nodos que componían la red fueran capaces de descubrir la topología (nodos y enlaces) que les rodeaba y crearse una imagen propia de como estaba formada la red. Además, este procedimiento debía ser dinámico para que la inserción de nuevos nodos o enlaces en la red fueran detectados y asimilados automáticamente por los otros nodos. Esta filosofía de red, que es muy común en las redes de banda estrecha (redes de routers, Frame Relay), se implanta en la banda ancha con la tecnología ATM.

Los administradores de la red de transporte ATM pueden decidir libremente el cambio de ancho de banda de un enlace o la creación de uno nuevo (por ejemplo, para disponer de caminos alternativos) sin tener que, por ello, reconfigurar de nuevo la red. Todos los nodos afectados por la modificación topológica actuarán inmediatamente como respuesta al cambio (por ejemplo, usando el nuevo enlace para balancear tráfico). Los problemas de cobertura tampoco significan ningún problema en esta tecnología, ya que un nodo que se inserta en la red, es descubierto por el resto de nodos sin ninguna intervención por parte del administrador.

De lo anterior podemos citar un balance general de la descripción de los puntos anteriores y a la vez nos permite ver como la tecnología de transporte ATM incorpora y mejora muchas de las técnicas utilizadas únicamente, hasta entonces, en las redes de banda estrecha. Esto quiere decir que ATM es también una tecnología válida para este tipo de redes. Así mismo ATM se define como una tecnología universal válida tanto como transporte digital de banda ancha, como para backbone de alta velocidad en redes LAN o integración de servicios en redes corporativas sobre enlaces de baja velocidad, además ATM es una solución global extremo a extremo y es tanto una tecnología de infraestructura como de aplicaciones.

Estandarización

Si bien sus orígenes se remontan a los años 60, es a partir de 1988 cuando el CCITT ratifica a ATM como la tecnología para el desarrollo de las redes de banda ancha (B-RDSI), apareciendo los primeros estándares en 1990. Desde entonces hasta nuestros días ATM ha estado sometida a un riguroso proceso de estandarización; destinado no solamente a una simple interoperabilidad a nivel físico (velocidades SONET y SDH...), sino a garantizar la creación de redes multifabricantes a nivel de servicio, estandarizándose aspectos como Señalización (UNI, NNI), Control de Congestión, Integración LAN, etc. Esta característica garantiza la creación de redes multifabricante, que garantizan la inversión y permiten un fuerte desarrollo del mercado, con la consiguiente reducción de costos.

Multiplexación basada en celdas

Para que se pueda gestionar correctamente el ancho de banda sobre un enlace, es necesario que las diferentes fuentes que lo utilizan presenten sus datos en unidades mínimas de información. Para ATM se decidió una unidad mínima de 53 bytes fijos de tamaño. El uso de un tamaño fijo permite desarrollar módulos hardware muy especializados que conmuten estas celdas a las velocidades exigidas en la banda ancha (actuales y futuras). La longitud de la unidad debe ser pequeña para que se pueden multiplexar rápidamente sobre un mismo enlace celdas de diferentes fuentes y así garantizar calidad de servicio a los tráficos sensibles (voz, vídeo).

Orientado a la conexión

Que ATM fuera una tecnología orientada a la conexión permitía, entre otras cosas, conseguir una unidad mínima de información de tamaño pequeño. Como se ha dicho anteriormente, las previsiones de crecimiento para ATM obligaban al uso de un sistema de numeración de terminales de 20 bytes. Las tecnologías no orientadas a la conexión requieren que cada unidad de información contenga en su interior las direcciones tanto de origen como de destino. Obviamente, no se podían dedicar 40 bytes de la celda para ese objetivo (la sobrecarga por cabecera sería inaceptable).

Los únicos datos de direccionamiento que se incluye en la celda es la identificación del canal virtual que supone, únicamente, 5 bytes de cabecera (48 bytes útiles para la transmisión de información).

Calidad de Servicio (QoS)

Se definen cuatro categorías de tráfico básicas: CBR (Constant Bit Rate), VBR (Variable Bit Rate), UBR (Undefined Bit Rate) y AVR (Available Bit Rate).

En el momento de la creación, el DTE caracteriza el tráfico que va a enviar por el circuito mediante cuatro parámetros (PCR, SCR, CDVT y MBS) dentro de una de esas cuatro categorías. La red propaga esa petición internamente hasta su destino y valida si los requerimientos exigidos se van a poder cumplir. En caso afirmativo, la red acepta el circuito y, a partir de ese momento, garantiza que el tráfico se va a tratar acorde a las condiciones negociadas en el establecimiento. Los conmutadores ATM ejecutan un algoritmo llamado dual leaky buckets que garantiza, celda por celda, que se está ofreciendo la calidad de servicio requerida. Está permitido que el DTE envíe los datos por un circuito a más velocidad de la negociada. En ese caso el conmutador ATM puede proceder al descarte de las celdas correspondientes en caso de saturación en algún punto de la red.

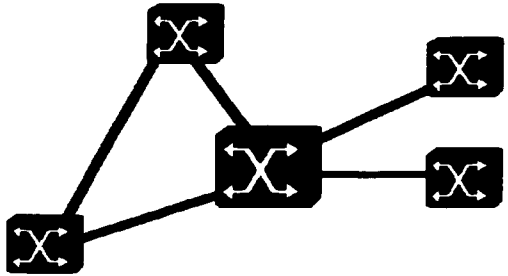
Red inteligente

Una red de transporte ATM es una red inteligente en la que cada nodo que la compone es un elemento independiente. Como se ha comentado anteriormente, los conmutadores que forman la red ATM descubren individualmente la topología de red de su entorno mediante un protocolo de diálogo entre nodos. Este tipo de aproximación, novedoso en las redes de banda ancha, abre las puertas a un nuevo mundo de funcionalidades

(enlaces de diferente velocidad, topología flexible, balanceo de tráfico, escalabilidad) y es, sin lugar a dudas, la piedra angular de la tecnología ATM.

Topología de las redes ATM

Con tecnología ATM se consigue crear una red de transporte de banda ancha de topología variable. Es decir, en función de las necesidades y enlaces disponibles, el administrador de la red puede optar por una topología en estrella, malla, árbol, etc. con una configuración libre de enlaces (E1, E3, OC-3), y esto se muestra en el grafico de la figura (2.2a).



En la figura (2.2a) se observa que ATM no tiene topología asociada

Por esta razón podemos ver la ventaja indiscutible de capacidad de adaptación a las necesidades que ATM ofrece. Una empresa puede empezar a desarrollar su red de transporte de banda ancha en base a unas premisas de ancho de banda y cobertura obtenidas a raiz de un estudio de necesidades. La evolución de las aplicaciones puede conducir a que una de esas premisas quede obsoleta y que se necesite una redefinición del diseño. En este caso, el administrador dispone de total libertad para cambiar enlaces o añadir nodos allí donde sea necesario. En el gráfico (2.2b) observamos la modificación de enlaces y supongamos, por ejemplo, el caso de una dependencia que accede al resto de la red de transporte ATM mediante un enlace E1 a 2Mbps. Por un crecimiento inesperado en el nombre de trabajadores en dicha dependencia, las necesidades de ancho de banda sobrepasan el umbral de los 2Mbps que, en el momento del diseño de la red, se consideró suficiente.

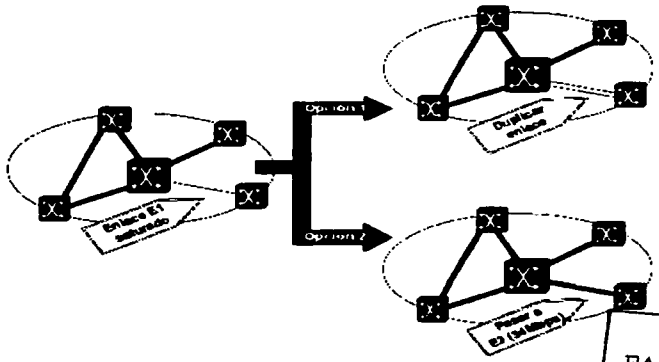


Figura (2.2b) muestra la libertad de actuación frente a cambios de enlace

Ante tal situación, el administrador de la red puede optar por dos soluciones. Una de ellas consiste en contratar un segundo enlace E1 para el acceso de la dependencia (un agregado de 4Mbps) o cambiar el enlace principal al otro nivel en la jerarquía (E3 a 34Mbps) Cualquiera de las dos actuaciones será detectada instantáneamente por los conmutadores ATM afectados sin necesidad de reconfigurar la red.

Otro problema muy frecuente con el que se encuentran los administradores de las redes de transporte es como adaptarse a los cambios relativos a requerimientos de cobertura geográfica. Estos cambios, que muchas veces son debidos a cambios estratégicos de las empresas y por lo tanto imprevisibles, estaban asociados a graves problemas tecnológicos y económicos antes de la aparición de la tecnología ATM. Como hemos explicado anteriormente, los nuevos nodos insertados, son descubiertos automáticamente por el resto de conmutadores que conforman la red ATM. El procedimiento asociado para añadir una nueva dependencia a la red de transporte ATM es tan sencillo como elegir el tipo de enlace (E1, E3, ...) y instalar el nuevo conmutador. Para ello en la grafica de figura (2.2c) se muestra que la red responderá automáticamente a esta ampliación sin ninguna necesidad de reconfigurar nada.

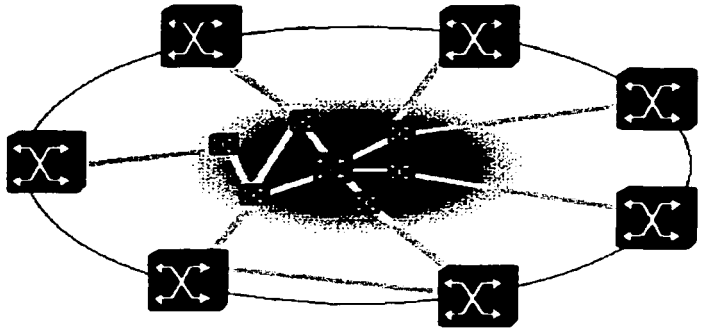


Figura (2.2c) Crecimiento ordenado en capas.

PNNI

En los dos puntos anteriores hemos explicado que los conmutadores que componen una red ATM son capaces de detectar, dinámicamente, los cambios de topología que ocurren a su alrededor. La base de todo este comportamiento es la existencia de un protocolo interno entre nodos: el PNNI

Un conmutador ATM intenta, continuamente, establecer relaciones PNNI con otros conmutadores por cada uno de sus puertos. Tan pronto se establece una de estas relaciones (por ejemplo, entre dos conmutadores adyacentes), se procede a un intercambio de información topológica entre ellos. De esta manera, cada conmutador puede hacerse una idea de como esta diseñada la red, de ello damos cuenta en la grafica de la figura (2.2d).

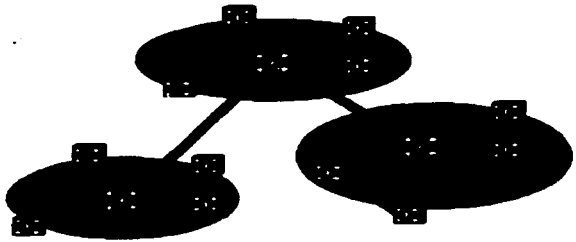


Figura (2.2d) muestra como el protocolo PNNI permite organizar las redes en áreas.

Frente a un cambio topológico (inserción de un nuevo nodo, fallo de un enlace existente) los nodos afectados notifican el evento a través de sus relaciones PNNI a el resto de conmutadores en la red. Este procedimiento está basado en el algoritmo SPF (Shortest Path First).

Para permitir que este tipo de protocolo no represente un problema a la escalabilidad de la red, el PNNI usa una aproximación jerárquica. La red puede ser dividida en áreas dentro de las cuales se ejecuta una copia independiente del algoritmo. Cada área, a su vez, puede estar compuesta por un número indeterminado de sub-áreas y así indefinidamente. Las redes basadas en tecnología ATM con PNNI pueden crecer hasta más de 2500 conmutadores. En el campo de las aplicaciones, una red de transporte digital ATM ofrece un conjunto nuevo de funcionalidades disponibles sin, por ello, dejar de ofrecer las funciones tradicionales.

Emulación de circuito

Mediante la emulación de circuito una red ATM se puede comportar exactamente igual que una red de transporte basada en tecnología SDH. La técnica de emulación de circuito consiste en la creación de un canal permanente sobre la red ATM entre un punto origen y otro de destino a una velocidad determinada. Este canal permanente se crea con características de velocidad de bit constante (CBR). En los puntos extremos de la red ATM se disponen interfaces eléctricos adecuados a la velocidad requerida (E1, V.35, V.11, ...) y los equipos terminales a ellos conectados dialogan transparentemente a través de la red ATM, como se observa en la figura (2.2e).

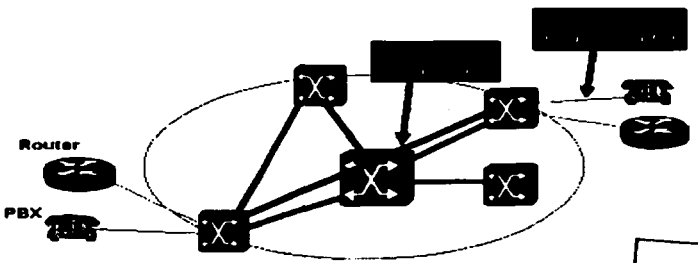


Figura (2.2e) muestra la Emulación de circuito

Los datos que envían los DTE en los extremos de la emulación de circuito, son transformados en celdas y transmitidos a través del circuito permanente CBR hacia su destino. A la vez que se procede a la transformación de la información en celdas, se ejecuta un algoritmo de extremo a extremo, que garantiza el sincronismo del circuito. Este conjunto de procedimientos está documentado en el método de adaptación a ATM AAL1. Mediante la técnica de emulación de circuito, una red ATM puede comportarse como una red de transporte basada en la multiplexación en el tiempo (TDM). Este tipo de servicio permite transportar enlaces digitales de central, líneas punto a punto, enlaces E1 para codecs, etc. transparentemente.

El objetivo en la definición de ATM fue que ésta fuera la nueva generación de red de transporte de banda ancha, con un conjunto de funcionalidades nuevas, pero completamente compatible con los servicios tradicionales de transporte.

Frame Relay

Sin evolucionar a aplicaciones nativas, ATM ofrece un conjunto nuevo de opciones para el transporte de datos que se benefician de la nueva concepción de la red de transporte. Este es el caso del transporte de Frame Relay sobre ATM. Una opción (no recomendada) consiste en el uso de la técnica de emulación de circuito para el transporte de Frame Relay sobre ATM. Esta aproximación obliga a la creación de una infraestructura de equipos de conmutación Frame Relay sobre la infraestructura ATM. Siguiendo este esquema, el tráfico de un DTE (DTE1) a otro DTE (DTE2) atraviesa dos veces la red ATM. La primera por la emulación de circuito hasta el conmutador Frame Relay externo y la segunda desde el conmutador FR hasta DTE2.

La opción correcta para el transporte del tráfico Frame Relay sobre ATM se consigue con el uso del protocolo ATM-DXI. Mediante este protocolo se logra que la red ATM se comporte como un gran conmutador Frame Relay. Los DLCI de FR se transforman en VCI de ATM en la capa externa de la red de transporte. De este modo, los equipos terminales pueden transmitirse información directamente sobre la red ATM (sin la necesidad de un equipo externo que los interconecte). Esta aproximación tiene dos ventajas adicionales. Por un lado, la red ATM conoce el volumen de tráfico que hay en cada momento y, por lo tanto, puede reasignar el ancho de banda no utilizado hacia otros servicios de datos. Por otro lado, en caso de congestión en algún punto de la red, se pueden usar los mecanismos de Frame Relay de control de flujo para informar a los DTE que ralenticen sus transmisiones y, por lo tanto, solucionar la congestión sin descartar celdas.

Independientemente del transporte ATM, el uso de Frame Relay para el transporte de datos evita el uso de grandes y costosos routers centrales de comunicaciones que concentran múltiples líneas punto a punto.

Conmutación de voz (VSTN)

Como para el tráfico Frame Relay, ATM ofrece una nueva manera de transportar el tráfico de voz sobre la red de transporte (a parte de la obvia de emulación de circuito). La aproximación consiste en conseguir que la red de transporte ATM sea emulada como una gran central de tránsito (tandem PBX). Esta técnica recibe el nombre de conmutación de voz sobre ATM.

Lo que se busca es que el propio conmutador ATM pueda interpretar el canal de señalización de la central y crear canales conmutados para la transmisión de cada circuito de voz independientemente. El circuito va desde la central origen hasta la de destino sin la necesidad de pasar por ninguna central de tránsito externa.

Al igual que en el caso de Frame Relay, la red ATM puede conocer el número de llamadas de voz que hay en cada momento del tiempo y, por lo tanto, usar únicamente el ancho de banda necesario para su transmisión (el resto se reasigna a otros servicios).

Otras ventajas de esta aproximación es la capacidad de la red ATM de informar a las centrales por el canal de señalización de como prosperan sus llamadas individualmente. Frente a estas notificaciones, una central puede decidir conmutar una llamada determinada por la red pública en caso de congestión en la red de transporte

corporativa. En el caso que las centrales usen compresión de voz, el uso de la técnica de conmutación de voz sobre ATM les asegura que un determinado circuito se comprime/descomprime en un único punto y, por lo tanto, la señal no sufre la pérdida de calidad asociada a las redes basadas en muchos saltos entre centrales.

La conmutación de voz sobre ATM elimina la necesidad de grandes centrales de tránsito existentes en las grandes redes de voz y hace más sencillas las tablas de encaminamiento con lo que la escalabilidad es mucho mayor.

NUEVAS APLICACIONES NATIVAS EN ATM

- **broadcasting de vídeo,** mediante el uso de circuitos multipunto, una red ATM puede replicar en su interior una fuente de datos única hacia múltiples destinos. La replicación se realiza únicamente, siguiendo una estructura de árbol, allí donde el circuito multipunto se replica. De esta manera, el consumo de ancho de banda en el núcleo de la red se minimiza. La aplicación más inmediata de los circuitos multipunto de ATM se encuentra en la distribución masiva de señal de vídeo desde un origen hasta múltiples destinatarios (televisión por cable, broadcasting de vídeo).

- **Videoconferencia,** las aplicaciones de videoconferencia pueden verse como un caso específico de broadcasting de vídeo en el que múltiples fuentes envían señal hacia múltiples destinos de manera interactiva. Los circuitos multipunto conmutados abren un nuevo mundo de posibilidades para las aplicaciones de videoconferencia de alta calidad. Una determinada dependencia puede entrar a formar parte de la vídeo conferencia pidiendo, dinámicamente, una extensión de los circuitos multipunto correspondientes hacia su punto de conexión.

- **LAN virtual (VLAN),** desde el punto de vista del transporte de datos LAN, las infraestructuras de comunicaciones ATM permiten la aplicación de técnicas de redes virtuales. El administrador de la red puede hacer que un conjunto de dependencias conectadas a la red de transporte interconecten sus LAN de manera aislada de como lo hacen otras dependencias. Las redes virtuales son muy útiles en aquellos casos en los que las dependencias conectadas a la red de transporte no forman parte de un mismo segmento y se requiere, por lo tanto, una invisibilidad de los datos para cada organismo. Aunque aisladas, se podrían interconectar las diferentes redes virtuales mediante una función de routing disponible en cualquier punto de la red que, entre otras cosas, garantizase unas determinadas políticas de seguridad.

De todo esto podemos concluir que ATM, como infraestructura básica de transmisión de banda ancha, en redes corporativas de área metropolitana (MAN) o extensa (WAN), está sustituyendo a las soluciones basadas en multiplexores SDH. Los gráficos (2.2f) nos dan una muestra de las diferentes aplicaciones nativas de que soporta la tecnología de ATM.

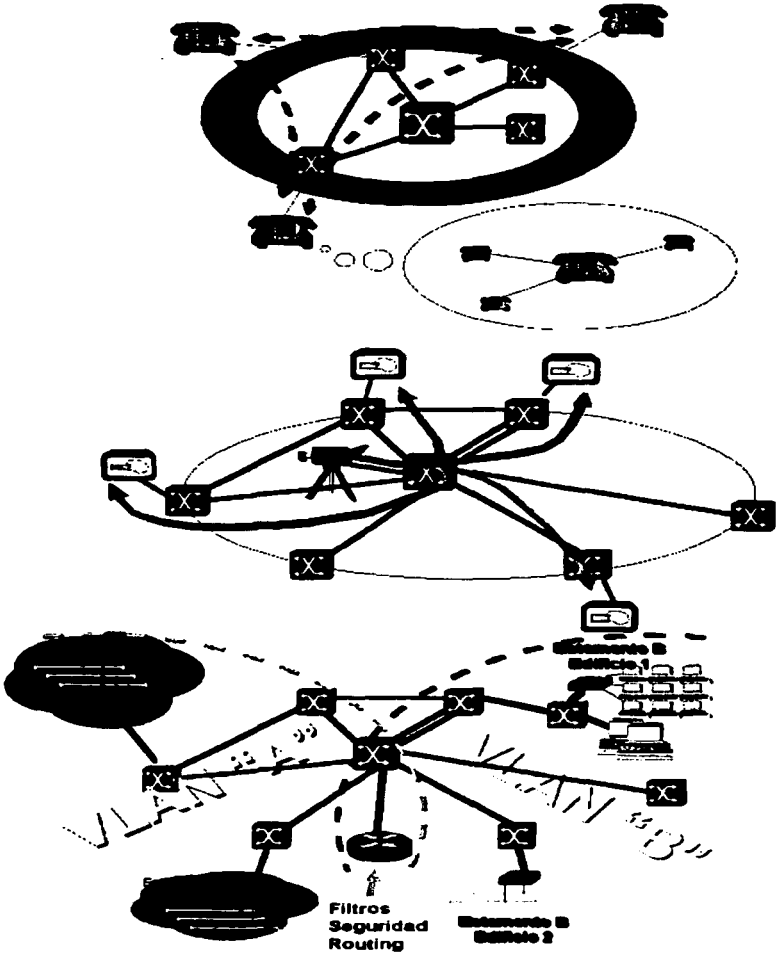
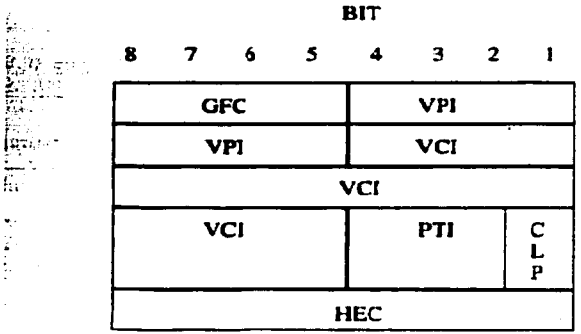


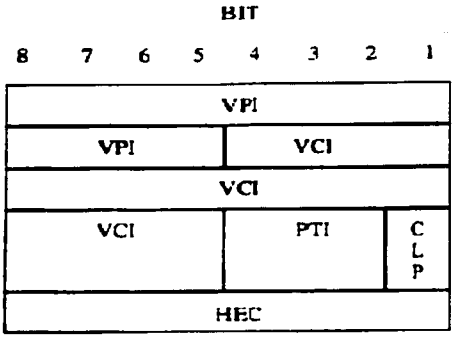
Figura (2.2f) aplicaciones ATM.

Estructura de la célula ATM

La célula ATM consta de una cabecera de 5 octetos y un campo de información de 48 octetos. En la recomendación I.361 de la UIT-T se especifican dos formatos de células, para la UNI (User to network Interface), y la NNI, (Network to Network Interface), respectivamente. La diferencia radica en la necesidad de que la UNI disponga de un campo para GCF. En la siguiente figura (2.2g) podemos ver los formatos de las células:



a) Formato de la cabecera de la célula ATM en la interfaz UNI



b) Formato de la cabecera de la célula ATM en la interfaz NNI

Figuras (2.2g) formatos de las células ATM.

Los campos de las células ATM son los siguientes:

- campo GCF (en la UNI): consta de 4 bits.

- campos ITV/ICV: tiene 24 bits en la UNI (8 para ITV y 16 pata ICV) y 28 bits en la NNI (12 para ITV y 16 pata ICV). Los 4 bits de diferencia se deben al campo GCF de la UNI.

- campo de tipo de carga útil, PTI, Payload Type Identifier. Está constituido por 3 bits. Indica el contenido de carga útil (datos de usuario, información de gestión, información OAM), así como situación de congestión en algún punto de la red.

- campo de Prioridad de Pérdida de Células, CLP, Cell Loss Priority. Tiene un bit de longitud. Las células con este bit a 1 son las primeras en ser descartadas en caso de congestión.

- campo de Control de Error de Cabecera, HEC. Consta de 8 bits. Es procesado por el nivel físico para detectar errores en la cabecera. El código utilizado permite la corrección de errores simples o detección de errores múltiples.

2.3 LANE/VPN

ANTECEDENTES

En el punto anterior dejamos claro que la tecnología del Modo de Transferencia Asíncrona (ATM) juega un papel central en la evolución de trabajo en grupo, campus y redes en los negocios. ATM posee grandes ventajas sobre las tecnologías LAN y WAN existentes, incluyendo la capacidad en ancho de banda y puntos de desarrollo como el de Quality of Service (QoS) las cuales facilitan nuevas clases de aplicaciones en multimedia.

Las nuevas tecnologías de LAN han sido desarrolladas y conducidas para introducir nuevas aplicaciones de banda ancha para los negocios y las organizaciones. Estas aplicaciones incluyen el escritorio de video para la corporación del aprendizaje a distancia y aplicaciones de conferencias, multimedia, imágenes, visualización, trabajo en conjunto, e interfaces con gráficos intensos. Por ejemplo, videoconferencias, acceso remoto a librerías de video o material de multimedia. Todas estas aplicaciones requieren conexiones de altos anchos de banda local y metropolitanamente disponibles. Otras aplicaciones necesitan sistemas auxiliares de colaboración para el incremento de anchos de banda, accesos a internet, uso de Web, hipermedia e intranet.

El próximo paso en la evolución fue desarrollar efectivamente las aplicaciones de multimedia e hipermedia, aplicaciones de áreas metropolitanas, regionales, nacionales y hasta continentales, con la Red siendo una Corporación y que el trabajo en conjunto llegara a ser un modo de operación estándar. La planeación de los productos, desarrollo, y el diseño podrán ser hechos en diferentes localidades, inclusive en diferentes continentes.

LAN'S BASADAS EN ATM

ATM ha sido posicionado por un amplio segmento de la industria como la tecnología de opción para construir redes backbone que puedan soportar una considerable carga de tráfico, y como la única plataforma común posible para soportar video digital, imágenes y multimedia. Algunos proponen el desarrollo de ATM a todos los niveles de redes, otros recomiendan el uso de ATM en WAN's. Esta discusión relaciona el uso de ATM como una aplicación de LAN. El desarrollo requiere de un NIC (Network Interface Card) basado en ATM en la PC o estación de trabajo y un switch o hub ATM listo.

La ventaja de ATM sobre las otras tecnologías de banda ancha es que ésta es escalable, con agregados de ancho de banda en el rango de 5 a 80Gbps. Los usuarios individuales pueden obtener 155Mbps dedicados exclusivamente para cada uno. Como es una tecnología orientada a conexión, aquí no se tiene la inquietud que las otras tecnologías tienen. Por lo tanto la tecnología es mejor para aplicaciones de video y multimedia.

LAN EMULADA USANDO ATM (APROXIMACIÓN A LANE)

Como ampliación a lo discutido anteriormente, algunos usuarios de las corporaciones pueden emigrar a LAN's basados en ATM inmediatamente, mientras que otros no, basados en sus requerimientos específicos de ancho de banda y requerimientos en la habilidad de afrontar la tecnología. Las LAN's ATM pueden ser desempeñadas por la instalación de NIC's ATM y conectándolos sobre un medio hacia un hub basado en ATM. Sin embargo, hay la necesidad y el deseo de interconectar en una manera cohesiva a todos los usuarios de la corporación. En estos ambientes, la plataforma ATM soporta puentes LAN a través de su infraestructura. Por otro lado, una LANE basada en ATM puede ser usada para la creación de VLAN's. Sin embargo, aunque LANE retiene la compatibilidad de las últimas capas de aplicación, en el control lógico de enlace, y más arriba, éstas son restringidas en términos de cómo soportan la conectividad de Quality of Service (QoS) hacia la capa IP y más arriba.

A nivel técnico, hay dos aproximaciones de operación de la red a niveles de protocolos a través de una red basada en ATM: Native Mode y LANE. En la operación en modo nativo los métodos de resolución de dirección son usados para mapear las direcciones en la capa de red a direcciones ATM. Los PDU's de la capa de

red son transportados directamente en celdas ATM a lo largo de la red ATM. LANE es el método alternativo estandarizado por el ATM Forum para transportar el tráfico a través de la red ATM.

LANE define cómo las aplicaciones existentes de LAN pueden correr sin cambio a través de la red ATM. El servicio y tecnología de LANE apuntan en el mercado de las redes ATM como una red LAN. Específicamente, soporta el legado de conexión de LAN's sobre ATM, esto es la interconexión de los usuarios de LAN con los usuarios de ATM, esto permite el acceso entre los puertos nativos de alta velocidad de ATM y los de LAN's. Básicamente, la tecnología LANE es el puenteado con los servicios de resolución de dirección estandarizadas de IEEE802 (MAC Address) hacia ATM y viceversa.

El protocolo LANE define una interface de servicio hacia los protocolos de las capas más altas, específicamente la capa de red, la cual es idéntica a las de las LAN's existentes y envía datos a través de las redes ATM encapsulados en un formato apropiado para LAN's, el MAC PDU. En otras palabras, los protocolos LANE hacen que una red ATM se vea y se comporte como una red Ethernet o Token Ring más rápida. El objetivo de esta tecnología es el de eliminar las modificaciones en los protocolos de las capas más altas y las aplicaciones. Desde el protocolo LANE se representa el mismo servicio de interface de las LAN's existentes específicamente en los drivers de la capa de red. El protocolo LANE se desarrolla actualmente en NIC's ATM y en los equipos switcheados de interconexión de LAN's.

Las telecomunicaciones futuras, necesitarán servicios de multimedia; por ejemplo, películas con movimiento combinadas con sonido de alta fidelidad. Las redes de telecomunicaciones convencionales diseñadas para teleservicios individuales, no pueden desarrollar o soportar en algunos casos servicios de multimedia. Por lo tanto como primer paso en las comunicaciones con multimedia, el ISDN (Integrate Services Digital Network) ofrece una interface integrada y tiene acceso a la red de modo de transferencia en paquetes. Los servicios de telecomunicaciones existentes como el teléfono, el telex requieren promedios de transmisión menos que un megabit por segundo. Los nuevos servicios de telecomunicaciones tales como teleconferencias (TV conference) e información visual, los promedios de transmisión para estos servicios pueden requerir de 100Mbps. Ninguno de los servicios actuales, teléfono, telex, o redes pueden desarrollar estas velocidades en su transmisión.

Enseguida se puede ver en la figura (2.3a) en forma gráfica cómo es el tráfico de información para los diferentes tipos de aplicaciones.

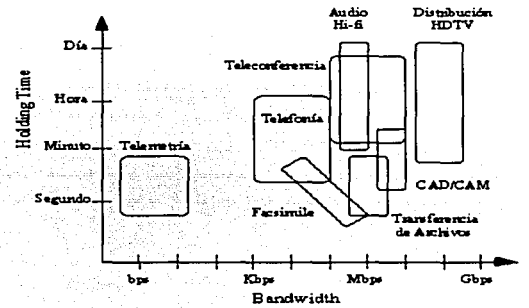


Figura (2.3a) Tráfico de información para los tipos de aplicaciones

PRINCIPIOS

En la siguiente sección se discutirá la interconexión de los protocolos existentes a través de las redes ATM. Dada la vasta base instalada de LAN's y WAN's actualmente, las redes y los protocolos de la capa de enlace operando en esas redes, una clave para el éxito de ATM será la habilidad para permitir la interoperabilidad entre estas tecnologías y ATM. Pocos usuarios tolerarían la presencia de islas ATM sin conectividad al resto de la red de una empresa. La clave para tal conectividad es el uso de los mismos protocolos en la capa de red, tales como IP o IPX en ambas plataformas, sobre las redes existentes y sobre ATM; puesto que

esta es la función de la capa de red, el proveer un panorama red uniforme hacia los protocolos de los niveles más altos y a las aplicaciones, figura (2.3b).

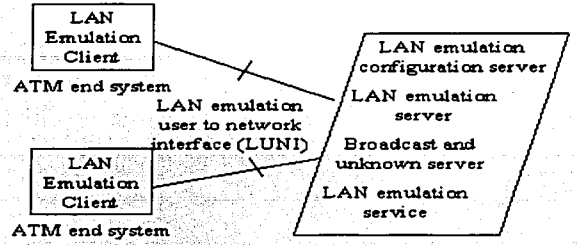


Figura (2.3b) Arreglo básico de LANE

PROBLEMAS BASICOS DE INTEGRACIÓN DE LAN-ATM

Debido a las diferencias estructurales de diseño entre ATM por un lado, y Ethernet, Token Ring, o FDDI; no es trivial integrar a las redes ATM y las LAN's tradicionales. Los principales problemas son la velocidad de transmisión y las diferencias de incompatibilidad de paquetes o formatos de celdas. Tales diferencias pueden ser eliminadas a través de puentes o ruteadores como se hecho hoy en día entre las redes Ethernet, Token Ring y FDDI existentes.

La diferencia crucial entre las redes ATM y las LAN's tradicionales es que ATM está basado en procesos de comunicaciones orientadas a conexión, mientras que las LAN's tradicionales utilizan principios de no conexión para transferir datos. El último envío de datos en un medio de transmisión común, esperando que éste llegue a su destino sin problemas. El no requerimiento del reconocimiento desde la estación receptora. La pérdida de los datos solamente puede ser retransmitida desde mecanismos en los protocolos de las capas superiores. Puesto que todos los nodos se comunican a través de un mismo medio de transmisión, cada paquete es alcanzado por otras estaciones también, solamente por el filtrado de las direcciones destino a través de tarjetas de interface de red, cada estación vista tiene una trayectoria de comunicación exclusiva. Si la dirección destino tiene el formato de 'broadcast-address', entonces los paquetes serán procesados por cada estación activa, por lo tanto todas las otras estaciones pueden alcanzar un paquete. Un número de protocolos, tales como broadcast packets, se usan para realizar ciertas funciones. Un ejemplo son las terminales de X-windows, las cuales recuperan su dirección IP con la ayuda de transmisión de mensajes desde un protocolo BOOT-P durante el encendido. Otro ejemplo es la resolución de direcciones entre las direcciones MAC e IP con la ayuda del protocolo ARP. Estos mecanismos de transmisión, forman parte de la naturaleza de las LAN's tradicionales; son en extremo contrastantes con las funciones principales de ATM y solamente pueden ser simulados con un esfuerzo grande.

El protocolo ATM orientado a conexión provee de una trayectoria de comunicación lógica exclusiva (VP/VC) para cada conexión. Los atributos de cada conexión son negociados antes de la activación y garantizados en toda la duración de la comunicación. Cada paquete de datos (celda) es ruteada solamente en su destino exacto, y no puede verse por ningún otro usuario. Un transmisor hacia n estaciones puede solamente lograr n conexiones, una hacia cada estación de emisión-recepción. Las funciones tales como la resolución de direcciones entre las direcciones de hardware ATM y las direcciones de los protocolos no pueden realizarse con un transmisor en ATM, pero si con la resolución de tablas dentro de los switches ATM.

METODOS PARA LA EMULACIÓN DE LAN

Desde el punto de vista de las aplicaciones de LAN's, la forma más flexible para integrar las estructuras existentes de LAN's tradicionales a redes ATM es la emulación completa de la Capa LAN-MAC. De esta manera, todas las aplicaciones LAN existentes pueden ser usadas vía redes ATM sin ninguna modificación. Para el software de LAN el servicio LANE se comporta como un manejador LAN MAC tradicional. La primera especificación de una emulación a nivel de LAN MAC para redes ATM fue publicado en enero de 1995 por el ATM Forum. (LAN Emulation sobre ATM Versión 1.0)

En esta parte haremos una descripción sobre los conceptos de LAN Emulation, su operación y estándares. También se realizará un análisis del funcionamiento de los protocolos existentes a través de redes ATM.

Hay dos formas distintas para ejecutar los protocolos en la capa de red sobre la plataforma de redes ATM, como se muestra en la figura (2.3c). Un método es conocido como modo de operación nativa (native mode), los mecanismos de resolución de direcciones son usados para mapear las direcciones de capas de red a directamente a direcciones ATM, y los paquetes contenidos en dicha capa son transportados a través de la red ATM. Aquí ATM provee una conexión paralela, con lo que el usuario toma las ventajas de los perfiles que ATM presenta. El método alternativo para la transportación de la información desde la capa de red a través de ATM es conocido como LAN Emulation.

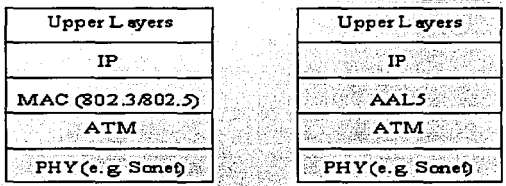


Figura (2.3c) Protocolos de la capa de red sobre ATM

CONCEPTOS BÁSICOS DE EMULACIÓN

Las comunicaciones de datos provistas por las LAN's difieren de las capacidades de ATM, como se detalla:

- Los servicios LAN pueden ser caracterizados como de no conexión comparados con el enfoque ATM de orientado a conexión.
- Los emisores y multiemisores son fácilmente realizables a través de un medio LAN compartido.
- Las direcciones LAN MAC basados en la manufactura de números seriales, son independientes de la topología de red.
- La función del protocolo LANE, es emular una LAN sobre una red ATM. Específicamente, el protocolo LANE define los mecanismos para la emulación en una IEEE802.3 Ethernet, IEEE802.5 Token Ring LAN, Fast Ethernet (100BaseT) e IEEE802.12 (100VG-AnyLAN). Ethernet o Token Ring Emulation pueden ser mapeados sin cambiar los formatos o procedimientos puesto que ambos usan el mismo formato.

El protocolo LANE define una interface de servicio para los protocolos de las capas superiores. Este habilita el envío de datos a través de la red ATM al ser encapsulados en el formato de paquete LAN MAC apropiado. Esto no significa que no se ha hecho ningún intento para emular el protocolo de control de acceso a medio (MAC) actual concerniente a una LAN específica. El protocolo LANE soporta un rango de tamaños de máximo de protocolos de unidad de datos (MPDU), correspondiendo a un tamaño de paquetes Ethernet (4Mbps)

y Token Ring (16Mbps); y también correspondiendo al valor de MPDU de por defecto para IP sobre ATM. El MPDU apropiado se usará dependiendo de qué tipo de LAN será emulada, y soportada por los switches LAN puenteados hacia la ELAN.

Una ELAN con solamente hosts ATM nativos, además, pueden usar opcionalmente cualquiera de los tamaños de MPDU disponibles, aún si éste no corresponde al MPDU actual en una LAN real emulada. Todos los LAN Emulation Client's (LEC's) dados en una ELAN deben usar el mismo tamaño de MPDU.

Los protocolos LANE hacen que una red ATM se vea y se comporte como una LAN Ethernet o Token Ring, aunque operan a una velocidad más alta que una red normal (figura 2.3d). La razón para hacer esta aproximación es que no requiere modificaciones en los protocolos de las capas más superiores para habilitar su operación sobre una red ATM. El servicio LANE presenta la misma interface que los protocolos MAC existentes sobre los manejadores (drivers) de la capa de red, por lo tanto no se requieren cambios en esos drivers. El objetivo es acelerar el despliegue de ATM.

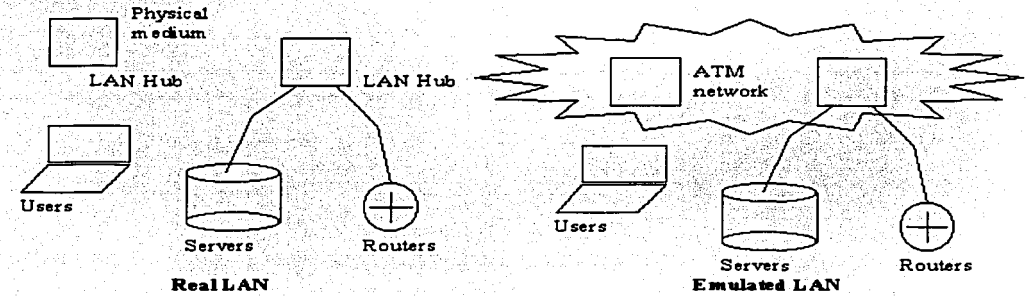


Figura (2.3d) Comparación entre una LAN tradicional y una LAN emulada

Está contemplado que el protocolo LANE pueda desarrollarse en dos tipos de equipo basado en ATM.

- ATM NICs: los ATM NICs comerciales implementan el protocolo LANE y la interface a las redes ATM, pero presentará una interface de servicio a la LAN en los protocolos de drivers de los niveles más altos dentro de sistema de conexión final. Esto es, los protocolos de la capa de red sobre el sistema final, continuaran comunicándose como si fueran una LAN, usando procedimientos conocidos. Estarán sin embargo disponibles para utilizar el vasto ancho de banda de redes ATM.
- Equipo de Internetworking y switches LAN: los switches LAN ligados a ATM y los ruteadores también se implementarán en LANE. Estos dispositivos juntos con los host ATM conectados directamente, equipados con los NIC's ATM, se utilizan para proveer el servicio de Virtual LAN (VLAN), donde los puertos de los switches LAN serán asignados hacia alguna VLAN en particular, independientemente de la localidad física.

El protocolo LANE no tiene un impacto directamente en equipo ATM como los switches. LANE se constituye sobre un modelo de capa. Los protocolos LANE operan transparentemente sobre y a través de switches ATM, utilizando solamente procedimientos estándar de señalización en ATM. Prácticamente hablando, los switches ATM pueden ser utilizados como plataforma sobre los cuales se implementarán algunos componentes de los servidores LANE, independientemente de la operación de la transmisión de celdas de los mismos switches ATM.

Este desacoplamiento es una de las ventajas del modelo, puesto que permite que además de los propósitos de los switches ATM, proceder independientemente de la operación de los protocolos de internetworking y viceversa. LANE implementa un protocolo para el puenteado de la capa MAC a ATM. El funcionamiento básico de LANE es el mapear las direcciones MAC a direcciones ATM. El objetivo de LANE es

ejecutar tales direcciones mapeadas y que los sistemas terminales de LANE puedan establecer conexiones entre ellos mismos y reenvíar datos. Nótese que mientras las especificaciones LANE especifican dos tipos de ELAN's, no permite la conectividad entre un LEC que implementa una LAN Ethernet y otro que implemente una LAN Token Ring. Tales ELAN's solamente podrán ser interconectadas a través de un ruteador ATM que actúe como un cliente en cada ELAN.

ELEMENTOS DE LANE

Como ya se pudo ver, el protocolo LANE define la operación de una sola ELAN en particular. Está propiamente dicho, emula tanto como una red Ethernet o Token Ring y consiste esencialmente de las siguientes entidades.

LAN EMULATION CLIENT (LEC)

Es la entidad en un sistema terminal que se encarga de la transmisión de datos, la resolución de direcciones, y otras funciones de control para un sistema terminal en cada ELAN. Un LEC también provee una interface estándar de servicio de LAN para cualquier entidad de las capas superiores. Un NIC ATM o switch LAN utilizado soporta un solo LEC por cada ELAN al cual está conectado.

El sistema terminal que se conecta a múltiples ELAN's tendrá un LEC por cada ELAN. Cada LEC es identificado por una única dirección ATM y es asociada con una o más direcciones MAC alcanzable a través de direcciones ATM. En el caso de un NIC ATM el LEC puede ser asociado como una sola dirección MAC, mientras que en caso de un switch LAN, el LEC puede ser asociado con todas las direcciones MAC leíbles a través de los puertos que un switch LAN están asignados a una ELAN en particular.

LAN EMULATION SERVER (LES)

El LES implementa las funciones de control para una ELAN en particular. Hay solamente un LES lógico por ELAN, y el pertenecer a una ELAN en particular significa tener una relación de control de el LES al cual pertenece dicha ELAN. Cada LES es identificado por una única dirección ATM.

BROADCAST AND UNKNOWN SERVER (BUS)

El BUS es un servidor multiemisor (multicast) que es utilizado para fluir el tráfico de las direcciones destino desconocidas y reenviar el tráfico de los emisores y multiemisores a los clientes en una ELAN en particular. Cada LEC es asociado con un solo BUS por ELAN, pero ahí pueden haber muchos BUS's dentro de una ELAN que comunique y coordine de manera específica. La conexión del BUS al LEC es identificado por una dirección ATM, en el LES, ésta es asociada con el emisor de direcciones MAC y este mapeo es configurado normalmente hacia el LES.

LAN Emulation Configuration Server (LECS)

Los LECS son una entidad que asigna a los clientes LANE individualmente a una ELAN en particular, direccionándolos hacia el LES que corresponde a una ELAN específica. Lógicamente hay un LECS por dominio administrativo y éste sirve a todas las ELAN's dentro del dominio. Las especificaciones de LANE no declaran donde debe ser localizado cualquiera de los componentes del servidor. Por propósitos de seguridad y desarrollo, los vendedores implementarán estos componentes de servidor en el equipo de red como switches ATM o ruteadores, en vez de una estación de trabajo o host.

LANE especifica solamente la operación del usuario de LAN Emulation hacia la interface de red LANE (LUNI), entre un LEC y la red que provee el servicio de LANE. Esto puede contrastar con la interface LAN Emulation NNI (LNNI) la cual opera entre los componentes del servidor dentro de un sistema ELAN, figura (2.3e).

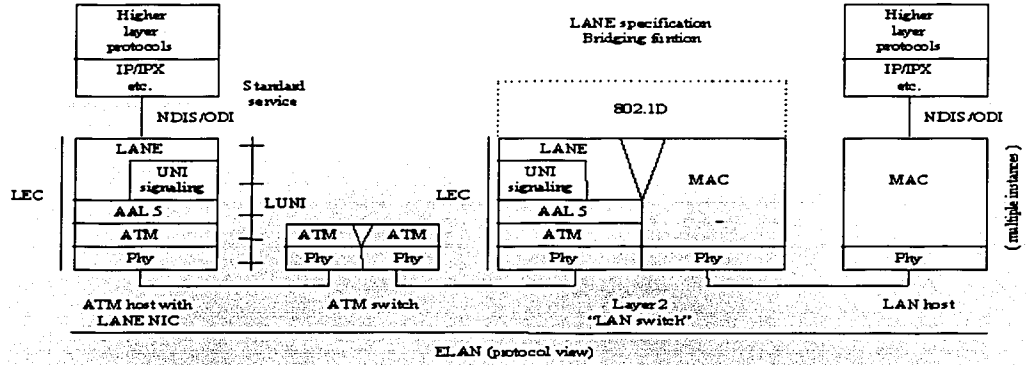


Figura (2.3e) Componentes de un sistema LANE

La fase 1 de los protocolos LANE figura (2.3e) especifica solamente la operación de LUNI; además, ésta no permite soporte para el estándar de un múltiple LES o BUS dentro de una ELAN. Las interacciones entre cada componente del servidor en LANE en la fase 1 no son especificados y serán implemetados de manera apropiadas por el distribuidor.

ATM Forum actualmente está trabajando en la fase 2 del protocolo LANE, el cual especifica los protocolos para LNNI y para permitir la redundancia en LES y reduplicar BUS's. Los protocolos LNNI especificarán interfaces abiertas entre varias entidades de servidores LANE y permitirán jerarquías de BUS para una mayor escalabilidad dentro de las ELAN's.

Las entidades de la fase 1 se comunican utilizando una serie de conexiones ATM. Los LEC's mantienen conexiones separadas para la transmisiones de datos y el control de tráfico.

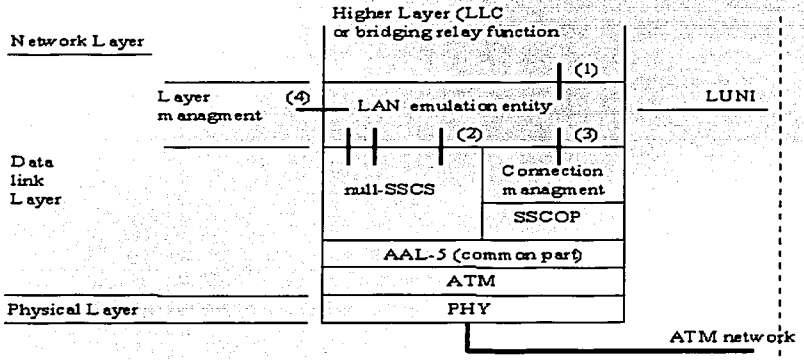


Figura (2.3f) interfaces LANE

- La interface entre la capa LAN emulation y las capas más altas incluye las facilidades para transmitir y recibir los data frames de usuario.
- Las interfaces entre la entidad de LAN emulation y la capa de adaptación ATM (AAL) incluye las facilidades para transmisión y recepción tramas de AAL-5 utiliza las capas más bajas, incluyendo las capas ATM y PHY. Los puntos de acceso a servicios de interface son identificados por SAP-Ids (que hace un mapeado uno a uno a los VCCs)
- La interface entre la entidad de LAN emulation y la entidad de manejo de conexión incluye las facilidades que requiere la activación o liberación de las conexiones virtuales. Esta entidad maneja SVCs y PVCs.
- La interface entre la entidad LAN emulation y la entidad de manejo de capas incluye las facilidades para iniciar y controlar la entidad la LAN emulation y regresa el estatus del mismo.

Lo anterior se observa en la figura (2.3f) Interfaces LANE

Los controles de conexiones son como siguen:

- Conexión de canal virtual de configuración directa (VCC): Es una VCC bidireccional punto a punto, y es activado por el LEC hacia los LECS.
- VCC de control directo: es una VCC bidireccional y es activado por el LEC hacia el LES.
- VCC de control distribuido: este es una VCC unidireccional activada desde los LES de respaldo hacia el LEC; típicamente es una conexión punto a multipunto.

Las conexiones de datos son:

- VCC de Datos Directos (Data Direct VCC): es una VCC bidireccional punto a punto y es activada por medio de dos LEC's que deseen intercambiar datos, figura (2.3g). Los dos LEC's típicamente usaran la misma VCC de datos directos para transportar todos los paquetes entre ellos, además que abren una VCC nueva por cada par de dirección MAC entre ellos, para conservar los recursos de la conexión. Puesto que LANE emula las LAN's existentes, incluyendo sus carencias de soporte de QoS, las conexiones de datos directos, serán típicamente conexiones UBR o ABR que no ofrecen garantías de QoS.
- Multiemisor VCC de envío (Multicast Send VCC): este es una VCC bidireccional punto a punto que es activada por el LEC hacia el BUS, figura (2.3h).
- Multiemisor VCC de reenvío (Multicast Forward VCC): esta es una VCC unidireccional que es activada hacia el LEC desde el BUS; típicamente es una conexión punto a multipunto, con cada LEC como terminal.

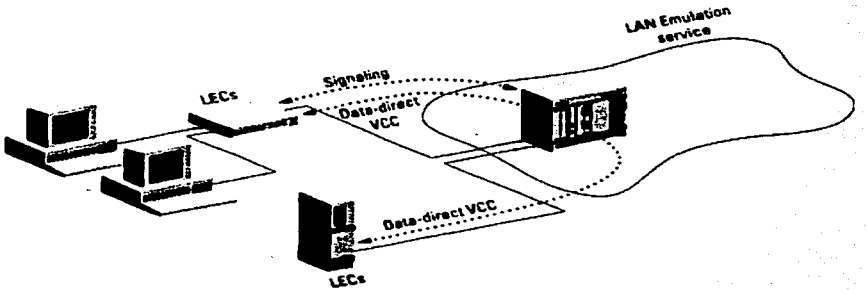


Figura (2.3g) VCC de Datos Directos

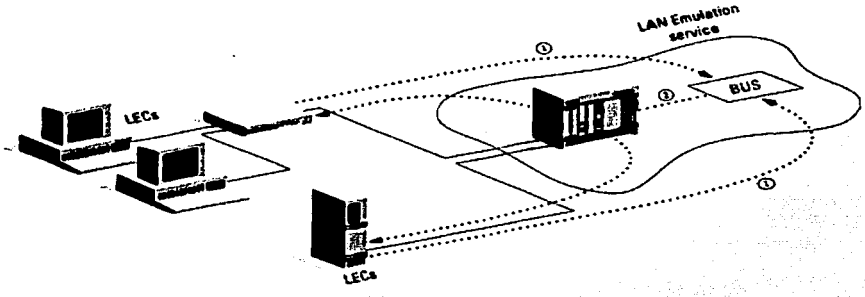


Figura (2.3h) Mensajes broadcast y multicast manejados por el BUS

ETAPAS DE OPERACIÓN DE LANE

La operación de un sistema LANE será descrita por las siguientes etapas:

ETAPA DE INICIALIZACIÓN Y CONFIGURACIÓN

Sobre la inicialización, el LEC primero debe obtener su propia dirección ATM (típicamente, esto será a través del registro de dirección). El LEC entonces activa una conexión de configuración directa hacia el LECS. Haciendo esto, el LEC deberá encontrar la localidad de el LECS usando un procedimiento ILMI definido para determinar la dirección de LECS, usando una dirección de LECS conocida; o usando una conexión permanente conocida hacia el LECS (VPI=0, VCI=17).

Después de encontrar el LECS, el LEC establecerá el VCC de configuración directa hacia el LECS. Una vez conectado, un protocolo de configuración es utilizado por el LECS para informar al LEC de la información que este requiere al conectarse a su tarjeta ELAN. Esta incluye la dirección ATM del LES, el tipo de LAN que está siendo emulada, tamaño máximo de los paquetes en la ELAN, y el nombre de la ELAN (es un texto tipo string para desplegar propósitos). El LECS es configurado generalmente por el manejador de red, con esta información, se indica a cual VLAN (donde una VLAN pertenece a una ELAN) pertenece el LEC, figura (2.3i).

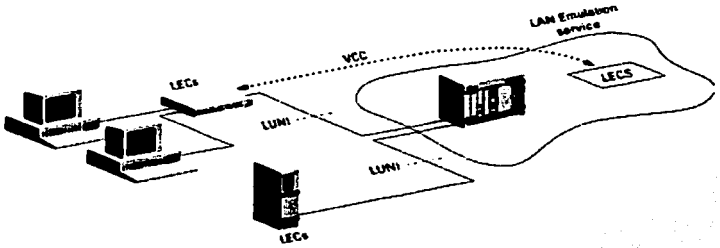


Figura (2.3i) Configuración del LEC inicial a través de LECS

ETAPA DE UNIÓN Y REGISTRO

Después de que el LEC obtiene la dirección del LES, éste podrá limpiar oportunamente el VCC de configuración directa hacia el LECS. Entonces este activa el VCC de Control Directo hacia el LES. Una vez

esto, el LES asigna el LEC con un identificador LEC único (LECID). El LEC entonces registra su propia dirección MAC y ATM con el LES. Esto puede ser opcional, también cualquier otro registro de direcciones MAC aproximado puede funcionar. En general, el soporte de una fuente ruteada de Token Ring ELAN es la misma también para una Ethernet ELAN, excepto que todas las aplicaciones desarrolladas en una Ethernet ELAN sobre direcciones MAC están correspondientemente desarrolladas dentro de las ELAN Token Ring en los descriptores de ruta, figura (2.3j).

El LES entonces activa, el respaldo hacia el LEC, el VCC de Control Distributivo. Los VCC de control directo y distributivo ahora pueden ser utilizados por el LEC para el procedimiento LAN Emulation ARP (LE-ARP) requiriendo la dirección ATM que corresponde a una dirección MAC en particular. Haciendo esto, el LEC formula un LE-ARP y lo envía a un LES. Si el LES reconoce este mapeo, este puede escoger una respuesta directamente sobre el VCC de control directo. Si no, este reenvía el requerimiento en el VCC de control distributivo para solicitar una respuesta de un LEC que reconozca a la dirección de MAC requerida.

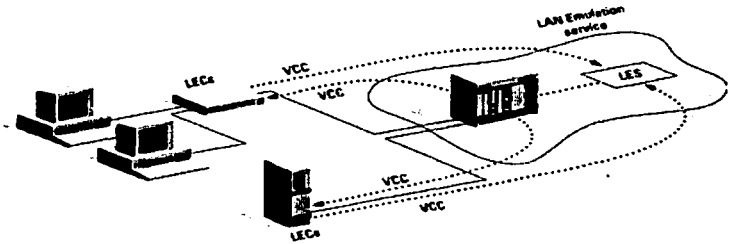


Figura (2.3j) Uniendo una LAN Emulada

Una razón porqué el LES no conocería el mapeo es porque la dirección está detrás de un puente MAC y el puente puede que no tenga la dirección registrada. Un NIC ATM, por otro lado, podría soportar uno o un número pequeño de direcciones MAC, muchas de las cuales pueden ser registradas fácilmente. Típicamente cualquier dirección MAC no conocida para el LES podría ser encontrada en un LEC dentro de un puente y no dentro de un NIC, y solamente los LEC's dentro de tales dispositivos necesiten recibir LE-ARP's redireccionados. Para acomodar esto, los LEC's pueden registrarse con los LES como un nodo apoderado (proxy nodes), indicando que este puede ser apoderado para otras direcciones y necesita obtener los LE-ARP's. Los LES entonces tienen la opción de activar las VCC de control distributivo y que los LE-ARP's son solamente enviados hacia tales LEC's apoderados. Por ejemplo, a través de dos conexiones punto a multipunto conectados a un LES como se muestra en la figura (2.3k) a todos los nodos apoderados y a uno de todos los nodos no apoderados (nonproxy nodes). Esto no es un requisito, sin embargo, los LES pueden escoger para simplificar la distribución a los LE-ARP's hacia todos los LEC's.

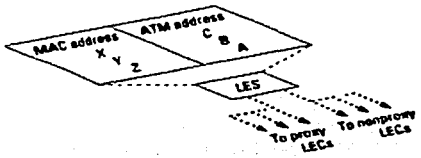


Figura (2.3k) LES inteligente con árbol Dual Point to Multipoint

ETAPA DE TRANSFERENCIA DE DATOS

Durante la transferencia de datos, un LEC recibe un paquete de la capa de red para transmitirlo desde un protocolo de las capas superiores (en el caso del NIC) o lo recibe de la capa MAC para reenviarlo a través de un puerto LAN (en el caso de un LAN switch). En primera instancia, la fuente LEC no tendrá la dirección ATM del LEC destino a través de la cual una dirección MAC puede ser obtenida. En este caso, el LEC primero formula y envía hacia el LES una respuesta LE-ARP. Mientras espera la respuesta del LE-ARP, el LEC también retransmite el paquete hacia el BUS, usando un encapsulado definido. El BUS en turno distribuirá el paquete a todos los LEC's. Esto debe ser realizado porque en el caso de un dispositivo pasivo que esté detrás de un switch, no habrá forma que LEC pueda saber donde está localizada una dirección MAC. Como un puente de aprendizaje, un LEC aprenderá la localización del dispositivo si solo si este responde al paquete reenviado. Adicionalmente, resolviendo un LE-ARP puede tomar algo de tiempo y como muchos protocolos de red son intolerantes a estas pérdidas o latencia. En este modo, el BUS provee análogamente el procedimiento utilizado por el puente de árbol espaciado para los paquetes con destinos desconocidos.

Si una respuesta de un LE-ARP se recibe, el LEC entonces activa la VCC de datos directos hacia el nodo destino y usa a éste para la transferencia de datos así como la trayectoria del BUS. Antes que pueda hacer esto, el LEC puede necesitar el uso del procedimiento de transporte de LANE para asegurar que todos los paquetes enviados al BUS sean reenviados al destino prioritario que utiliza la VCC de datos directos. En este mecanismo, se envía un control de celdas como bajo la primer trayectoria de transmisión siguiendo hasta último paquete. No hasta que la recepción de la celda de transporte sea reconocida por el destinatario se utiliza la segunda trayectoria para enviar los paquetes. El mecanismo es la forma de garantizar el encontrar la LAN estándar en uso que requiere los puentes LAN para preservar estrictamente la trama requerida.

Si una conexión de datos directos existe hacia un LEC (en la misma ELAN) a través del cual una dirección MAC es alcanzable, la fuente LEC puede escoger opcionalmente para reuso la misma conexión de datos directos, tanto para conservar las conexiones y guardarlas. Si una respuesta no es recibida hacia el LE-ARP, el LEC continuará enviando datos hacia el BUS, pero regularmente reenviará LE-ARP's hasta que una respuesta sea recibida. Una vez un paquete sea fluido a través del BUS y el destinatario responda a la fuente, algún LEC aprenderá la localidad de el destinatario y entonces responderá a un LE-ARP subsecuente, figura (2.31).

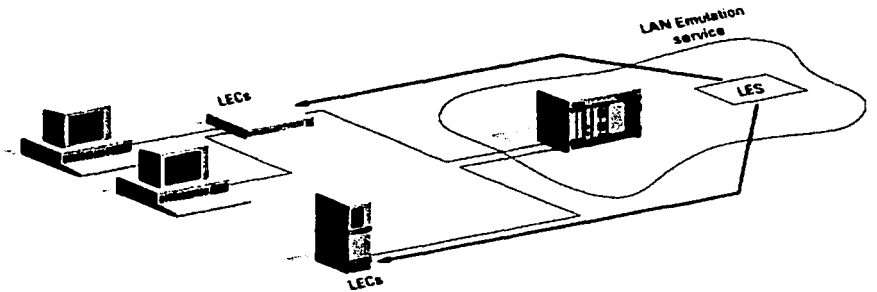


Figura (2.31) Transmisión de LE ARP desde LES hacia todos los LEC's

Con la primer versión de las especificaciones de ATM Forum LANE, se tiene el camino hecho para la integración de ATM con sus sistemas, protocolos, y aplicaciones en las empresas. Este define las formas estándares para los Clientes LANE en resolver los problemas de direcciones, comunicación con otros clientes y envío de datos en las redes ATM.

Usando LANE, los administradores de redes pueden disfrutar los beneficios de ancho de banda de ATM sin modificar los protocolos, software o hardware existentes. Por la definición de la múltiple LAN emulada a través de una red ATM, se pueden crear LAN's virtuales switcheadas para desarrollar seguridad y una mayor flexibilidad de configuración. Las aplicaciones inteligentes de manejo de redes, proveen panoramas lógicos y control de las LAN's virtuales switcheadas.

Con las especificaciones de LANE una vez ya maduras, proveerán una gran flexibilidad, e interoperabilidad para las redes ATM. Los administradores de red que elijan las implementaciones del estándar LANE hoy tienen una migración de trayectoria con potencial amplio para tomar las ventajas de este desarrollo.

2.4 MPLS

Multiprotocol Label Switching (MPLS).

Uno de los factores de éxito del internet actuales esta en la aceptación de los protocolos TCP/IP como estándar de facto para todo tipo de servicios y aplicaciones. El internet ha desplazado a las tradicionales redes de datos y ha llegado a ser el modelo de red pública del siglo XXI, pero una carencia fundamental del internet es la imposibilidad de seleccionar diferentes niveles de servicio para distintos tipos de aplicaciones usuario. Ahora por otra parte el internet se valora mas por el servicio de transporte de datos, conocido como de best-effort. Por lo que si el modelo de Internet ha de consolidarse como la red de datos del próximo milenio, se necesita introducir cambios tecnológicos fundamentales que permitan ir más allá del nivel best-effort.

Junto a los últimos avances tecnológicos en transmisión por fibra óptica (principalmente DWDM), que lleva a conseguir anchos de banda de magnitudes muy superiores, y en tecnología de integración de circuitos ASIC (Aplication Specific Integrate Circuitos), que permite aumentar enormemente la velocidad de proceso de información en la red, hemos de considerar la arquitectura MPLS.

MPLS es un estándar emergente del IETF que surgió para consensuar diferentes soluciones de conmutación multinivel, como concepto MPLS es un tanto difícil de explicar. Como protocolo es bastante sencillo, pero las implicaciones que supone su implementación real son enormemente complejas de tal manera que trataremos de dar una descripción que sea lo bastante digerible en este punto del capitulo dos.

MPLS se puede presentar como un sustituto de la conocida arquitectura IP sobre ATM, también como un protocolo de túneles (sustituyendo a las técnicas habituales de tunneling). O bien, como una técnica para acelerar el encaminamiento de paquetes, etc. En realidad MPLS hace un poco de todo eso, ya que integra sin discontinuidades los niveles 2 (transporte) y 3 (red), combinando eficazmente las funciones de control del routing con la simplicidad y rapidez de la conmutación de nivel 2.

Pero, ante todo y sobre todo, debemos considerar MPLS como el avance de las tecnologías de routing y forwarding en las redes IP, lo que implica una evolución en la manera de construir y gestionar estas redes. Los problemas actuales que presentan las soluciones de IP sobre ATM, tales como la expansión sobre una tecnología virtual superpuesta, así como la complejidad de gestión de datos de redes separadas y tecnológicamente diferentes, quedan resueltos con MPLS, al combinar en uno solo lo mejor de cada nivel (la inteligencia de routing con la velocidad de switching), MPLS ofrece nuevas posibilidades en la gestión de backbones, así como en la provisión de nuevos servicios de valor añadido. Para poder entender mejor las ventajas de la solución MPLS, vale la pena realizar antes los esfuerzos anteriores de integración de los niveles 2 y 3 que han llevado finalmente a la adopción del estándar MPLS.

EL CAMINO HACIA LA CONVERGENCIA DE NIVELES: IP SOBRE ATM

A mediados de los noventa IP fue ganando terreno como protocolo de red a otras arquitecturas en uso (SNA, IPX, AppleTalk, OSI). Por otro lado, hay que recordar que los backbones IP que los proveedores de servicios (NSPs) habían empezado a desplegar en esos años estaban construidos a base de routers conectados por líneas dedicadas T1/E1 Y T3/E3. El crecimiento explosivo de internet había generado un déficit de ancho de banda en aquel esquema de enlaces individuales. La respuesta de los NSPs fue el crecimiento del número de enlaces y la capacidad de los mismos, del mismo modo, los NSPs se plantearon la necesidad de aprovechar mejor los recursos de red existentes, sobre todo la utilización eficaz del ancho de banda de todos los enlaces. Con los protocolos habituales de encaminamiento (basados en métricas del menor numero de saltos). Ese aprovechamiento del ancho de banda global no resulto efectivo, por lo que había que idear otras alternativas de Ingeniería de tráfico.

Como consecuencia se impulsaron los esfuerzos para poder aumentar el rendimiento de los routers tradicionales. Estos esfuerzos trataban de combinar de diversas maneras, la eficacia y la rentabilidad de los conmutadores ATM con las capacidades de control de los routers IP. A favor de integrar los niveles 2 y 3 estaba el hecho de las infraestructuras de redes ATM que estaban desplegando los operadores de telecomunicaciones; estas redes ofrecían entonces (1995-97) una buena solución a los problemas de crecimiento de los NSPs. Por un lado proporcionaban mayores velocidades (155 Mbps) y, por otro las características de repuesta determinísticas de los circuitos virtuales ATM posibilitaban la implementación de soluciones de Ingeniería de tráfico. El

modelo de red IP sobre ATM (IP/ATM) pronto gano adeptos entre la comunidad de NSPs, a la vez que facilito la entrada de los operadores telefónicos en la provisión de servicios IP y de conexión a internet al por mayor.

El funcionamiento de IP/ATM supone la superposición de una topología virtual de routers IP sobre una topología real de conmutadores ATM. El backbone ATM se presenta como una nube central (el núcleo) rodeada por los routers de la periferia, cada router comunica con el resto mediante los circuitos virtuales permanentes (PVCs) que se establecen sobre la topología física de la red ATM. Los PVCs actúan como circuitos lógicos y proporcionan la conectividad necesaria entre los routers de la periferia, estos sin embargo, desconocen la topología real de la infraestructura ATM que sustenta a los PVCs. Los routers ven a los PVCs como enlaces punto a punto entre cada par. La figura (2.4a) nos muestra un ejemplo en el que se observa y se compara la diferencia entre la topología física de una red ATM con la topología lógica IP.

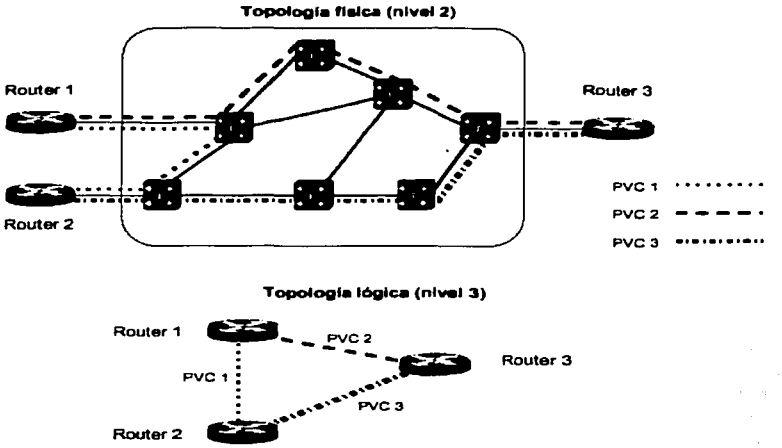
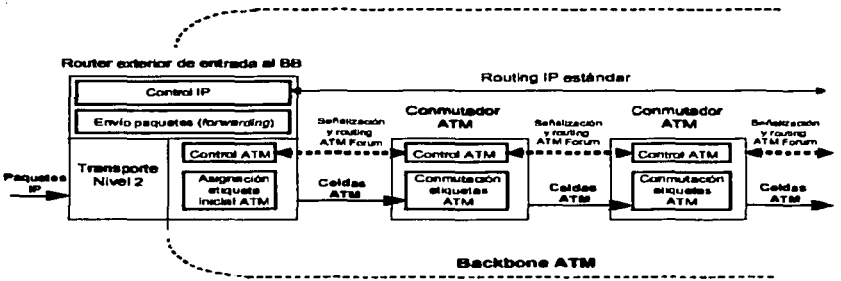


Figura (2.4a)

La base del modelo IP/ATM esta en la funcionalidad proporcionada por el nivel ATM, es decir, los controles de software (señalización y routing) y el envió de las celdas por hardware (conmutación). En realidad los PVCs se establecen a base de intercambiar etiquetas en cada conmutador de la red, de modo que la asociación de etiquetas entre todos los elementos ATM determina los correspondientes PVCs. Las etiquetas tienen solamente significado local en los conmutadores y son la base de la rapidez en la conmutación de celdas, la potencia de esta solución de topologías superpuestas esta en la infraestructura ATM del backbone; el papel de los routers IP queda relegado a la periferia, que a mitad de los 90, tenía una calidad cuestionable al estar basados en funcionamiento por software. Aunque se trata de una misma infraestructura física en realidad existen dos redes separadas con diferentes tecnologías, con diferente funcionamiento y lo que quizá es mas sorprendente concebidas para dos finalidades totalmente distintas. La solución de superponer IP/ATM permite aprovechar la

infraestructura ATM existente, las ventajas intermedias son el ancho de banda disponible y la rapidez de transporte de datos que proporcionan los conmutadores. En los casos de NSPs de primer nivel ellos poseen y operan el backbone ATM al servicio de sus redes IP. Los caminos físicos de los PVCs se calculan a partir de la velocidad del trafico IP, utilizando la clase de servicio ATM UBR (Unspecified Bit Rate), ya que en este caso el ATM se utiliza solamente como infraestructura de transporte de alta velocidad (no hay necesidad de apoyarse en los mecanismos inherentes del ATM para control de la congestión y clases de servicio). La ingeniería de tráfico se hace a base de proporcionar a los routers los PVCs necesarios con una topología lógica entre routers totalmente mallada. El punto de encuentro entre la red IP y la ATM esta en el acoplamiento de las subinterfaces en los routers con los PVCs a través de los cuales se intercambian los routers la información de encaminamiento correspondiente al protocolo interno IGP. Lo habitual es que entre cada par de routers haya un PVCs principal y otro de respaldo que entra automáticamente en funcionamiento cuando falla el principal. En la figura (2.4b) se observa el modelo IP/ATM.

Figura (2.4b)



Sin embargo el modelo IP/ATM tiene sus inconvenientes: hay que gestionar dos redes diferentes una infraestructura ATM y una infraestructura lógica IP superpuesta, lo que supone a los proveedores de servicio mayores costos. Existen además lo que se llama la tasa impuesta por celda, un overhead de aproximado del 20 % que causa el transporte de datagramas IP sobre las celdas ATM y que reduce en ese mismo porcentaje el ancho de banda disponible. Por otro lado la solución IP/ATM presenta los típicos problemas de crecimiento exponencial n x(n-1) al aumentar el número de nodos IP sobre una tecnología completamente mallada. Por ejemplo en una red con 5 routers externos con una topología virtual totalmente mallada sobre una red ATM son necesarios 5 x 4 = 20 PVCs (uno en cada sentido de transmisión), si se añade un sexto router se necesitan 10

PVCs mas para mantener la misma estructura (6x5 = 30), que se traduce en mayor esfuerzo que tiene que hacer el correspondiente protocolo IGP de los routers.

UN PASO MÁS EN LA CONVERGENCIA HACIA IP: CONMUTACIÓN IP

La convergencia continuada hacia IP de todas las aplicaciones existentes junto a los problemas de rendimiento derivados de la solución IP/ATM llevaron posteriormente (1997-98) a que varios fabricantes desarrollasen técnicas para la integración de niveles de forma efectiva sin las discontinuidades señaladas anteriormente. Estas técnicas se conocieron como conmutación IP (IP switching) o conmutación multinivel (multilayer switching). Una serie de tecnologías privadas entre las que merecen citarse: IP Switching de Ipsilon Networks, Tag Switching de Cisco, Aggregate Route-Base IP Switching (ARIS) de IBM, IP Navigator de Cascade/Ascend/Lucent y Cell Switching Router (CSR) de Toshiba condujeron finalmente a la adopción del actual estándar MPLS del IETF. El problema que presentaban tales soluciones era la falta de interoperatividad ya que usaban diferentes tecnologías privadas para combinar la conmutación de nivel 2 con el encaminamiento IP (nivel 3). A continuación se resumen los fundamentos de esas soluciones integradoras, que nos permitirán comprender la esencia de la solución MPLS.

Todas las soluciones de conmutación multinivel incluido MPLS se basan en dos componentes básicos comunes:

- La separación entre las funciones de control (routing) y de envio (forwarding).
- El paradigma de intercambio de etiquetas para el envío de datos.

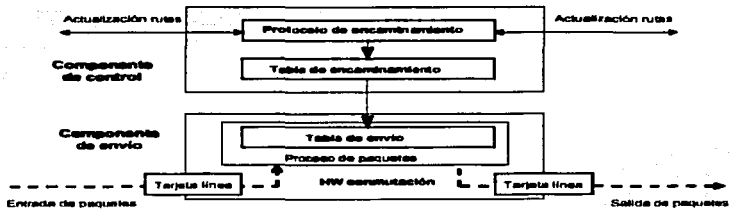


Figura (2.4c) Separación funcional de encaminamiento y envío.

En la figura (2.4c) se representan la separación funcional de esas dos componentes, una de control y la otra de envío. La componente de control utiliza los protocolos estándar de encaminamiento (OSPF, IS-IS y BGP-4) para el intercambio de información con los otros routers para la construcción y el mantenimiento de las tablas de encaminamiento. Al llegar los paquetes la componente de envío busca en la tabla de envío que mantiene la componente de control para tomar la decisión de encaminamiento para cada paquete. En concreto la componente de envío examina la información de la cabecera del paquete, busca en la tabla de envío la entrada correspondiente y dirige el paquete desde la interfaz de entrada a la de salida a través del correspondiente hardware de conmutación.

Al separar la componente de control (encaminamiento) de la componente de envío, cada una de ellas se puede implementar y modificar independientemente, el único requisito es que la componente de encaminamiento mantenga la comunicación con la de envío mediante la tabla de envío de paquetes y actualice la información. El mecanismo de envío se implementa mediante el intercambio de etiquetas, similar a lo visto para ATM, la diferencia esta en que ahora lo que se enviara por la interfaz física de salida son paquetes etiquetados. De este modo se esta integrando realmente en el mismo sistema las funciones de conmutación y de encaminamiento.

En cuanto a la etiqueta que marca cada paquete, es un campo de unos cuantos bits de longitud fija que se añade a la cabecera del mismo y que identifica una clase equivalente de envío (Forwarding Equivalence Class, FEC. Una FEC es un conjunto de paquetes que se envían sobre el mismo camino a través de una red aún cuando sus destinos finales sean diferentes. Por ejemplo, el encaminamiento convencional IP por prefijos de red (longest-match) una FEC serian todos los paquetes unicast cuyas direcciones de destino tengan el mismo prefijo. Realmente una etiqueta es similar a un identificador de conexión (como el VPI/VCI de ATM o el DLCI de Frame Relay). Tiene solamente significado local y por consiguiente no modifica la información de la cabecera de los paquetes; tan solo los encapsula asignando el tráfico a los correspondientes FEC.

El algoritmo de intercambio de etiquetas permite así la creación de caminos virtuales conocidos como LSPs (Label Switched Paths), funcionalmente equivalentes a los PVCs de ATM y Frame Relay. En el fondo lo que hace es imponer una conectividad entre extremos a una red no conectiva por naturaleza como son las redes IP, pero todo ello sin perder la visibilidad del nivel de red (de aquí los nombres de conmutación IP o Conmutación Multinivel). Esta es la diferencia básica con el modelo IP/ATM; al hablar de MPLS con mas detalle se entenderán mejor estas peculiaridades.

LA CONVERGENCIA REAL: MPLS

Como ya se dijo anteriormente que el principal problema que presentaban las diversas soluciones de conmutación multinivel eran la falta de interoperatividad entre productos privados de diferentes fabricantes. Además de ello la mayoría de esas soluciones necesitaban ATM como transporte, pues no podían operar sobre infraestructuras de transmisión mixtas Frame Relay, PPP, SONET/SDH Y LANs). Por lo que se quería obtener un estándar que pudiera funcionar sobre cualquier tecnología de transporte de datos en el nivel de enlace de aquí que el grupo de trabajo de MPLS que se estableció en el IETF en 1977 y propuso como un objetivo la adopción de un estándar unificado e interoperativo.

IDEAS PRECONCEBIDAS SOBRE MPLS

Si bien es cierto que MPLS mejora notablemente el rendimiento del mecanismo de envío de paquetes, pero este no era el principal objetivo del grupo IETF. Los objetivos establecidos por ese grupo en la elaboración del estándar:

- MPLS debía funcionar sobre cualquier tecnología de transporte, no sólo ATM.
- MPLS debía soportar el envío de paquetes tanto unicast como multicast.
- MPLS debía ser compatible con el Modelo de Servicios Integrados del IETF, incluyendo el protocolo RSVP.
- MPLS debía permitir el crecimiento constante de internet.

- MPLS debía ser compatible con los procedimientos de operación, administración y mantenimientos de las actuales redes IP.

También alguien pensó que MPLS perseguía eliminar totalmente el encaminamiento convencional por prefijos de red. Esta idea es falsa y nunca se planteo como objetivo del grupo, ya que el encaminamiento tradicional de nivel tres sería un requisito en internet por los siguientes motivos:

- El filtrado de paquetes en los cortafuegos (FW, Fire Walls) de acceso a las LAN corporativas y en límites de las redes de los NSPs es un requisito fundamental para poder gestionar la red y los servicios con las necesarias garantías de seguridad. Para ello se requiere examinar la información de la cabecera de los paquetes, lo que impide prescindir del uso del nivel tres en ese tipo de aplicaciones.
- No es probable que los sistemas finales (Host) implementen MPLS. Necesitan enviar los paquetes a un primer dispositivo de red (nivel 3) que pueda examinar la cabecera del paquete para tomar luego las correspondientes decisiones sobre su envío hasta su destino final. En este primer salto se puede decidir enviarlo por routing convencional o asignar una etiqueta y enviarlo por un LSP.
- La etiqueta MPLS tienen solamente significado local (es imposible mantener vínculos globales entre etiquetas y hosts en toda la internet). Esto implica que algún punto del camino algún dispositivo de nivel 3 debe examinar la cabecera del paquete para determinar con exactitud por dónde lo envía: por routing convencional o entregándolo a un LSR, que lo expedirá por un nuevo LSP.
- Del mismo modo, el último LSR de un LSP debe usar encaminamiento de nivel 3 para entregar el paquete al destino, una vez suprimida la etiqueta, como se verá seguidamente al describir la funcionalidad MPLS.

DESCRIPCION FUNCIONAL DEL MPLS.

La operación del MPLS se basa en los componentes funcionales de envío y control, aludidas anteriormente, y que se actúan ligadas íntimamente entre sí. Empecemos por la primera.

a) FUNCIONAMIENTO DE PAQUETES EN MPLS.

La base del MPLS está en la asignación e intercambio de etiquetas ya expuesto, que permiten el establecimiento de los caminos LSP por la red. Los LSP son simples por naturaleza (se establecen para un sentido del tráfico en cada punto de entrada a la red) el tráfico duplex requiere dos LSP, uno en cada sentido. Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un conmutador de etiquetas (Label-Switching Router) a otro, a través de paquetes etiquetados por MPLS. En la figura (2.4d) se muestra el esquema funcional de MPLS.

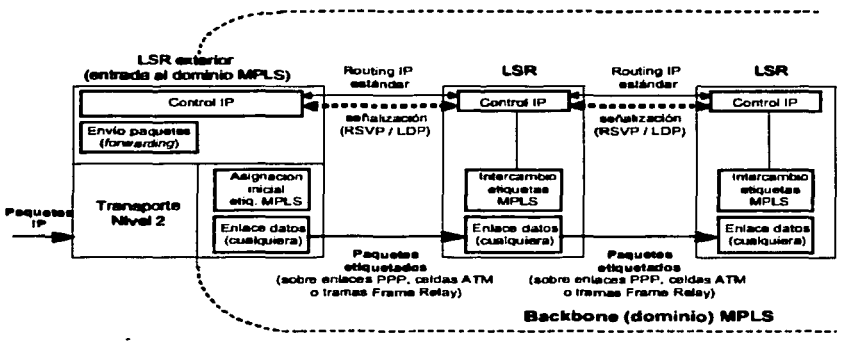


Figura (2.4d)

En la figura (2.4d) se puede ver la funcionalidad del MPLS. Compárese con los esquemas vistos antes en las figuras (2.4b) y (2.4c) para observar las analogías y diferencias. Al igual que en las soluciones de conmutación multinivel, MPLS separa las dos componentes funcionales de control (routing) y de envío (Forwarding). Del mismo modo, el envío se implementa mediante el intercambio de etiquetas en los LSP. Sin embargo, MPLS no utiliza ninguno de los protocolos de señalización ni de encaminamiento definidos por el ATM forum; en lugar de ello, en MPLS o bien se utiliza el protocolo RSVP o un nuevo estándar de señalización (el Label Distribution Protocol, LDP, del que trataremos más adelante) pero de acuerdo con los requisitos del IETF, el transporte de datos puede ser cualquiera. Si éste fuera ATM, una red IP habilitada para MPLS es ahora mucho más sencillo de gestionar que la solución clásica IP/ATM. Ahora ya no hay que administrar dos arquitecturas diferentes a base de transformar las direcciones IP y las tablas de encaminamiento ATM: esto lo resuelve el procedimiento de intercambio de etiquetas MPLS. El papel de ATM queda restringido al mero transporte de datos a base de celdas para MPLS esto es indiferente, ya que puede utilizar otros transportes como Frame Relay, o directamente sobre líneas punto a punto.

Un camino LSP es el circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC. Al primer LSR que interviene en un LSP se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola. Los dos están en el exterior del dominio MPLS. El resto, entre ambos, son LSRs interiores del dominio MPLS. Un LSR es como un router que funciona a base de intercambiar etiquetas según una tabla de envío. Esta tabla se construye a partir de la información de encaminamiento que proporciona la compone de control (recuérdese el esquema de la figura 2.4c), según se veremos más adelante. Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada que se utilizan para acompañar a cada paquete que llega por esa interfaz y con la misma etiqueta (en los LSR exteriores sólo hay una etiqueta, de salida en el de cabecera y de entrada en el de cola). En la figura (2.4e) se ilustra un ejemplo del funcionamiento de un LSR por la interfaz 3 de entrada con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por el interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.

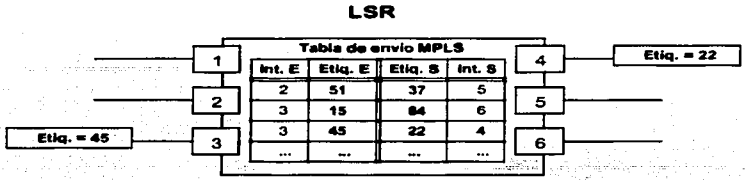


Figura (2.4e)

El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera. En la figura (2.4f) el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1 el LSR consulta la tabla de encaminamiento y asigna el paquete a la clase FEC definida por el grupo 212.95/16. Así mismo, este LSR le asigna una etiqueta (con valor 5 por ejemplo) y envía el paquete al siguiente LSR del LSP. Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas. Al llegar el paquete al LSR de cola (salida), ve que el siguiente salto lo saca de la red MPLS; al consultar ahora la tabla de conmutación de etiquetas quita está y envía el paquete por Routing convencional.

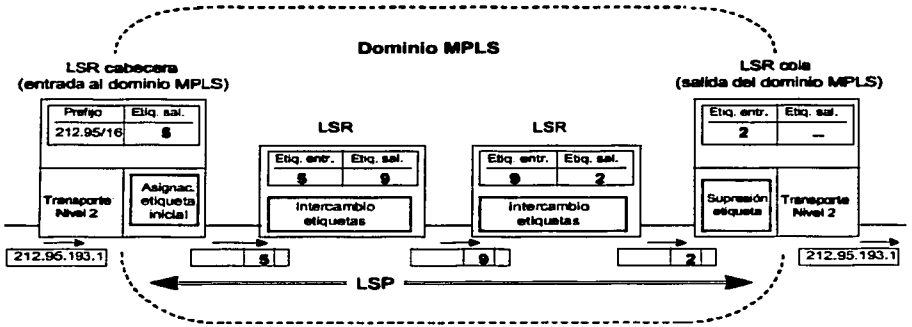


Figura (2.4f)

Como se ve, la identidad del paquete original IP queda enmascarada durante el transporte por la red MPLS, que no mira sino las etiquetas que necesita para su envío por los diferentes saltos de LSR que configuran los caminos LSP. Las etiquetas se insertan en cabeceras MPLS, entre los niveles 2 y 3. Según las especificaciones del IETF, MPLS debía funcionar sobre cualquier tipo de transporte: PPP, LAN, ATM, Frame Relay, etc. Por ello. Si el protocolo de transporte de datos contiene ya un campo para etiquetas (como ocurre con los campos VPI/VCI de ATM y DLCI de Frame Relay), se utilizan esos campos nativos para las etiquetas. Sin embargo, si la tecnología de nivel 2 empleada no soporta un campo para etiquetas (p. Ej. Enlaces PPP o LAN), entonces se emplea una cabecera genérica MPLS de 4 octetos, que contiene un campo específico para la etiqueta ya que se inserta entre la cabecera del nivel 2 y la del paquete (nivel 3).

En la figura (2.4g) se representa el esquema de los campos de la cabecera genérica MPLS y su relación con las cabeceras de los otros niveles. Según se muestra en la figura, los 32 bits de la cabecera MPLS se reparten en: 20 bits para la etiqueta MPLS, 3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamado CoS). 1 Bit de Stack para poder apilar etiquetas de forma jerárquica (s) y 8 bits para indicar el TTL (time to live) que sustenta la funcionalidad estándar TTL de las redes IP. De este modo, las cabeceras MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un proveedor IP a la hora de extender su red.

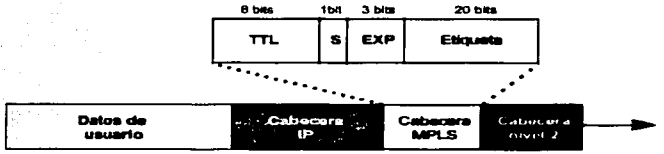


Figura (2.4g) estructura de la cabecera genérica MPLS.

b) CONTROL DE LA INFORMACIÓN EN MPLS.

Hasta ahora se ha visto el mecanismo básico de envío de paquetes a través de los LSP mediante el procedimiento de intercambio de etiquetas según las tablas de los LSR. Pero queda por ver dos aspectos fundamentales:

- Cómo se generan las tablas de envío que establecen los LSP.
- Cómo se distribuye la información sobre las etiquetas a los LSR.

El primero de ellos está relacionado con la información que se tiene sobre la red: topología, patrón de tráfico, características de los enlaces, etc. Es la información de control típica de los algoritmos de encaminamiento. MPLS necesita esta información de routing para establecer los caminos virtuales LSPs. Lo más lógico es utilizar la propia información de encaminamiento que manejan los protocolos internos IGP (OSPF, ISS-IS, RIP) para construir las tablas de encaminamiento (los LSR son routers con funcionalidad añadida). Esto es lo que hace MPLS precisamente: para ruta IP en la red se crea un camino de etiquetas a base de concatenar las de entrada/salida en cada tabla de los LSRs; el protocolo interno correspondiente se encarga de pasar la información necesaria.

El segundo aspecto se refiere a la información de señalización. Pero siempre que se quiera establecer un circuito virtual se necesita algún tipo de señalización para marcar el camino, es decir, para la distribución de etiquetas entre los nodos. Sin embargo, la arquitectura MPLS no asume un único protocolo de distribución de etiquetas.; de hecho se están estandarizando algunos existentes con las correspondientes extensiones; uno de ellos es el protocolo RSPV del Modelo de Servicios Integrados del IETF. Pero, además en el IETF se están definiendo otros nuevos, específicos para la distribución de etiquetas, cual es el caso del Label Distribution Protocol (LDP).

c) FUNCIONAMIENTO GLOBAL MPLS.

Una vez vistos todos los componentes funcionales, el esquema global de funcionamiento es el que se muestra en la figura (2.4h), donde quedan reflejadas las diversas funciones en cada uno de los elementos que integran la red MPLS. Es importante destacar que en el borde de la nube MPLS tenemos una red convencional de routers IP. El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de routers a una distancia de un solo salto. Funcionalmente es como si estuvieran unidos todos en una topología mallada (directamente o por PVC ATM). Ahora, esa unión a un solo salto se realiza por MPLS mediante los correspondientes LSPs (puede haber más de uno para cada par de routers). La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y que no se pierde la visibilidad sobre los paquetes la vialidad sobre los paquetes IP. Todo ello abre enormes posibilidades a la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario, tal como explicaremos en la sección siguiente.

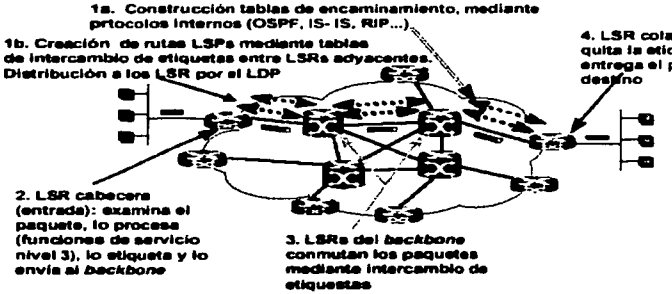


Figura (2.4h)

APLICACIÓN DEL MPLS.

Las principales aplicaciones que hoy en día tiene MPLS son:

- Ingeniería de tráfico.
- Diferenciación de niveles de servicio mediante clases (CoS)
- Servicio de redes privadas virtuales (VPN).

Veamos brevemente las características de estas aplicaciones y las ventajas que MPLS supone para ello frente a otras soluciones tradicionales.

INGENIERIA DE TRÁFICO.

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén suprautilizados, con posibles puntos calientes y cuellos de botella, mientras otros puedan estar infrautilizados. A comienzos de los 90 para adaptar de forma efectiva los flujos de tráfico a la topología física de las redes IP eran bastante rudimentarios. Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente. En casos de congestión de algunos enlaces, el problema se resolvía a base de añadir más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre los enlaces mas congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos). En el esquema de la figura (2.4i) se comparan estos dos tipos de rutas para el mismo par de origen-destino.

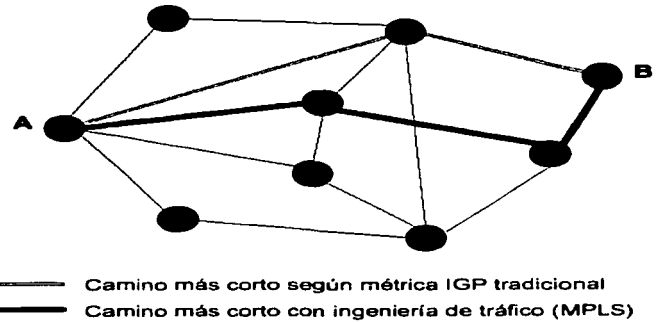


Figura (2.4i)

El camino más corto entre A y B según la métrica normal IGP es el que tiene sólo dos saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los routers correspondientes hagan aconsejable la utilización del camino alternativo indicado con un salto más. MPLS herramienta efectiva para esta aplicación en grandes backbones, ya que:

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.
- Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.
- Permite hacer encaminamiento restringido (Constraint Based Routing, CBR), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad). Por ejemplo, con garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.

La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre un red IP, al margen de que haya o no una infraestructura ATM por debajo, todo ello de manera más flexible y con menores costos de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

CLASES DE SERVICIO (CS)

MPLS esta diseñado para poder cursar servicios diferenciados, según el modelo Diffserv del IETF. Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios. Diffserv permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucha más dependientes del retardo y de la variación del mismo, como son las de video y voz interactiva. Para ello se emplea el campo ToS (type of service), rebautizado en Diffserv como el octeto DS. Esta es la técnica QoS de marcar los paquetes que se envían a la red.

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tiene el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP. De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que:

- El tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP.
- Entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. Por ejemplo, un LSP puede ser tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico best effort, tres niveles de servicio, primera, preferente y turista, que lógicamente, tendrán distintos precios.

REDES PRIVADAS VIRTUALES (VPNs)

Una red privada virtual (VPN) se construye a base de conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y seguridad equivalentes a las que se obtienen con una red privada. El objeto de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos

y video sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone el aislamiento, y privada indica que el usuario cree que posee los enlaces. Las IP VPNs son soluciones de comunicación VPN basadas en el protocolo IP de Internet. En esta sección vamos a describir brevemente las ventajas que MPLS ofrece para este tipo de redes frente a otras soluciones tradicionales.

Las VPNs tradicionales se han venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada, tal es el caso de las redes de datos Frame Relay, que permiten establecer los PCVs entre diversos nodos que conforman la VPN. La seguridad y la garantía las proporcionan la separación de tráficos por PVC y el caudal asegurado (CIR). Algo similar se puede hacer con ATM, con diversas clases de garantías, pero los inconvenientes de este tipo de solución es que la configuración de las rutas se basa en procedimientos mas bien artesanales, al tener que establecer cada PVC entre nodos, con la complejidad que esto supone al proveedor en la gestión. Si se quiere tener conectados a todos con todos, en una tocología lógicamente mallada, añadir un nuevo emplazamiento supone retocar todos los CPEs del cliente y reestablecer todos PVCs (algo muy similar a lo que se vio en la solución IP/ATM). Además, la popularización de las aplicaciones TCP/IP, así como la expansión de las redes de los NSPs, ha llevado a tratar de utilizar estas infraestructuras IP para soporte de VPNs tratando de conseguir una mayor flexibilidad en el diseño e implantación, menores costos de gestión y provisión del servicio. La forma de utilizar la infraestructura IP para servicio VPN (IP VPN) ha sido la de construir túneles IP de diversos modos.

El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente parezcan conectados. Lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de tubería privadas por las que no pueden entrar nadie que no sea miembro de esa IP VPN. No es el objetivo de esta sección dar una exposición completa de IP VPN sobre túneles; solo se pretende resumir sus características para poder apreciar las ventajas que ofrece MPLS frente a esas soluciones. Se puede obtener más información sobre IP VPN con túneles en las referencias correspondientes a VPNs con MPLS.

Los túneles IP en conexiones dedicadas (no se van a tratar aquí de las conexiones conmutadas de acceso) se pueden establecer de dos maneras.

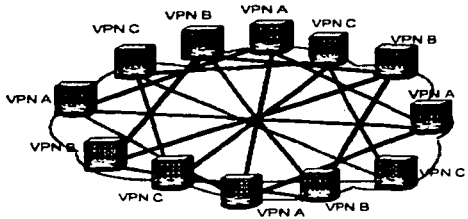
- En el nivel 3, mediante el protocolo IPSec del IETF.
- En el nivel 2, mediante el encapsulamiento de paquetes privados (IP u otros) sobre una red IP publica de un NSP.

En la VPNs basadas en túneles IPSec, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte por la red del proveedor. Es relativamente de implementar, bien sea en dispositivos especializados, tales como cortafuegos, como en los propios routers de acceso del NSP. Además como es un estándar IPSec permite crear VPNs a través de redes de distintos NSPs que sigan el estándar IPSec. Pero como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS son bastantes limitadas, ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes clases de servicio. Además, solo vale para paquetes IP nativos, IPSec no admite otros protocolos.

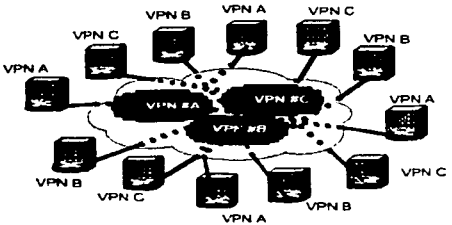
En los túneles de nivel 2 se encapsulan paquetes multiprotocolos (no necesariamente IP), sobre los datagramas IP de la red del NSP. De este modo la red del proveedor no pierde la visibilidad IP, por lo que hay mayores posibilidades de QoS para priorizar el tráfico por tipo de aplicación IP. Los clientes VPN pueden mantener su esquema privado de direcciones, estableciendo grupos cerrados de usuarios, si así lo desean. (Además de encapsular los paquetes, se puede cifrar la información para mayor seguridad, pero en este caso limitando las opciones QoS). A diferencia de la opción anterior, la operación de túneles de nivel 2 esta condicionada a un único proveedor. A pesar de las ventajas de los túneles IP sobre los PVCs, ambos enfoques tienen unas características comunes que los hacen menos eficientes frente a la solución MPLS:

- Están basados en conexiones punto a punto (PVCs o túneles).
- La configuración es manual
- La provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones.
- Plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales.
- La gestión de QoS es posible en cierta medida, pero no se puede mantener extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte.

Realmente, el problema que plantean estas IP VPNs es que están basadas en un modelo topológico superpuesto sobre la topología física existente, a base de túneles extremo a extremo (o circuitos virtuales) entre cada par de routers de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos. Con una arquitectura MPLS se obvian estos inconvenientes ya que el modelo topológico no se superpone sino se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una nube común en las que solamente pueden entrar los miembros de la misma VPN. Las nubes que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mismo intercambio de etiquetas MPLS. Los LSPs son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo. Aquí esta la diferencia: en los túneles se utiliza en encaminamiento convencional IP para transportar la información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de routing IP. Sin embargo, si se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada de rutas MPLS sino que ve una Internet privada (intranet) entre los miembros de su VPN. De este modo, se pueden aplicar técnicas QoS basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hasta el destino, pudiendo así reservar el ancho de banda, priorizar aplicaciones establecer CoS y optimizar los recursos de la red con técnicas de ingeniería de trafico.



Modelo "superpuesto" (Túneles o PVCs)
Topología VPN conectiva



Modelo "acoplado" (MPLS)
Topología VPN no-conectiva

Figura (2.4j)

En la figura (2.4j) se presenta una comparación entre ambos modelos, la diferencia entre los túneles IP convencionales (o los circuitos virtuales) y los túneles MPLS (LSPs) esta en que estos se crean dentro de la red, a base de LSP y no de extremo a extremo a traves de la red.

Como resumen, las ventajas que MPLS ofrece para IP VPNs son:

- Proporcionan un modelo acoplado o inteligente, ya que la red MPLS sabe de la existencia de VPNs (lo que no ocurre con túneles ni PVCs).
- Evita la complejidad de los túneles y PVCs.
- La provisión del servicio es sencilla: una nueva conexión afecta a un solo router.
- Tiene mayores opciones de crecimiento modular.
- Permite mantener garantías de QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones de diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con clases definidas a la entrada.
- Permite aprovechar las posibilidades de ingeniería de tráfico para poder garantizar los parámetros críticos y la respuesta global de la red (ancho de banda, retardo, fluctuación) lo que es necesario para un servicio completo VPN.

2.5 SONET/SDH

En 1987 los laboratorios de investigación Bell propusieron un nuevo sistema de multiplexado denominado SONET (Synchronous Optical Network, Red Óptica Síncrona) para sustituir a PDH, con una velocidad base de 51Mbps. SONET fue estandarizado por ANSI, compatible con SDH (Synchronous Digital Hierarchy, Jerarquía Digital Síncrona) estándar de ITU-T, el modelo OSI/ISO estándar de capa 1 (physical layer)

PROBLEMAS DE PDH(Plesiochronous Digital Hierarchy, Jerarquía Digital Plesiocróna)
Incompatibilidad internacional.

- No pensada para fibra óptica (diseñada en los 60)
- Capacidades máximas bajas: Japón 98Mbps, Norteamérica 274 Mbps, resto del mundo 139Mbps.
- Carece de herramientas de gestión ni posibilidad de tolerancia de fallas.
- El uso de bits de relleno impide el multiplexado entre niveles contiguos.

SONET/SHD

- El sistema americano (SONET) no es idéntico al internacional (SDH) pero ambos son compatibles.
- Defines interfaces de fibra óptica.
- La capacidad llega de momento a 10 Gbps.
- Disponen de herramientas de gestión y tolerancia a fallas (recupera averías en 50 ms)
- Utiliza punteros; permite el multiplexado entre niveles no contiguos.
- Permite seguir utilizando PDH en enlaces de menor capacidad.

ELEMENTOS FISICOS DE SONET/SDH

- Una red SONET/SDH esta formada por:
  - Repetidores
  - Multiplexores, llamados ADM (Add Drop Multiplexor). Permiten intercalar o extraer tramas (ej. Un STM-1 en un STM-4).
  - Digital Cross Connect: actúan como los ADM Pero permiten crear anillos.

- A menudo se utilizan topologías de anillo para aumentar la fiabilidad.

ARQUITECTURA DE SONET/SDH

- SONET/SDH divide la capa física en cuatro subcapas:
  - Fotónica: transmisión de la señal y las fibras.
  - De sección: la interconexión de equipos contiguos.
  - De línea: multiplexación/desmultiplexacion de circuitos entre dos ADM.
  - De rutas: problemas relacionados con la comunicación extremo a extremo.

PACKET OVER SONET/SDH

Packet Over SONET (PoS) es una tecnología que envía, traza o mapea los datos IP directamente por encima de una capa SONET. PoS toma ventaja de la robustez de SONET/SHD infraestructura que aumenta al máximo la eficacia de transportar el paquete. La tecnología PoS es comúnmente usada por los ISPs a lo largo de su extenso tendido en el backbone de red para soportar o proveer alta disponibilidad. Mientras las interfaces de velocidad de PoS están aumentando, la tecnología subyacente de PoS no ha cambiado. PoS traza paquetes de IP por defecto en tramas de SONET/SHD; hay tres elementos principales para PoS: (1) un protocolo de acceso de eslabón como PPP (2) el octeto asíncrono HDCL ideado como (RFC1662: PPP in HDCL) y (3) la carga útil preparada (RFC2615: PPP over SONET/SDH) antes de su inserción en SONET la carga útil síncrona es envuelta (SPE). El mismo modelo de PoS puede ser usado para mapear datos Ethernet soportados en L2.

VENTAJAS DE PoS

PoS (Packet over SONET, o PPP over SONET)

- Usando PPP (Point to Point Protocol) el overhead se reduce al 3%(campos de control, CRC y relleno de bits).
- Además de mejorar el rendimiento se reduce equipamiento y por tanto costos.
- PPP over SONET/SDH esta estandarizado en el RFC 2615(6/99) y el RFC 5/1994) ya obsoleto.
- Actualmente PoS es de uso habitual en redes SONET/SDH de grandes ISPs (solo trafico IP)
- Al suprimir la capa ATM se pierde capacidad de gestión y multiplexación. No se pueden conectar centrales, solo trafico IP.
- En PoS la multiplexación ha de hacerse con circuitos SONET/SDH. Ejemplo: un enlace STM-4 se puede dividir en cuatro STM-1, tres para IP y uno para ATM.
- Interesa usar POS cuando:
  - Todo el trafico es IP, ó
  - La mayor parte del tráfico es IP y el que no lo es se puede encapsular en IP (ej. VoIP).

INCONVENIENTES DE SONET/SDH

- SONET/SDH se diseño pensando en telefonía, donde la fiabilidad del circuito era fundamental. Para datos SONET/SDH presenta algunos inconvenientes:
  - La comunicación no siempre va por el camino mas corto.
  - Hay un reparto estático de la capacidad entre circuitos.
  - La fibra de reserva no se utiliza, pero ha de estar preparada con todo su equipamiento por si falla la otra.
  - En IP el nivel de red ya incorpora fiabilidad (OSPF), por lo que las funciones de SONET/SDH son innecesarias.

Las siguientes tablas nos muestran los acrónimos sobre aquellas jerarquías mayores y su vez nos describen las equivalencias en anchos de banda o caudales de diferentes medios y tipos de enlaces mas comúnmente usados en redes WAN.

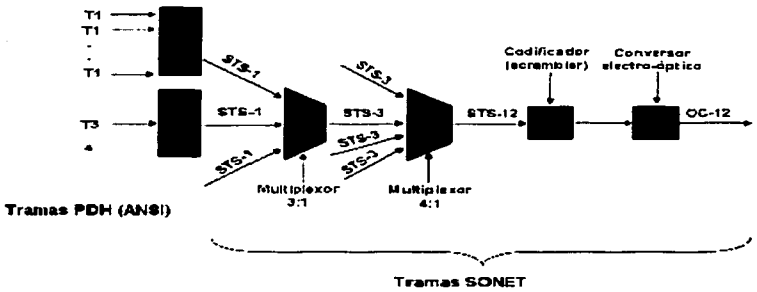
STM	**SYNCHRONOUS TRANSPORT MODULE**
DS	**DIGITAL SIGNAL**
OC	**OPTICAL CARRIER**
STS	**SYNCHRONOUS TRANSPORT SIGNAL**
PDH	**PLESIOCHRONUS DIGITAL HIERARCHY**
SDH	**SYNCHRONOUS DIGITAL HIERARCHY**
SONET	**SYNCHRONOUS OPTICAL NETWORK**

PDH		SDH	SONET
NORMA EUROPEA	NORMA AMERICANA		
E0 = 64 Kbps	DS0 = 64 Kbps	STM-1 = 155.52Mbps	OC-1= 51.84 Mbps
E1 = E0 x 32	DS1 = 24 x DS0	STM-4 = 4 x STM1	OC-3 = 3 x OC-1
E2 = E1 x 4	DS2 = 4 x T1	STM-16 = 4 x STM-4	OC-12 = 4 x OC-3
E3 = E2 x 4	DS3 = 7 x T2	STM-64 = 4 x STM-16	OC-48 = 4 x OC-12
E4 = E3 X 4			OC-192 = 4 x OC-48

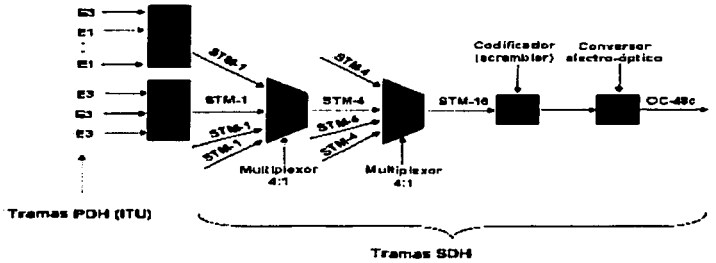
ENLACES	ANCHO DE BANDA O CAUDAL
STM-64	9953.28 Mbps
STM-16	2488.32 Mbps
STM-4	622.68 Mbps
STM-1	155.52 Mbps
OC-192	9953.28 Mbps
OC-48	2488.32 Mbps
OC-12	622.68 Mbps
OC-3	155.52 Mbps
OC-1	51.84 Mbps
DS3/T3	44.736 Mbps
DS2/T2	6.312 Mbps
DSO	64 Kbps

Los siguientes gráficos de las figuras (2.5a) nos muestran el esquema general del mutiplexaje tanto de SONET como en SDH.

Multiplexación SONET

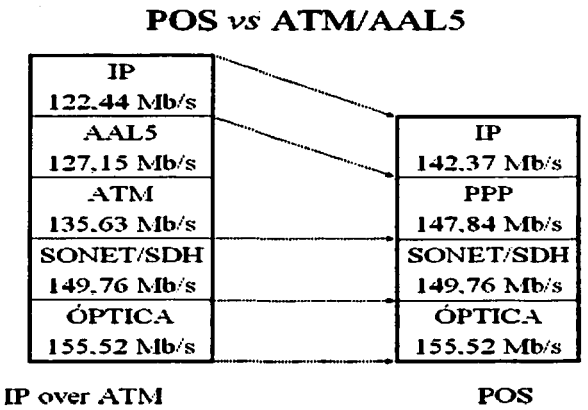


Multiplexación SDH



Figuras (2.5a)

En la gráfica de la figura (2.5b) se aprecia la ventaja de PoS vs ATM utilizando SONET/SDH.
Figura (2.5b)



DESARROLLO DE LA PROBLEMÁTICA

3.1 ANTECEDENTES

En el siguiente capitulo dejaremos plasmados los elementos más importantes de cómo opera hoy en día la Red Nacional de Telecomunicaciones IMSS (RITEL, Red Integral de Telecomunicaciones), así como una breve descripción de los antecedentes de la misma, para ello hemos tomando como referencia y punto de partida la ultima actualización tecnológica 1998 que tuvo gran impacto y repercusión sobre la RITEL.

La falta de continuidad en las directrices informáticas registradas en los últimos años del siglo XX originadas por la rotación en los niveles directivos de la entonces Coordinación de Informática, incidieron directamente en el tiempo con que se contaba para afrontar los retos (especialmente el relativo al año 2000) y compromisos informáticos del Instituto razón por la cual se torno particularmente necesario poner en contexto dichos factores que dieron origen a la situación que actualmente enfrenta la Dirección de Innovación y Desarrollo Tecnológico antes Coordinación General de Informática.

En septiembre de 1995, se estableció el plan informático que marcaría las líneas de acción para el periodo 1996-2000 en concordancia con los planes, programas y estrategias definidas por la entonces presente administración. Cabe señalar sin embargo que dicho plan no considero el advenimiento del año 2000, esto presumiblemente, en virtud de que aun no se marcaba el impacto que tendría en las áreas informáticas, por lo tanto en dicho documento no se previo ninguna acción al respecto. Sin embargo se consideraba entre otras cosas el fortalecimiento de la infraestructura de computo en los niveles operativos, delegacionales y regionales, integrando la función informática en estricta consistencia con la evolución, prioridades y estrategias del Instituto, asegurando el uso de las tecnologías adecuadas.

En 1997, la transición de titulares registrada, dio origen a un cambio hacia un nuevo esquema estratégico informático que se traducía en cambios radicales en la plataforma tecnológica, destacando la aparición de los Centros Informáticos de Zona para centralizar las funciones que estos efectuaban en uno solo con los riesgos que esta decisión implicaba, no contemplando ninguna estrategia preventiva para abordar la problemática del año 2000, hecho que quedo de manifiesto en la sesión del 28 de julio de 1997 donde se presento al Comité de Informática la carpeta de proyectos 1997-2000.

En febrero de 1998, como parte de las acciones de una nueva administración de Informática, se determino como proyecto de alta prioridad la problemática del año 2000. por consiguiente y como parte de la estrategia para hacerle frente, la Coordinación de Informática solicito apoyo a los proveedores para determinar la situación del Instituto y estar en posibilidades de generar las acciones pertinentes.

En abril del mismo año, se sometió a la consideración del comité de Informática el proyecto que tenia por objetivo retomar la zonificación de los servicios, fortaleciendo la infraestructura tecnológica de los Centros Informáticos de Zona; toda vez que la conclusión de dicho estudio fue que la mejor estrategia para apegarse a los lineamientos Institucionales, era mantener los tres CIZ's (Centro Informático de Zona), al representar el menor riesgo para la operación del Instituto. Para atender los compromisos impostergables, se elaboro un programa de trabajo con diferentes requerimientos para atenderlos en tiempo y forma. Dentro de ese programa, un parte importante lo constituyo la adquisición de bienes informáticos.

El manejo y administración de los recursos informáticos por parte del IMSS hoy en día han permitido fincar las bases para afrontar la demanda actual con un nivel optimo. Sin embargo el crecimiento de esta demanda, hace imperante replantear las necesidades que en materia de recursos de computo y comunicaciones se requieren. Por ello, y dando continuidad a la estrategia del IMSS, se considero la infraestructura dividida en tres regiones o CIZ (Centro Informático de Zona), manteniendo la estabilidad e integridad de la información al soportar la base de datos más grande de América Latina y considerando los nuevos requerimientos. Así mismo, al conocer los escenarios que con el paso del tiempo el IMSS pretende alcanzar, por ello en su momento se estructuro la propuesta que de alguna forma correspondía a las necesidades planteadas y la infraestructura contemplada le permitiría al IMSS crecer con el ritmo y evolución que sus necesidades le requerían.

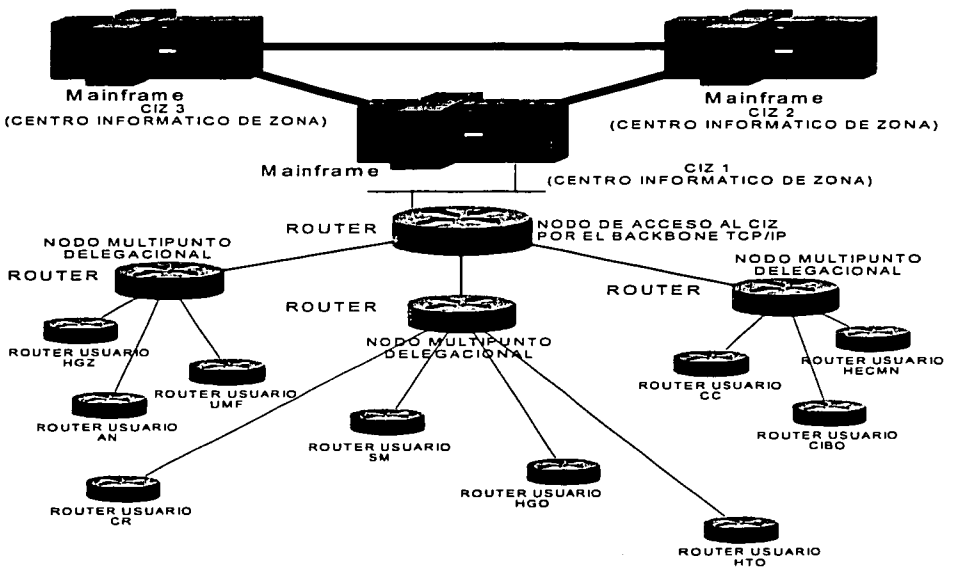
3.1.1 ESQUEMA JERÁRQUICO DE COMUNICACIONES EN LA RITEL

A partir del siguiente esquema de la figura (3.1.1a) se describe el orden y jerarquía de cómo se encuentran hoy en día establecidas las comunicaciones hacia los diferentes nodos de la RITEL. Ello nos sirve de referencia para observar a que nivel se ha estado trabajando en la RITEL en los últimos años y el impacto que causa cuando se presentan fallas y contingencias sobre la WAN, además también nos aporta los niveles de operación y jerarquía que ocupan las diferentes áreas institucionales, ya que esto nos servirá de guía para abordar los siguientes puntos de este capitulo.

Por lo que se refiere al nivel de operación, jerarquía e importancia los sitios de la WAN están asignados de la siguiente manera:

- El nivel mas alto en prioridad de comunicaciones lo ocupan los CIZ's, ya que el solo hecho de que algún CIZ salga de la red impacta a todos los usuarios que dependan del mismo puesto que ocupa la jerarquía mayor en la topología, aunque su salida no impacte a los demás CIZ's.
- Nodos delegacionales ocupan la segunda jerarquía ya que a través de ellos se enruta a la gran mayoría de los usuarios finales hacia los CIZ's para la consulta e introducción de información vital para la institución. Aquí se podemos observar que si llega a salirse un nodo delegacional solo impacta este a los usuarios que dependan del mismo y no afectando al todo el CIZ.
- El tercer nivel lo ocupan los usuarios finales que es donde radica la mayor parte de operación del instituto; en este nivel tenemos a las clínicas, hospitales, subdelegaciones administrativas, almacenes, centros de capacitación. Figura (3.1.1a)

ESQUEMA JERARQUICO DE CONECTIVIDAD HACIA LOS SITIOS DE LA RITEL



NODOS USUARIO FINAL

3.2 ACTUALIZACIONDE 1998

El objetivo de esos días era responder a los requerimientos técnicos planteados en el documento "Modernización de servicios Informáticos" presentados al IMSS en donde se planteo las soluciones técnicas y económicas. La propuesta considero los siguientes rubros y equipamiento:

a) Tres procesadores 9672, uno en cada CIZ.
b) Crecimiento de espacio en disco por 790 GB, repartidos en los tres CIZ.
c) Dos unidades de cartucho para Monterrey y dos para Guadalajara.
d) Crecimiento de los controladores de comunicaciones de cada CIZ.
e) Un controlador de terminales 3174 local para Monterrey y uno para Guadalajara.
f) Administración y control del proyecto a través de un project manager.
g) Servicio de asesoría técnica a tiempo y materiales por parte de ingeniería de sistemas durante un periodo de 100 horas.
h) Servicios de migración del sistema operativo y programas producto IBM.
i) Servicios de capacitación para la actualización en la nueva versión del sistema operativo y programas productos asociados.

A continuación se describe la solución IBM que de acuerdo a sus requerimientos, cubrió las necesidades planteadas, cuyo objetivo era aumentar la capacidad para atender la demanda de servicios tecnológicos de información y atención a requerimientos adicionales que anteriormente no eran cubiertos. Para ellos se propuso un procesador CMOS (Complementary Metal Oxide Semiconductor) por cada CIZ, capacidad de almacenamiento incrementada 790GB adicionales por los tres CIZ's. Cambios en la estructura de comunicaciones y los servicios de migración de sistema operativo OS/390 y programas producto, así como los recursos de actualización a los nuevos productos.

PROCESADORES

Para el caso de los procesadores y debido a los avances tecnológicos IBM propuso instalar equipos con tecnología CMOS. Específicamente los equipos propuestos para cada una de las localidades.

Equipo	Localidad	Memoria	Capacidad	Canales	Grupo SW
9672-RB6	MEXICO	1 GB	169 MIPS	32 ESCON Y 15 PARALELOS	60
9672-RA6	MONTERREY	1 GB	87 MIPS	24 ESCON Y 6 PARALELOS	40
9672-RA6	GUADALAJARA	1 GB	87 MIPS	24 ESCON Y 6 PARALELOS	40

Cabe señalar:

- El incremento de canales se hace a través de adicionar tarjetas y cada tarjeta contempla ya sea 3 canales paralelos o 4 ESCON.
- El grupo de software esta en función de la capacidad de proceso del equipo.

UNIDADES DE DISCOS

A fin de satisfacer las necesidades de espacio en disco del IMSS se propuso continuar con la tecnología RVA-2 turbo, ya que es una de la s tecnologías mas recientes del mercado, la distribución en cada CIZ quedo de la siguiente manera:

Equipo	Localidad	Capacidad	Mem cache	Adaptadores
9393-T82	MEXICO	420 GB	2GB	8 ESCON
9393-T82	MONTERREY	240 GB	2GB	8 ESCON
9393-T82	GUADALAJARA	290 GB	2GB	8 ESCON

Nota: en el caso de Monterrey, se instalo el equipo 9393-T42 que se encontraba en México creciéndolo en 80GB de espacio y 1GB de memoria cache.

UNIDADES DE CARTUCHOS

Equipo	Localidad	Capacidad	Adaptadores
(1) 3490-FC0 (2) 3490-F11	MONTERREY	2 DRIVERS	2 ESCON
(1) 3490-FC0 (2) 3490-F11	GUADALAJARA	2 DRIVERS	2 ESCON

En caso de México se mantuvieron los equipos actualmente instalados.

SOLUCIÓN DE COMUNICACIONES

Para la red de comunicaciones (RITEL, Red Integral de Telecomunicaciones), la propuesta del año de 1998 pretendía resolver los requerimientos tales como: puntos únicos de falla, capacidad limitada de usuarios de la red TCP/IP debida a los Gateways, facilitando la operación tanto para la adición de usuarios y recursos como para permitir trabajar configuraciones dinámicas.

Adicionalmente el equipo manejaría tanto protocolo SNA como TCP/IP, por lo que soportaría la conexión entre los centros de computo con protocolo SNA puro como lo hacen los 3745 (función cross domain). De igual forma tendría que soportar la conexión de Mainframes IBM que pertenezcan a otras redes en protocolo SNA puro función (EBN).

Cabe señalar, que el equipo propuesto hoy en día tiene la capacidad de soportar hasta 16,000 usuarios y si fuese necesario puede ser incrementado.

Dentro de las nuevas características de los controladores de comunicaciones están el tener adaptadores de redes LAN tanto en Token Ring como en Ethernet, funciones como la de conversión de protocolo SNA a TCP/IP y viceversa (TN3270S) a demás de dispositivos con mayor capacidad para el manejo de líneas y canales ESCON, entre otras funciones.

Para llevar a acabo esa actualización tecnológica, la propuesta contemplaba el cambio de los equipos que actuaban en esos días, de esta manera los controladores de comunicaciones 3746-900 existentes cambiarían a 3746-950 cuando no estuvieran unidos los existentes 3745.

Los controladores de comunicaciones actualmente requieren programas de software para el manejo de los recursos de la red, tales programas son: NCP, SSP y NPSI. Los equipos 3746-950 no requieren de estos programas para trabajar, por lo que los programas productos NCP, SSP y NPSI serán canceladas cuando se desacoplen los 3745.

Por lo tanto se tendrían ahorros tanto en el software que utilizan los controladores, así como en el mantenimiento del hardware de la parte 3745 del equipo actual. Adicionalmente se obtendrían ahorros en la renta de equipo de TELMEX, ya que se contempla la eliminación de equipo exterior como son los Gateways (RS-6000) y algunos routers que están entre los controladores y la red de TELMEX.

La solución consideraba el crecimiento de los equipos 3746-900 de cada localidad, para darles la capacidad de proceso en la parte 3746-900 y poder independizarlos después de los 3745. Para el caso de Monterrey y Guadalajara se proponen 2 procesadores de comunicaciones (NNP) para poder tener respaldo entre ellos mismos. Para la ciudad de México se considero un procesador por cada uno de los 3746-900 y el respaldo se haría con los LANs de Token Ring y Ethernet interconectando ambos 3746-900. el procesador de comunicaciones (NNP) permite que el controlador 3746-900 pueda trabajar sin la necesidad de los programas de SW de comunicaciones (NCP, NPSI y SSP). Otros dispositivos propuestos fueron los canales ESCON, de acuerdo a los requerimientos en cada localidad: dos canales ESCON para Monterrey y Guadalajara (uno por cada procesador), dos canales ESCON para

el 3746-900 actualmente conectado al 9021 (finalmente 9672), y tres canales ESCON para el equipo, conectado al 9121 (finalmente 9672). También se considero la instalación de adaptadores Token Ring para cada uno de los 3746-900: 2 procesadores Token Ring y estos con 3 acopladores para LAN Token Ring y un acoplador para LAN Ethernet.

En cuanto a las líneas de comunicación seriales se contemplaron: 2 acopladores para soportar líneas a velocidad de E1 para cada CIZ, adicionalmente para México el 3746-900 conectado a la CPU ex9121 (finalmente 9672) y tendría: 20 líneas a 19.2 Kbps, y 5 a 64 Kbps. Y para el 3746-900 actual, conectado a la CPU ex9121 (finalmente 9672): 10 líneas a 19.2 Kbps y 4 a 64 Kbps. Los equipos de Monterrey y Guadalajara cuentan ya con líneas seriales en el equipo 3746-900, por lo que no se incluyo ningún adaptador para soportar líneas seriales. De manera que el crecimiento propuesto para cada controlador 3746-900 de cada CIZ se resume en el siguiente cuadro.

Localidad	Procesador Nodo de Red (NNP)	Procesador ESCON (ESCP3)	Procesador Token Ring (TRP3)	Procesador de líneas (CLP3)	Exp. Memoria 64 Mb para NNP2	MAE
México(9021)	1	3	2	2	1	1
México(9021)	1	2	2	2	1	1
Monterrey	2	2	2	1	1	1
Guadalajara	2	2	2	1	1	1

El MAE (Multiaccess Enclosure), es un componente de avanzada tecnología que integra múltiples adaptadores para conectarse a diversos medios y ambientes además de una gran variedad de funciones. La propuesta contemplo un MAE por cada 3746-900, el cual tendría 128 Mb de memoria (64 de memoria base y 64 Mb de expansión), además cada MAE cuenta con 2 adaptadores Ethernet 10/100, adaptador Token Ring y la función de conversión de protocolos SNA y TCP/IP y viceversa, así como una tarjeta de 6 puertos para conexión serial. Este componente esta integrado al controlador 3746 y su configuración se resume en el siguiente recuadro.

Localidad	Puertos Ethernet10/100	Puertos Token Ring	Exp. Memoria 64 Mb para MAE
México(ex 9021)	2	1	1
México(ex 9021)	2	1	1
Monterrey	2	1	1
Guadalajara	2	1	1

Es importante considerar de ello lo siguiente:

a) Tanto el 3746-900 como el MAE en sí mismo consideran una fuente de poder redundante.

b) Se le llama ex9021 y ex9121 solo por referencia a la configuración actual, pero finalmente se conectaran al procesador 9672.

Adicionalmente a los crecimientos de comunicaciones fue necesario considerar que los procesadores trabajarían con particiones, en la ciudad de México se requirió de tres particiones, mientras que Monterrey y Guadalajara dos. Cada partición requiere al menos de un controlador de terminales 3174 en el modelo local la ciudad de México tiene tres de estos controladores 3174 por lo que no tiene problema, pero Monterrey y Guadalajara solo tienen un controlador 3174 por lo que se requirió tener un controlador 3174 local mas en cada

caso. La propuesta considero dos controladores 3174 modelo 11L con puertos para conexión de hasta 8 terminales para conectarse a canal paralelo, uno para monterrey y el otro para Guadalajara.

Esta infraestructura de comunicaciones propuesta considero la posibilidad de hacer adiciones posteriores y según las necesidades del IMSS a una serie de facilidades, funciones y ambientes tales como: participar en LAN o WAN en ATM, LAN en FDDI, líneas E3, líneas con E1 canalizados, Fast Ethernet además de tener la facilidad de participar como Gateways, Routers y/o Switches en una Red TCP/IP conectada o no a los procesadores, poder hacer un segundo Backbone entre México, Monterrey y Guadalajara tanto en SNA como en TCP/IP según se requiriera

SOFTWARE

En cuanto al software se propuso reemplazar el sistema operativo MVS/ESA V4 Release, por el nuevo OS/390 V2 Release 6.

BENEFICIO DE LA PROPUESTA

1. Recuperación de espacio físico dentro del centro de computo actual destinado a los procesadores y discos.

2. Ahorro en el consumo de energía eléctrica en los procesadores, en donde este consumo al año le da al Instituto ahorros significativos. La nueva tecnología CMOS, permitió dejar de utilizar la instalación de agua que era parte del sistema de enfriamiento, con los ahorros respectivos en energía eléctrica.

3. La tecnología en equipos periféricos que estaban instalados como cintas, controladores de comunicaciones podían seguir siendo utilizados.

4. El contar con tres centros de computo, le permite al IMSS contar con la infraestructura necesaria para que el instituto minimice los riesgos sociales y/o políticos en caso de alguna contingencia, ya que al considerar el escenario 3, al cual el IMSS deseaba llegar, cada centro de computo realizaría la función de respaldo.

5. Los impactos del año 2000 en hardware IBM con esta nueva tecnología se eliminaron, permitiendo al departamento de sistemas enfocarse a los impactos en las aplicaciones.

6. Con la nueva tecnología, se vio disminuido el costo de mantenimiento de los equipos, en base al rendimiento de los mismos.

3.3 EL BACKBONE SNA

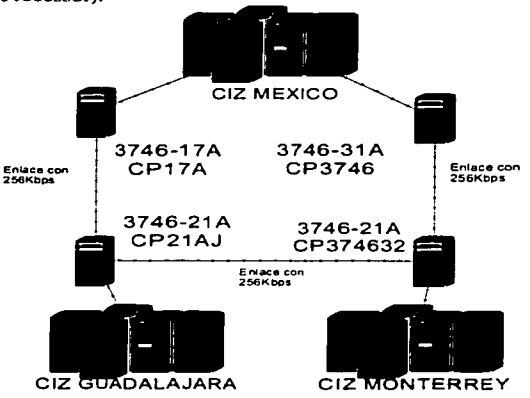
El siguiente punto del capítulo presente tiene como objetivo plantear la descripción del entorno de comunicaciones que se utiliza actualmente el Instituto Mexicano del Seguro Social en el ámbito de su Red WAN utilizada hoy en día exclusivamente para datos y más adelante en lo que toca al backbone TCP/IP daremos un pequeño esbozo de la red de voz; los servicios de voz y datos hoy en día no están integrados en la misma red por lo cual también podemos citar indiscutiblemente que esto también forma parte de la problemática actual.

La Red Integral de Telecomunicaciones (RITEL) del Instituto Mexicano del Seguro Social hoy en día cuenta con un esquema de comunicaciones que consta e involucra 795 puntos o nodos principales distribuidos a lo largo y ancho de la República Mexicana en las diferentes Delegaciones Metropolitanas del D.F. y área conurbada, así como en las distintas Delegaciones Estatales del interior de la República. Cada una de estas Delegaciones alberga dentro de su entorno geográfico y en el ámbito de su jurisdicción un determinado número de usuarios (nodos terminales), redes LAN.

En la Red de Nacional de Telecomunicaciones se cuenta con dos arquitecturas principales para las comunicaciones de toda la red. Estas son la arquitectura SNA propia de IBM y la arquitectura TCP/IP estándar con mas difusión, de las cuales ya hablamos en el capitulo uno.

La arquitectura SNA es usada básicamente para enlazar los Centros Informáticos de Zona (CIZ's), de los cuales el IMSS cuenta con tres de ellos a nivel nacional, CIZ 1 para la región del centro y suroeste del país con cede en la ciudad de México Distrito Federal, CIZ2 para la región norte del país con cede en la ciudad de Monterrey Nvo León y CIZ 3 para atender la región occidente del país con cede en la ciudad de Guadalajara Jalisco. Estos CIZ's se encuentran conectados entre sí con la siguiente topología física que asemeja una delta, la cual se detalla en el esquema de la figura (3.3a)

Figura (3.3a) Esquema sobre la Arquitectura, y Backbone SNA implementada en telecomunicaciones, así como su conectividad hacia los 3 CIZ's del Instituto Mexicano de Seguro Social, en la cual también se observa la manera de cómo están integrados los equipos IBM Main Frame y controladores de Comunicaciones o también denominados FEP's (Front End Processor).



ESQUEMA SNA
DE LA RED NACIONAL
DEL IMSS

Para enlazar los CIZ's se dispone de 3 enlaces de 256 Kbps (4 E0's) entre cada CIZ, mismos que integran el backbone SNA con en ancho de banda total de 768 Kbps (12 E0's). Este backbone conecta los diferentes procesos en línea y batch entre con cada uno de los CIZ's, ya que sobre la arquitectura SNA es donde residen la gran mayoría de los sistemas sustantivos y bases de datos con las que cuenta el Instituto Mexicano del Seguro Social; tales como:

- SINDO (Sistema Nacional de Derechos y Obligaciones)
- CANASE (Catalogo Nacional de Asegurados)
- PSM (Pago de Subsidios Médicos)
- IDSE (IMSS desde su Empresa)
- SAI (Sistema de Abasto Institucional) Hp Unix
- SISCOB (Sistema de Cobranza)
- SPES (Sistema de Prestaciones Económicas y Sociales)
- SIAP (Sistema Informático de Asistencia y Puntualidad)
- SUE (Sistema Único de Emisión)
- SAIIA (Sistema de Acopio Interactivo de Información Afiliatoria)
- CAVD (Certificado Automatizado de Vigencia de Derechos)
- Seguridad de Mainframe, RACF y Soporte Técnico
- Operación
- Mesa de ayuda

La tecnología de WAN implementada para las comunicaciones sobre el backbone SNA es Frame Relay.

3.4 EL BACKBONE TCP/IP

De la misma manera que el backbone SNA, se cuenta con un backbone TCP/IP con un esquema de topología jerárquica a partir de cada CIZ regional. En ancho de banda del que se dispone para interconectar los diferentes nodos es variable, a partir del tipo de nodo y su importancia según la jerarquía que este ocupe en la RITEL. 12 E0's a nivel de Backbone entre cada CIZ's (Nodos concentradores en TCP/IP) con un ancho de banda de 768 Kbps ocupan la jerarquía mayor y 1E0 con 64 Kbps a nivel de usuario final (Nodos Final de WAN) ocupan el enlace de datos mas pequeño actualmente utilizado sobre la red. De lo anterior se desprende la siguiente tabla y el grafico de la figura (3.4a) que nos indican la manera de los diferentes sitios con los que cuenta la RITEL, así como la forma en que se encuentra asignado el ancho de banda correspondiente a los diferentes nodos (usuarios) con los que cuenta la RITEL.

Grafico (3.4a)

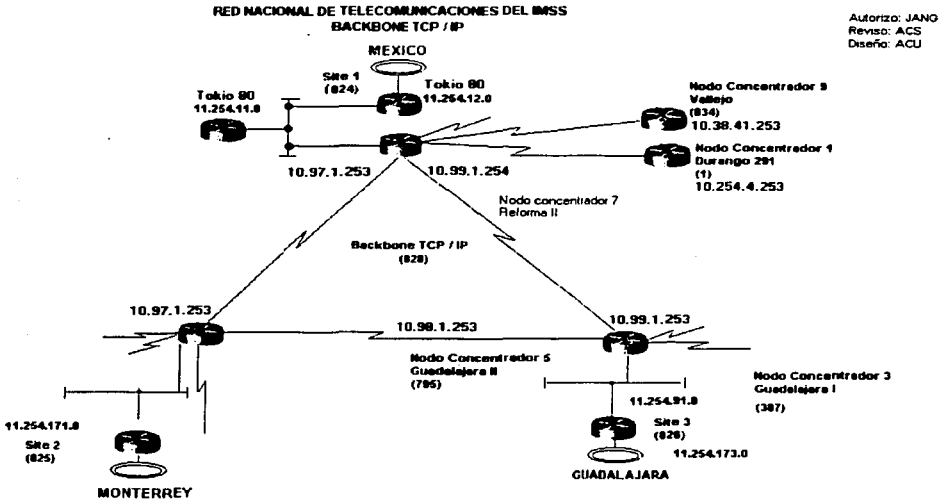
Tipo de Sitio	Numero de Enlaces	Ancho de Banda	Tipo de Nodo
Nodo Concentrador México D.F.	12 E0's	768 Kbps	Enlace Backbone
Nodo Concentrador Monterrey Nvo. León	12 E0's	768 Kbps	Enlace Backbone
Nodo Concentrador Guadalajara Jalisco	12 E0's	768 Kbps	Enlace Backbone
Nodo Concentrador Durango 291 México D.F.	12 E0's		Multipunto Intermedio
Delegaciones Metropolitanas	2 E0's	128 Kbps	Multipunto Intermedio
Delegaciones Estatales	2 E0's	128 Kbps	Multipunto Intermedio
Almacén Nacional Vallejo	6 E0's		Nodo Final
Almacenes Delegacionales	2 E0's	128 Kbps	Nodo Final
Subdelegaciones Metropolitanas	1 E0	64 Kbps	Nodo Final
Subdelegaciones Estatales	1 E0	64 Kbps	Nodo Final
Hospitales	1 E0	64 Kbps	Nodo Final
Oficinas y Edificios Administrativos	1 E0	64 Kbps	Nodo Final
Unidades Medico Familiares	1 E0	64 Kbps	Nodo Final
Centros de Capacitación	1 E0	64 Kbps	Nodo Final
Centros Vacacionales	1 E0	64 Kbps	Nodo Final
Nota: esta tabla solo ejemplifica la diversidad de los enlaces con los que se cuenta hoy en día, ya que el detallar todos y cada unos de los nodos a nivel Nacional nos ocuparía demasiado; esta tesis pretente dar en este capitulo un esbozo de la situación actual de las comunicaciones de la red de datos (RITEL)			

¿Por que un backbone SNA y otro TCP? La respuesta obedece a que como ya mencionamos el backbone SNA tiene la misión de mantener las comunicaciones levantadas al 100 % entre los tres CIZ's, ya que el IMSS cuenta con equipos Mainframe en cada CIZ, y no debemos omitir mencionar que el Instituto Mexicano del Seguro Social a mantenido sus aplicaciones nativas, sistemas, bases de datos etc. durante décadas atrás con Arquitectura de IBM por lo que estos equipos necesitan y requieren de ese ambiente de comunicaciones, sin que esto quiera decir

que no sea posible migrar a otros equipos o incluso a sistemas multiplataforma. Otra razón mas es por que al contar el IMSS con SNA como principal plataforma de comunicaciones se concibió la idea de contar además con la plataforma TCP/IP que es un estándar abierto, universal y que también es compatible con SNA lo cual nos permite ahorrar costos sin tener que deshechar la tecnología con la que se viene trabajando desde años atrás. De lo anterior se desprende la justificación de cómo y por que se decidió seguir trabajando con SNA y TCP/IP.

Por otra parte puesto que la gran mayoría de los usuario operativos en los diferentes sistemas no conocen ni tienen algún vinculo estrecho o conocimientos elevados con el esquema SNA, ya que es demasiado complejo, surge la necesidad de proveer de algunas herramientas para poder acceder a la consulta y a la introducción de información en los diferentes sistemas. Para esto se cuenta con el backbone TCP que es una estándar más universal en redes y que bastante compatible con los equipos utilizados para este fin, como son los sistemas operativos Windows y UNIX. Cabe señalar que el hecho de tener levantados los protocolos de la familia TCP/IP no basta para poder acceder a la información contenida en los CIZ's. Para ello también se dispone de herramientas de emulación 3270 que permiten interactuar, a los equipos con TCP/IP con la infraestructura SNA. De la misma manera que en SNA también es necesario dejar en claro que la tecnología de WAN utilizada sobre el backbone TCP/IP es HDLC.

En el inciso anterior hicimos mención que el IMSS cuenta con una gran cantidad de sistemas sustantivos propios, mismos que siguen evolucionando, desarrollándose y se ponen a disposición en la red para las diferentes áreas operativas que se involucren o trabajen con alguno de estos; pues bien hemos de citar que estos sistemas interactúan con los usuarios de la red con su adecuada emulación 3270 en el esquema TCP/IP, esto justifica la presencia del backbone TCP. La grafica (3.4b) nos muestra el esquema de conectividad del Backbone TCP/IP de la RITEL IMSS.



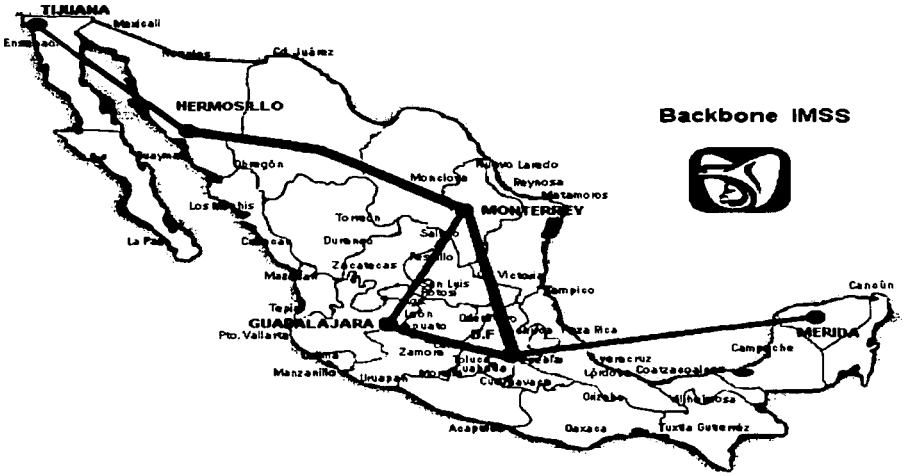
Tipos de Sitios:				
Site Nodo Concentrador Backbone TCP / IP Backbone SNA Delegación Subdelegación Metropolitana Subdelegación Foránea	Almacen Delegacional Almacen Regional Almacen Nacional Edificio Normativo Dirección Regional Centro de Capacitación Departamento de Informática	UMF HGZ HGR HGS HGO HGP HGZ/MF HGR/MF	HGS/MF HGO/MF H. Infectologia H. Psiquiatrico H. Ortopedia H. Traumatologia H. Especialidades H. Especialidades / G. O. Cen. de Inv. Biomedicas / CMN H. Consulta Externa / CMN	H. Especialidades / CMN H. Traumatologia / CMN H. Pediatria / CMN H. General / CMN HGO / CMN CMN Centro Regional de Suministros Cen. de Inv. Biomedicas Subalmacen Delegacional

Figura (3.4b)

No podemos dejar de mencionar que en el esquema TCP/IP están implementados los accesos desde otras instituciones con enlaces dedicados hacia el IMSS como son: CONSAR, BANXICO, SRIA DE GOBERNACION, CONACYT, así como los enlaces de los proveedores de los servicios de Internet, servidores de Abasto para proveedores de los insumos Institucionales, servidores WEB de IMSS, etc.

Por otra parte el mapa del grafico (3.4c) nos indica en la delta formada entre las ciudades de México, Monterrey y Guadalajara del backbone TCP/IP que enlaza los tres CIZ's de la Republica Mexicana mientras que la línea marcada en negro se visualiza la conectividad de todo el país con los enlaces principales o más robustos.

Figura (3.4c) Backbone TCP/IP IMSS a nivel Nacional.



BREVE DESCRIPCIÓN DE LA RED DE VOZ

Como mencionamos al plantear el backbone SNA, hoy en día los servicios de datos y voz a pesar de que operan y fluyen por la misma infraestructura no están integrados en la misma red; es decir no son parte de la misma RITEL. Los servicios de voz forman parte de una red superpuesta que opera sobre la infraestructura de comunicaciones que utiliza el proveedor TELMEX (Carrier) y equipamiento del mismo Instituto. De esto podemos citar un ejemplo para visualizar su modo de operación. En la grafica (3.4d) se muestra la manera en la que están conectados los dispositivos de la red de voz y datos en algunos sitios; es decir que aunque forman parte de la misma infraestructura de telecomunicaciones ello no quiere decir que sean parte de la misma RITEL ya que la red de voz es una red superpuesta sobre la WAN de la RITEL y el esquema nos muestra como la manera en que conviven ambas. Cabe señalar que en algunos sitios de la red WAN este es el esquema de comunicaciones que existe sobre todos en algunas Delegaciones del país, esto nos detalla la jerarquía que existe entre los distintos nodos en datos que hay en la red y a su vez nos muestra la función que desempeñan los equipos de multiplexaje (TMS y OCM del proveedor) con las comunicaciones de voz y datos.

Por desgracia en lo que concierne al esquema de numeración de la red de voz no lo hemos incluido debido a que este es demasiado extenso y solo daremos cuenta del número aproximado de nodos asignados en la red de voz y que aproximadamente el universo de estos es del orden de 834 los sitios con red de voz fueron asignados según las necesidades de la Institución y están asignados de la siguiente manera.

REGIÓN	NÚMERO DE NODOS ASIGNADOS EN LARED DE VOZ
AGUAS CALIENTES	11
COLIMA	12
GUERRERO	17
NAYARIT	10
QUINTANA ROO	12
TAMAULIPAS	18
ZACATECAS	9
BCN	13
LOMAS VERDES	26
CHIAPAS	10
HIDALGO	13
TIJUANA BCN	7
OAXACA	15
NUEVO LEON	32
SAN LUIS POTOSI	12
CHIHUAHUA	24
EDO. MEXICO	10
SINALOA	21
VERACRUZ NTE	20
DELEGACION 2 D.F.	14
CAMPECHE	8
DELEGACION 3 D.F.	17
CANTRO MEDICO LA RAZA	22
DURANGO	7
TLAXCALA	7
MICHOACAN	19
PUEBLA	17
SONORA	23
VERACRUZ SUR	14
C.M.N. SIGLO XXI	18
COAHUILA	25
DELAGACION 1 D.F.	17

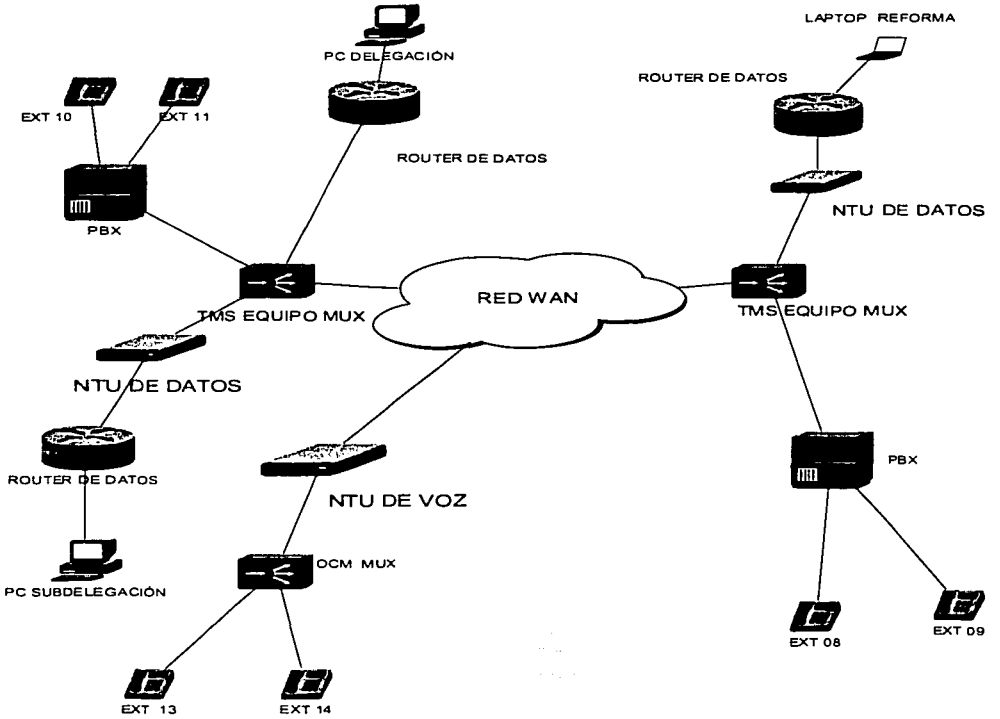
MORELOS	11
BCS	12
GUANAJUATO	27
QUERETARO	14
TABASCO	8
YUCATAN	16
DELEGACION 4 D.F.	16
JALISCO	43
NIVEL CENTAL Y OTROS	184

Como nota adicional cabe mencionar y dejar en correcta apreciación que el hecho de contar con una red de voz que solo cuenta con un limitado número de nodos asignados para las tareas primordiales y estratégicas de la institución a niveles directivos, ello no quiere decir que el IMSS no cuente con los servicios de telefonía y la infraestructura convencional para operar en la mayoría de los diferentes tipo de unidades, sitios e instalaciones ya que se cuenta con una gran variedad de equipos PBX en distintas capacidades y marcas. De lo anterior se desprende que los costos y gastos de estos enlaces dedicados son sufragados por la administración de cada unidad en donde se cuente y opere el servicio telefónico; sumando un aproximado de 38736 extensiones a nivel nacional. Los equipos PBX con que cuenta la institución se encuentran modelos de las siguientes marcas:

MARCA del PBX	MARCA del PBX
Alcatel	**Miditel**
Bosh	**Mytel**
Conmutel	**Nec**
Datacom Station	**Nitzuko**
Ericsson	**Nortel**
Fujitzu	**Panasonic**
GTE	**Samsung**
Hydel	**Siemens**
Indetel	**Standard**
Lucent	**Tadiran**
Macrotel	**Tenovis**

Figura (3.4d)

ESQUEMA DE LA RED SUPERPUESTA DE VOZ
SOBRE LA MISMA INFRAESTRUCTURA DE LA RED WAN



3.5 DIRECCIONAMIENTO

PROCEDIMIENTO PARA LA ASIGNACION DE DIRECCIONES IP

Con el objetivo de Normar y estandarizar el uso de las Direcciones IP (Direcciones Electrónicas) de cada uno de los dispositivos que componen la Red Integral de Telecomunicaciones (RITEL) del IMSS, así como la implantación de la Red Integral de Telecomunicaciones a Nivel Nacional para comunicar a la Unidades médico - Administrativas del Instituto, se libero el servicio interactivo para la operación de las diferentes aplicaciones del IMSS, en las áreas usuarias, lo cual hizo necesario Normar la "conexión lógica" de cada uno de los dispositivos que la componen de acuerdo a una arquitectura TCP / IP.

Para la "conexión lógica" de los dispositivos, será necesario que cada uno de ellos, tenga una Dirección IP como a continuación se describe:

11	**.**	**X2**	**.**	**X3**	**.**	**X4**	
1° Octeto		*2° Octeto*		*3° Octeto*		*4 ° Octeto*	

Donde: *1° Octeto* *El primer Octeto siempre será 11*
2° Octeto *El segundo y tercer octeto, indican Subdelegaciones, CMN., Hospitales,*
3° Octeto *Clínicas, etc. y la Delegación de la que dependen, respectivamente.*
4° Octeto *El cuarto octeto, identificara cada uno de los dispositivos que se integran a la RED.*

Dentro de la plataforma TCP / IP, la Red Integral de Telecomunicaciones del IMSS, esta clasificada como una Red Clase A **11 . 0 . 0 . 0** , con una Subnetmask tipo C **255 . 255 . 255 . 0** .

La siguiente tabla de la pagina siguiente describe un ejemplo claro de cómo se asigno el direccionamiento en los nodos delegacionales de todo el país, así como el tipo de enlace y el ancho de banda asignado para cada Delegación.

RELACIÓN DE DIRECCIONES IP DE LAS DELEGACIONES DE INFORMÁTICA DEL IMSS EN TODO EL PAÍS

DELEGACIÓN	DIRECCIÓN IP	IDENTIFICADORES	TIPO DE ENLACE
AGUASCALIENTES	11.1.1.254	D02-9910-0003	E0
BCN	11.1.2.254	D02-0002-0001	E0
BCS	11.1.3.254	D02-0105-0018	E0
CAMPECHE	11.1.4.254	D02-9910-0006	E0
COAHUILA	11.1.5.254	DPI-18487	E0
COLIMA	11.1.6.254	D02-9910-0008	E0
CHIAPAS	11.1.7.254	D02-9910-0035	E0
CHIHUAHUA	11.1.8.254	D02-0001-0021	E0
DURANGO	11.1.10.254	D02-9910-0011	E0
EDO. MEX	11.1.11.254	D02-9910-0012	E0
GUANAJUATO	11.1.11.254	D02-9910-0013	E0
GUERRERO	11.1.12.254	D02-9910-0036	E0
HIDALGO	11.1.13.254	D02-9910-0015	E0
JALISCO	11.1.14.254	D02-9910-0016	E0
LOMAS VERDES-REFORMA	11.1.15.254	L2D-0003-0030	E0
LOMAS VERDES-MULTIPUNTO	11.1.15.254	E1-9703-0025	E0
LOMAS VERDES-MULTIPUNTO	11.1.15.254	E1-9703-0026	E0
LOMAS VERDES-MULTIPUNTO	11.1.15.254	E1-9703-0027	E0
MICHOACAN	11.1.17.254	D02-9910-0017	E0
MORELOS	11.1.18.254	D02-9910-0037	E0
NAYARIT	11.1.19.254	D02-9910-0019	E0
NUEVO LEONN	11.1.20.254	D02-9910-0020	E0
OAXACA	11.1.21.254	D02-9910-0021	E0
PUEBLA	11.1.22.254	D02-9910-0022	E0
QUERETARO	11.1.23.254	D02-9910-0038	E0
QUINTANA ROO	11.1.24.254	D02-9910-0024	E0
SAN LUIS POTOSI	11.1.25.254	D02-9910-0025	E0
SINALOA	11.1.26.254	D02-9910-0026	E0
SONORA	11.1.27.254	D02-9910-0027	E0
TABASCO	11.1.28.254	D02-9910-0028	E0
TAMAULIPAS	11.1.29.254	D02-9910-0029	E0
TLAXCALA	11.1.30.254	D02-9910-0030	E0
VERACRUZ NORTE	11.1.31.254	D02-9910-0031	E0
VERACRUZ SUR	11.1.32.254	D02-9910-0032	E0
YUCATAN	11.1.33.254	D02-9910-0033	E0
ZACATECAS	11.1.34.254	D02-9910-0034	E0
DELEGACIÓN # 1	11.1.35.254	D02-9910-0009	E0
DELEGACIÓN # 2	11.1.36.254	D02-9910-0014	E0
DELEGACIÓN # 3	11.1.37.254	D02-9910-0018	E0
DELEGACIÓN # 4	11.1.38.254	D02-0012-0032	E0
BACKBONE TCP/IP MTY-GDL	10.98.1.253	D12-0001-0010	12 E0
BACKBONE TCP/IP MEX-GDL	10.99.1.253	D12-9910-0006	12 E0
BACKBONE TCP/IP MTY-MEX	10.97.1.253	D12-0001-0009	12 E0
BACKBONE SNA MTY-GDL		DPI-19111	4 E0
BACKBONE SNA MEX-GDL		DPI-19107 o IMS0067	4 E0
BACKBONE SNA MEX-MTY		DPI-19109 o IMS0054	4 E0

3.6 EL PROBLEMA DE SATURACIÓN DE LA RITEL

Originalmente como ya se había expuesto anteriormente la RITEL cuenta con 795 nodos WAN a nivel nacional (bajo contrato con TELMEX), hoy en día consta de aproximadamente de 800 (los costos de sitios adicionales son sufragados por las distintas entidades del IMSS, aunque operativamente se hallan incorporado a la RITEL). Estos sitios se han incrementado debido a que las necesidades de la Institución han ido creciendo paulatinamente en muchos sentidos, como el aumento del número de nodos WAN, equipo nuevo de computo en la gran mayoría de las redes LAN, equipos de comunicaciones, y el creciente numero de usuarios, así como nuevos sistemas en la RITEL, etc.

En siguiente grafico (3.6a) se muestra el estándar de la conectividad de la mayoría de los sitios LAN que integran la RITEL, este esquema muestra lo que se refiere a la parte de datos. También se puede observar que el incremento de equipamiento sobre los sitios LAN institucionales tienen un gran impacto sobre la red WAN.

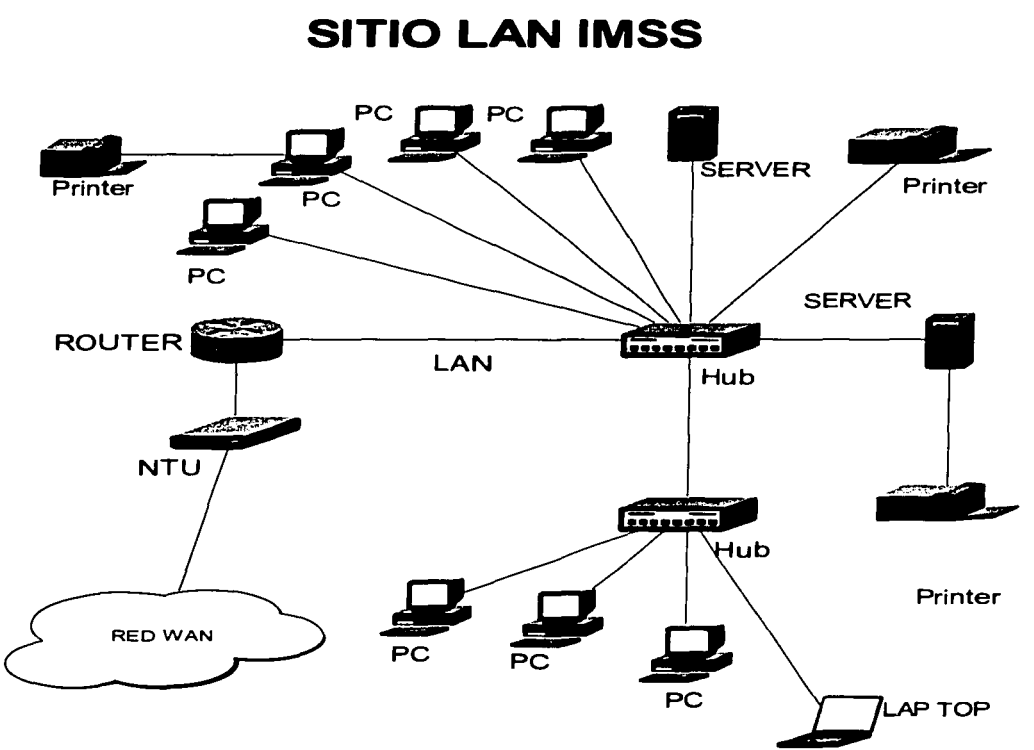


Figura (3.6a)

En sus inicios la RITEL contaba con un cierto número de equipos que operaban en la red, con el transcurso de los años fueron creciendo el número de usuarios sobre el direccionamiento IP asignado, se han ido liberando las nuevas versiones del software de los sistemas sustantivos existentes, así como también se han incrementado nuevas aplicaciones y sistemas que se han incorporado sobre la RITEL y en el ultimo par de años el crecimiento agigantado de los usuarios con acceso a los servicios de Internet y correo electrónico.

Todo lo anterior fue un detonante en la saturación y sobrecarga de los anchos de banda sobre los diferentes enlaces de la RITEL, mismos que por desgracia no fueron incrementados y a la fecha continúan operando con las mismas características (ancho de banda contratado para cada sitio de la WAN) con que iniciaron su operación en 1996. De este hecho se desprende lo siguiente, una vez que hemos descritos la tecnología y la manera de operación de la RITEL, ahora nos abocaremos a citar los problemas actuales que presenta la misma, cabe aclarar que si bien no son todos, si son los que más impacto han tenido y repercutido en su operación. En este momento entre los parámetros que se miden y que más impacto causan en la RITEL se encuentran:

- % de utilización de ancho de banda.
- % de paquetes perdidos.
- tiempo de latencia.
- Topología de red jerarquizada, que tiene por consecuencia dependencia de las comunicaciones.
- Tiempos muy altos para cambios o escalamientos de sitios.
- Tecnologías de comunicaciones que en estos momentos empiezan a ser obsoletas: TDM, HDLC y Frame Relay.
- En algunos sitios se tienen enlaces de voz y datos saturados.
- En algunos sitios se tienen enlaces de voz y datos occisos.
- Redes de voz y datos superpuestas (IP y SNA).
- Equipos Institucionales de comunicaciones en algunos casos obsoletos.
- No se tiene soporte para tráfico multimedia de las nuevas y futuras aplicaciones institucionales.
- Poca flexibilidad
- Poca escalabilidad ante las crecientes necesidades de la institución.
- Una red privada, implica altos costos de construcción, administración y mantenimiento. Hoy en día se paga una renta mensual aproximada a los 10 millones de pesos; es decir 120 millones de pesos anuales.
- Baja capacidad de cobertura (795 nodos actuales contratados), lo cual indica que no se atiende ni al 30% de la infraestructura institucional.
- El número de fallas diarias detectadas por el monitoreo en la red WAN es del orden de 12 a 15 aproximadamente a nivel nacional.
- Una gran cantidad de nodos y equipos de voz están fuera sin funcionar por diversas fallas.
- Los conmutadores y equipos de telefonía de la institución son de distintas marcas y proveedores.

Todo lo anterior nos la pauta y nos permite proponer la imperiosa necesidad de proponer y justificar un nuevo esquema de operación sobre la red WAN de la RITEL institucional, hecho que será descrito en el siguiente capitulo de este trabajo.

PROPUESTA

RECAPITULACIÓN

En los capítulos anteriores hemos descrito y sentado las bases, características, de una red de telecomunicaciones que hoy en día opera con grandes problemas y dificultades. A partir del análisis anterior y la problemática antes descrita, hemos entrado en una fase de planeación para darle seguimiento y desarrollo a un nuevo proyecto que tenga la viabilidad de poder migrar a una solución que sea capaz de absorber la gran cantidad de problemas acumulados y que sea sustentable tanto en costos como en las necesidades de crecimiento que el IMSS tendrá en el corto y mediano plazo con todas las variables que ello implique, para ello el área de telecomunicaciones de la misma institución se ha dado a la tarea de desarrollar el nuevo proyecto tecnológico que sustituirá el esquema de comunicaciones de la RITEL. Solución que será planteada en este capítulo 4 de este trabajo de tesis, misma que a su vez pretende justificar el hecho de haber sido aceptada como una solución tecnológica que presento la mejor opción y que cumple con los requerimientos que el IMSS solicita hoy en día para seguir operando y evolucionando en todos los aspectos legales y laborales que le confieren. Ahora bien para plantear los requerimientos técnicos de la VPN-IMSS de inicio nos abocaremos a los requisitos solicitados por el IMSS de acuerdo con su licitación publica nacional para servicios de VPN (00641149-037-02) de diciembre del 2002. Así como también hacemos mención que el planteamiento de dicha licitación cumple con lo estipulado en la ley de adquisiciones arrendamiento y servicios del sector publico.

4.1 REQUERIMIENTOS EN EL CORE (parte medular de la red) VPN-IMSS

UNIVERSO DE SITIOS COSIDERADOS EN LA VPN IMSS

Puesto que han aumentado los sitios y requerimientos para la RITEL es claro que se hace necesario contar con el universo total de sitios a considerar en el nuevo proyecto de modernización de la RITEL todo esto con el objeto de tener los primeros elementos a considerar sobre la estructura de la VPN. En la tabla se detallan la cantidad de sitios que serán incluidos en la VPN IMSS.

TIPO DE UNIDAD	Nº DE NODOS
ALMACENES	38
BANCOS DE SANGRE	3
CENTROS DE INVESTIGACIÓN BIOMEDICA	5
CENTROS DE INVESTIGACIÓN EDUCATIVA Y FORMACION DOCENTE	7
CIZ MEX, MTY y GDL, INTERNET MEX Y MTY, ISDN	6
COORDINACIONES REGIONALES DE ABASTECIMIENTOS	3
CENTROS VACACIONALES	4
CENTROS DE CAPACITACIÓN	39
COORDINACIONES DELEGACIONALES DE INFORMÁTICA	7
COORDINACIONES NORMATIVAS CENTRALES	34
DELEGACIONES	37
DIRECCIONES REGIONALES	4
FARMACIAS	2
GUARDERIAS	1
HOSPITALES	243
OFICINAS AUXILIARES	734
DEPARTAMENTOS NORMATIVOS DELEGACIONALES	120
PLANTAS DE LAVADO	4
OFICINAS SINDICALES	32
SUBALMACENES	3
SUBDELEGACIONES	134
TIENDAS IMSS	146
UNIDADES DE MEDICINA FAMILIAR	1112
VELATORIOS	17
HOSPITALES REGIONALES DE SOLIDARIDAD (PROGRAMA IMSS SOLIDARIDAD)	69
CENTROS DE SEGURIDAD SOCIAL	8
UNIDADES MÉDICAS DE ALTA ESPECIALIDAD	24
CENTRO INTERAMERICANO DE ESTUDIOS DE SEGURIDAD SOCIAL (CIESS)	1
ESCUELA DE ENFERMERÍA	1
UNIDADES DE MEDICINA RURAL (PROGRAMA IMSS SOLIDARIDAD)	78
GRUPOS MULTIDISIPLINARIOS (PROGRAMA IMSS SOLIDARIDAD)	3
ENLACES PRIVADOS PUNTO A PUNTO	2
DELEGACIONES IMSS SILIDARIDAD (PROGRAMA IMSS SOLIDARIDAD)	9
UNIVERSO TOTAL	2930

CORE (parte medular de la red) DE LA VPN

Una vez que hemos descrito el nuevo universo de sitios a considerar en la VPN IMSS y conociendo que el proveedor TELMEX-UNINET será el responsable de cubrir la infraestructura necesaria de telecomunicaciones en

el **core**, pasaremos al hecho de plantear los requerimientos tecnológicos propuestos y necesarios para llevar a cabo el proyecto de modernización de la RITEL como la VPN IMSS. Es por ello que aquí presentamos los lineamientos técnicos establecidos por el instituto, para la instalación, activación, operación y administración de la VPN IMSS para la transmisión de voz, datos, vídeo y servicios de valor agregado asociados para interconectar los inmuebles del IMSS. Así mismo se entenderá como servicios de valor agregado; el monitoreo y administración de la red, atención a fallas a través de una mesa de ayuda, soporte técnico y el acceso a Internet, entre otros que incluya el proveedor en su oferta.

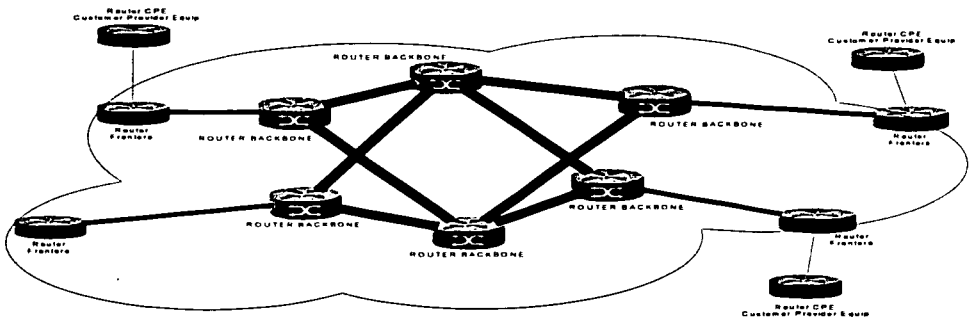
EL CORE (parte medular de la red)

Las grandes redes requieren de dispositivos poderosos de enrutamiento capaces de entregar datos rápidos y ser muy eficientes, sin importar el protocolo, la topología de la red u otros factores. Desde que las aplicaciones en red son de funcionamiento crítico, el tiempo fuera de servicio de las redes debe ser cero. Para esto los usuarios o clientes requieren routers que proporcionen la mayor cantidad de interfaces de WAN y que puedan producir la más alta capacidad de procesamiento a partir del costoso ancho de banda de la WAN, y a medida que más aplicaciones utilicen las funciones "multicast" y Calidad de Servicio "Quality of Service" (QoS), los usuarios o clientes querrán también esa inversión continúe funcionando sin problemas aun cuando aumenten sus necesidades y requerimientos.

El **core** es particularmente la parte medular de comunicaciones en redes grandes; y contiene la infraestructura de comunicaciones mas robusta y compleja de toda la red, por lo tanto derivado del análisis hecho en cuanto a tecnologías de redes telemáticas explicadas en el capitulo 2 de este trabajo podemos citar y justificar el hecho del por que se escogieron las tecnologías como SONET/SDH y MPLS como transporte para implementar la VPN IMSS. Ahora bien entrando en tema, para este caso el **core** propuesto para la VPN IMSS estará formado por una gama de equipos y dispositivos, poderosos como se menciono en el párrafo anterior y con capacidades enormes de operación y funcionalidad que provee las diferentes funciones exigidas por la red.

Para el proyecto de la VPN IMSS el **core** será formado por switches WAN IGX (de alta velocidad) de la familia Cisco 12000 y routers de capacidades altas de las familias 7500. Estos switches forman dos infraestructuras de comunicaciones que conforman la red frontera y el backbone, de tal manera que los routers de las familias 7500 forman la red frontera y los switches Gigabit switch de la familia 12000 forman el backbone, de esto damos referencia en la figura (4.1a).

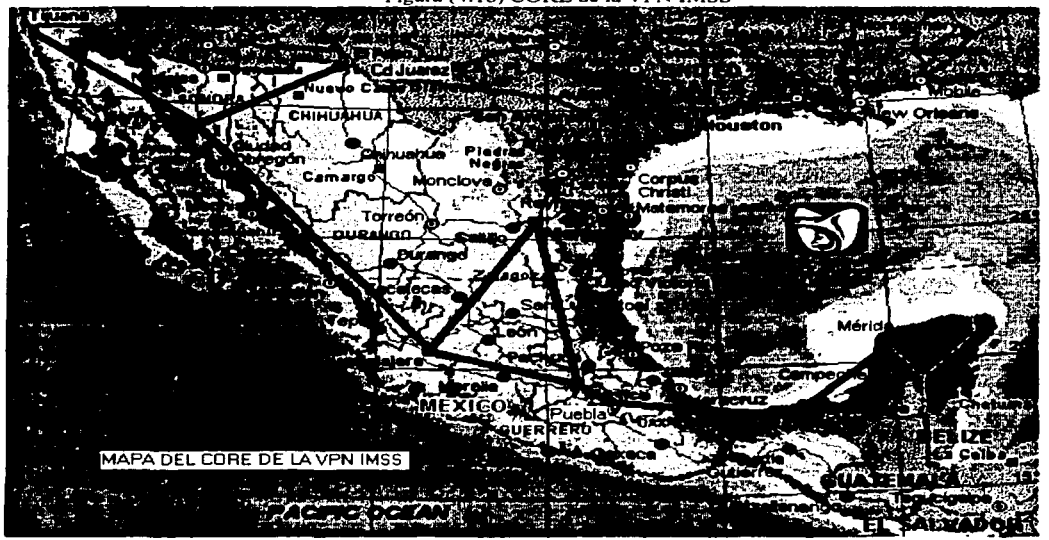
Figura (4.1a)
ESTRUCTURA DEL CORE PARA LA VPN



Por datos aportados por el proveedor se sabe que cuenta enlaces STM-1 (155 Mbps) con los que se le dará salida hacia el **core** de internet en los nodos CENATI's (Centro Nacional de Tecnologías de la Información) México y Monterrey antes CIZ1 México y CIZ2 Monterrey del IMSS.

Con respecto a la cobertura podemos citar que se cuenta con redundancia total en el **core** con 9 POP (Puntos de Presencia) a nivel nacional y diseminados en las siguientes ciudades del país, como se muestra en el esquema de la figura (4.1b).

Figura (4.1b) CORE de la VPN IMSS



Esta red publica mexicana de banda ancha de valor agregado y con capacidad de soportar aplicaciones de voz, datos y vídeo, incorpora una de las tecnologías de transporte mas avanzadas con mas de 56,000 Km de fibra óptica SDH en el ámbito nacional. Es obvio que con esta tecnología se rescata la gran mayoría de los equipos de comunicaciones con los que cuenta la institución, y de esto obtenemos las siguientes ventajas:

- Se utilizara la infraestructura en equipos de telecomunicaciones (Switches, PBX, Hubs, teléfonos, PCs, etc.) ya existentes e instalados en la mayoría de los inmuebles de la institución.
- Se tendrá ahorro y menores costos de inversión hacia la infraestructura y equipamiento que soporta voz, datos, video y servicios agregados.
- Habrá un ahorro sustancial de recursos económicos al usarse SONET/SDH como plataforma de transporte por el carrier, y se contara con tecnología de punta en toda la VPN.
- Se mantendrá la Conectividad IP con la arquitectura de MPLS.
- El protocolo de transporte SONET/SDH es una plataforma ideal para una multitud de servicios y es compatible con MPLS.
- Se tendrá un esquema de comunicación "any to any" (todos contra todos) entre los puntos finales del Instituto.
- Se proporcionan tres tipos de calidad de servicio en la VPN:
  - Calidad 1 para servicio de datos.
  - Calidad 2 para servicio de datos SNA.

- Calidad 3 para servicios de voz y video.

- Para aquellos equipos que no estén trabajando en plataforma IP actualmente, podría ser encapsulada la información en IP para que fluya adecuadamente en la VPN hacia su destino.
- Se reducen tiempos de respuesta.
- Se aumenta redundancia por parte del proveedor.
- Se reducen costos en soporte y costos por renta de lineas privadas.
- Aumentan la disponibilidad de ancho de banda en cada unos de los sitios de la VPN.

4.2 REQUERIMIENTOS EN EL CLIENTE VPN-IMSS

PROTOCOLO

Para la VPN todos los protocolos que operen serán implementados al Instalarse la infraestructura de conectividad para la emisión y recepción de paquetes con información encapsulada en protocolos de comunicación de red, y estarán apegados a lo dispuesto por los estándares G.728, G.729, QSig, 802.1p, 802.1Q, H.323 (mismos que se detallan en el Apéndice A de este trabajo) para los servicios de voz, datos y video, en adelante denominados "paquetes", en todos los nodos. Ahora por lo que respecta protocolos de transporte en la VPN se tiene que deberán operar los siguientes:

- PPP Point-to-Point Protocol. Sucesor de SLIP, PPP proporciona conexiones "router"-a-"router" y host-a-red sobre circuitos tanto síncronos como asíncronos.

- Transporte de información con tecnología MPLS encapsulando en IP sobre la Red Privada Virtual, con los niveles de servicios requeridos, por lo que el carrier proveerá los servicios requeridos de transporte de paquetes, a través de la VPN, sobre MultiProtocol Label Switching (MPLS descrito en el capitulo 2), debiendo cumplir con lo siguiente:

  - Instalación de la infraestructura de red privada virtual, para los servicios del proyecto, bajo protocolo IP.
  - Instalación, supervisión y puesta en operación de equipos para la red de voz, datos y video.
  - Operar en una plataforma IP/MPLS, dentro de la red dorsal del proveedor.
  - La red debe ser capaz de proporcionar todas las ventajas de la tecnología MPLS.
  - Comunicación "any to any" (todos contra todos) entre los puntos finales del Instituto.
  - El proveedor será responsable de la transmisión de los paquetes que se envíen y reciban por las aplicaciones que opera el Instituto. En dicha transmisión deberá aplicar las prioridades de calidad de servicio (Quality of Service, QoS), hasta el último puerto de comunicaciones provisto con esta facilidad y que forme parte de la solución de red propuesta para atender las necesidades del Instituto ("end – to – end").
  - Cumplir con las funcionalidades requeridas para el servicio de voz, descritas.

Nota: Ya hemos mencionado anteriormente que MPLS asigna etiquetas cortas de longitud fija por lo que una vez más recalcamos que también que dichas etiquetas sumarizan toda la información esencial acerca del enrutamiento de los paquetes como son:

- Destino.
- Precedencia
- Membresía de una VPN
- Calidad de servicio (QoS).
- La ruta para el paquete, escogida por ingeniería de tráfico.

MEDIOS DE COMUNICACIÓN

CONSIDERACIONES GENERALES DE CABLEADO

Enlaces para la interconexión de las Redes de Área Local

Los enlaces considerados son de los siguientes tipos principales:

- Enlace con cable UTP, Fast Ethernet, a 100 mbps: Entre el switch de distribución principal, y el equipo propuesto por el licitante de acceso a WAN en el caso de los campus.
- Enlace con cable UTP, Fast Ethernet, a 100 mbps: Entre el equipo propuesto por el licitante de acceso a WAN y el switch de distribución principal solicitado o primer Concentrador en el caso de los edificios independientes.
- Enlace con fibra óptica multimodo para distancias menores a 250 mts. Del tipo interior o exterior donde aplique, con tecnología Gigabit Ethernet a 1000 mbps. Entre los switches de distribución y los de distribución principal, cuando se trata del cableado de un campus.
- Enlace con fibra óptica monomodo para distancias mayores a 250 mts. Del tipo exterior donde aplique, con tecnología Gigabit Ethernet a 1000 mbps. Entre los switches de distribución y los de distribución principal, cuando se trata del cableado de un campus.

Cableado de campus

Se establecen los elementos funcionales de un cableado estructurado genérico, para formar redes de campus de acuerdo con lo solicitado por el Instituto, dichos elementos son:

- Cableado desde el distribuidor de campus (DCC): Este cableado conecta a todos los edificios incluidos en Campus, inicia donde se encuentra el equipo propuesto por el licitante de acceso a WAN y se conecta a cada uno de los switches de distribución principal de los inmuebles involucrados en el campus.

- Cableado de distribución de edificio (DCE): Este cableado distribuye internamente al edificio a los distribuidores de piso (DCP).

Este cableado se extiende desde el distribuidor de cables de *Campus* hasta los distribuidores de cables de edificio, e incluye lo siguiente: cables principales del *campus*, terminación mecánica de estos cables en ambos extremos (DCC y DCEs) y las conexiones de cruce e interconexiones en el distribuidor de cables de *campus*. El cable principal de *campus* también puede ser utilizado para interconectar distribuidores de cables de Edificio.

Distribuidor de cables de Campus

Distribuidor principal de un *campus*, en el que termina un extremo de los cables que interconectan los edificios del *campus*, que se emplea para efectuar conexiones con otros subsistemas de cableado y equipos de telecomunicaciones.

Terminación de cables

En el distribuidor de cables de campus, los cables de servicios de datos deben terminarse de la siguiente manera:

- Para proporcionar los servicios de datos, los equipos de comunicación correspondientes deben interconectarse con los paneles de parcheo donde se terminaron los cables de fibras ópticas que transportan los servicios de datos hacia los otros edificios del *campus*.

- Los accesorios de conexión para los distribuidores de cables de *campus*, para servicios de datos, deben ser paneles de parcheo ópticos, para montaje en herraje universal de 19 pulgadas, con charola integrada para el acomodo correcto del cable de fibra óptica, preferentemente con adaptadores 568 SC, o adaptadores que cumplan con las especificaciones indicadas en la Norma ANSI/EIA/TIA-568B.3, o equivalente.

Topología del cableado

El cableado estructurado genérico de un edificio o *campus* debe tener una estructura en estrella jerárquica, donde la cantidad y tipo de subsistemas de cableado que están incluidos en un diseño, depende de la geografía y

tamaño de éstos, así como de los requerimientos propios del usuario. La topología de un cableado genérico debe tomar la forma mostrada a continuación en la Figura (4.2a).

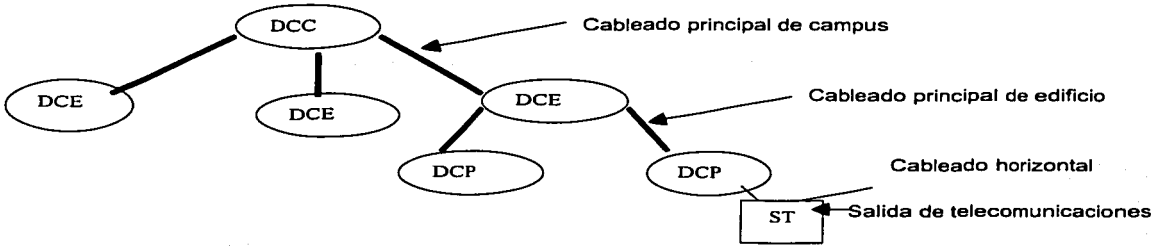


Figura (4.2a)

Los cables se deben instalar entre los niveles jerárquicos adyacentes de la topología de un cableado genérico, tal como se muestra en la figura.

Cables permitidos

Los tipos de cables para uso en campus son:
Esta sección especifica cinco tipos de cables para uso en el subsistema de cableado de campus:

- Cable de par trenzado sin blindaje (UTP), de cuatro pares de 100 ohms, con conductores calibre 24 AWG, categoría 5 mejorada (categoría 5E).
- Cable de par trenzado con pantalla (FTP), de cuatro pares de 100 ohms, con conductores calibre 24 AWG, categoría 5 mejorada (categoría 5E).
- Cable de fibra óptica, de 62.5/125 nm.
- Cable de fibra óptica, de 50/125 nm.
- Cable de fibra óptica monomodo 8-10/125 nm

Los cables de cobre permitidos dentro de un edificio deben estar aprobados y listados como resistentes al fuego y a la propagación de flama de acuerdo a lo indicado en los artículos 800-49, 800-50 y 800-51 de la Norma Oficial Mexicana NOM-001-SEDE-1999. Estos cables se deben instalar de acuerdo a lo indicado en el artículo 800-53 de la Norma Oficial Mexicana NOM-001-SEDE-1999. También se hace la aclaración que no se incluye cable categoría 6 por las siguientes razones:

- Su uso no esta todavía muy extendido.
- Hoy en día no esta estandarizado de manera universal.
- Esta en fase de experimentación.
- Es una categoría que acaba de salir.

También se permite instalar cables con cubierta con propiedades de bajo humo, cero halógenos y retardante a la flama, de acuerdo al estándar IEC 332-1, o equivalente, en cámaras de aire, cableado principal de edificio u otros espacios usados para manejar aire acondicionado.

Los cables de fibra óptica permitidos dentro de un edificio deben estar aprobados y listados como resistentes al fuego de acuerdo a lo indicado en los artículos 770-49, 770-50 y 770-51 de la Norma oficial Mexicana NOM-001-SEDE-1999.

Estos cables se deben instalar de acuerdo a lo indicado en el artículo 770-53 de la Norma Oficial Mexicana NOM-001-SEDE-1999. También se permite instalar cable con cubierta con propiedades de bajo humo, cero

halógenos y retardante a la flama, de acuerdo al estándar IEC 332-1, o equivalente, en cámaras de aire, cableado principal de edificio u otros espacios usados para manejar aire acondicionado.

Código de colores

- El código de colores para un cable de cobre 4 pares, deberá ser de acuerdo con la Norma para Cableados de Telecomunicaciones en Edificios Comerciales, ANSI/EIA/TIA –568 B.1, B.2- Mayo, 2001.
- El código de colores para un cable de fibra óptica hasta 12 hilos, Norma para Cableados de Telecomunicaciones en Edificios Comerciales, ANSI/EIA/TIA –568 B.1 y B.3.- Mayo, 2001.

Cuando se instalen cables de cobre o fibra óptica en canalizaciones subterráneas, estos deben tener protección adicional contra:

- Roedores
- Humedad y agua
- Radiación ultravioleta
- Tensión de instalación.

QoS

QoS (Quality of Service Calidad de Servicio), como se sabe es una medida de rendimiento para un sistema de transmisión que refleja la calidad de su transmisión y disponibilidad de servicio. QoS es un ingrediente esencial de una red IP VPN dado que provee la habilidad de direccionar dos requerimientos fundamentales en las VPNs:

- Rendimiento predecible y políticas de implantación
- Soporte a múltiples clases de servicios en una VPN sobre MPLS

Debido a que el trafico de la red esta clasificado y etiquetado en la frontera de la red, antes de que este sea enviado y transportado dentro del Backbone y basándose en las políticas definidas e implementadas por el carrier, tenemos que el trafico de la frontera y de la red principal puede ser diferenciado en diferentes clases por probabilidad de perdida de paquetes y retrasos.

De lo anterior se desprende que con el propósito de integrar a las diferentes entidades u oficinas y cubrir las demandas de los servicios de voz, datos y video, se sugiere considerar diferentes opciones de calidad de servicio (QoS) de acuerdo a las necesidades de cada dependencia; mismas que nos ofrecen la oportunidad de priorizar la transmisión por el tipo de aplicación, que dando de la siguiente manera:

- Nivel 1- Datos
- Nivel 2- SNA
- Nivel 3- Multiservicios (voz y video)

Ancho de banda

Para todos los nodos los enlaces estarán conectados a través de enlaces privados, ahora bien para las ciudades que conforman el Backbone se consideran enlaces E3, en el siguiente nivel las conexiones pueden ser desde 5 E1´s canalizados o N x 64 de acuerdo a la densidad del sitio y su numero servicios contemplados en la estructura de la nueva red. El ancho de banda para los niveles remotos esta considerado para que soporte al menos dos canales de voz analógicos y el transporte de tráfico de datos con 64Kbps y 128Kbps.

Latencia

Llamamos latencia (lantency) al tiempo que tarda un paquete de datos en llegar desde su origen hasta su destino, y se conoce que la latencia no es constante en el tiempo, por lo que también hay que considerar su variación, concepto que se conoce con el nombre de jitter. En la siguiente tabla se documenta los requerimientos

solicitados por la institución en cuanto a los parámetros de latencia y disponibilidad. La latencia esta definida por la siguiente expresión:

Latencia total = Overhead Tx + Tiempo de vuelo +Tiempo de transmisión + Overhead Rx

- **Tiempo de vuelo**.- tiempo para que el primer bit del mensaje llegue al receptor y es del orden en milisegundos en una WAN.
- **Overhead Tx**.- es el tiempo para que el procesador inyecte el mensaje a la red.
- **Overhead Rx**.- es el tiempo para que el procesador recoja el mensaje de la red y normalmente este tiempo es mayor al anterior.
- **Tiempo de transmisión**.- es el tiempo para que el mensaje pase a través de la red. Este es igual al tamaño del mensaje/BW.

DISPONIBILIDAD, LATENCIA Y PAQUETES PERDIDOS EN LA VPN

Nodo	Criticidad	Disponibilidad (%)	Tiempo de tolerancia mensual de falla (minutos)	Tiempo de Latencia máximo permitido "Round Trip" IP NSP (milisegundos)	Paquetes máximo perdidos (%)
Internet Data Center (IDC) • México • Monterrey	1 1	99.96 99.96	17.28 17.28	100 100	0.1 0.1
Centro Médico Nacional • Siglo XXI • La Raza	2	99.85	64.80	100	0.2
Unidades Medicas de Alta Especialidad (UMAE)	3	99.65	151.20	150	0.4
Subdelegaciones	3	99.65	151.20	150	0.4
Áreas Normativas	3	99.65	151.20	150	0.4
Direcciones Regionales	4	99.60	172.80	150	0.5
Delegaciones	4	99.60	172.80	150	0.5
Coord. Delega. De Inform.	4	99.60	172.80		0.5
Almacén	4	99.60	172.80	150	0.5
Coordinaciones Regionales de Abasto (CRA)	4	99.60	172.80	150	0.5
Hospitales	4	99.60	172.80	150	0.5
UMF's (I)	4	99.60	172.80	150	0.5
Centros de Capacitación	5	99.50	216.00	200	0.8
Centro de Investigación Biomédica (CIBIO)	5	99.50	216.00	200	0.8
Centro de Investigación Educativa y Formación Docente (CIEFD)	5	99.50	216.00	200	0.8
Centros Vacacionales	5	99.50	216.00	200	0.8

Tiendas (I)	5	99.50	216.00	200	0.8
Oficinas Auxiliares	5	99.50	216.00	200	0.8
UMF's (II)	5	99.50	216.00	200	0.8
HRS	5	99.50	216.00	200	0.8
UMR	5	99.50	216.00	200	0.8
Tiendas(II)	6	99.40	259.20	200	1
Velatorios	6	99.40	259.20	200	1
Oficinas Varias	6	99.40	259.20	200	1
SNTSS	6	99.40	259.20	200	1
Grupos Multidisciplinarios	6	99.40	259.20	200	1

- El tiempo de latencia requerido será medido entre el nodo CENATI (México y/o Monterrey) y cualquier otro nodo de la VPN.

- El tiempo de latencia será medido desde el equipo que da acceso a la VPN, instalado en el instituto.

- Para los nodos con enlace satelital, se considerara una latencia mayor de acuerdo con la solución del proveedor; siempre y cuando se cumpla con los Niveles de Servicios (Disponibilidad y el % Máximo de paquetes pedidos) para cada uno de los servicios solicitados.

- Una solución para el acceso a Internet solicitada al proveedor contempla el hecho de contener dos accesos a Internet (www), interconectándolos a los Centro de Procesamiento de Datos CENATI (Centro Nacional de Tecnologías de la Información) del Instituto en México y Monterrey, con una latencia menor o igual a 100 milisegundos a plena carga de ida y vuelta (Round Trip), dicho tiempo será midiéndolo desde el router de los nodos de origen CENATI's del Instituto, al router de los Punto(s) de Acceso de Red (Network Access Point, NAP) de primer nivel en los Estados Unidos de América correspondiente, a través de pruebas de comunicación con protocolo ICMP (Interconnect Messaging Protocol), mediante enlaces por demanda con capacidad mínima de 8E1 cada uno, hasta un E3 a través de la infraestructura del proveedor. Siendo el mismo proveedor, el responsable de administrar y garantizar la duración de la calidad del servicio para el traslado de información en dicho enlace, cabe mencionar esto por que la cantidad de usuarios concurrentes, estimada por el instituto con acceso a Internet será de 40,000.

Confiabilidad

El proveedor deberá incluir en su propuesta técnica, los procedimientos y mecanismos utilizados para implementar la seguridad y confidencialidad de la información enviada por la red, de acuerdo a lo especificado por el IMSS y considerando lo siguiente:

1. Proteger la información emitida y recibida por el Instituto, por medio de una solución de seguridad que permita implantar los mecanismos de control de accesos a la red privada virtual propuesta.

2. Evitar, dentro de la VPN-IMSS (Red Privada Virtual del IMSS) propuesta, intercepciones o intrusiones a esta y/o a la información que curse entre los nodos que la componen.

3. Toda la infraestructura de comunicaciones deberá contar con claves de acceso a las comunidades de monitoreo establecidas entre el Instituto y el proveedor.

4. El proveedor deberá asegurar que la infraestructura tecnológica de seguridad ofertada no afecte los niveles de servicio establecidos para el funcionamiento de cada uno de los nodos que abarca el proyecto.

Por otra parte también se considera que como parte del nuevo esquema a implantarse el proveedor deberá considerar lo siguiente:

- Garantizar los niveles de servicios durante el proceso de migración hacia el nuevo proyecto VPN-IMSS.

- Garantizar absoluta transparencia en la migración y puesta a punto en la implantación de los diferentes nodos que se integren a la VPN-IMSS, considerando las diferentes topologías y soluciones existentes y/o propuestas en cada uno de los nodos del país.

- Considerar las facilidades técnicas necesarias que permitan la desconexión de sus servicios durante el proceso de migración hacia algún nuevo "proyecto" en el futuro.

Administración y monitoreo

Para administrar la solución y la seguridad en esta propuesta, adicionalmente el proveedor deberá proporcionar en las instalaciones del IMSS (en la ciudad de México) una consola de monitoreo, idéntica a la que se encuentre operando en su NOC (Network Operations Center), para la comprobación de las funcionalidades requeridas por el Instituto, de acuerdo a lo estipulado.

El proveedor deberá contar con un Centro de Operaciones de Red (NOC, Network Operations Center) en sus instalaciones y será el responsable de administrar y monitorear los sistemas de comunicación incluidos en su solución hasta el último puerto de acceso, que permitan al IMSS obtener un uso eficiente de los recursos en la VPN. Así mismo, se debe proporcionar la herramienta o conjunto de herramientas que permitan al IMSS supervisar y auditar los acuerdos de niveles de servicio, y deberán operar bajo un esquema basado en web con soporte para al menos 30 usuarios simultáneos.

Para el monitoreo de la Red Integral de Telecomunicaciones (Red Privada Virtual del IMSS) se deberá de contar con las siguientes facilidades:

1. Administrar y monitorear en forma remota al menos los siguientes componentes:
   - Medios de comunicación.
   - Dispositivos de comunicación y puertos respectivos.

2. Contar con los mecanismos de seguridad de información que limite el acceso de usuarios de las comunidades de monitoreo desde y hacia la red donde residirá el centro de operaciones.

3. Proveer al Instituto en tiempo real a través de un sistema basado en el protocolo http, las alarmas de los eventos existentes en la operación de la infraestructura de conectividad, que impacten el cumplimiento de los niveles de servicio establecidos.

4. Monitoreo Central, el proveedor, deberá establecer como prioritario dentro del sistema de administración y monitoreo, un esquema bajo arquitectura web, para observar funcionalidades de desempeño y disponibilidad, incluyendo una herramienta de generación de reportes para la toma de decisiones relacionadas con los Sistemas de Seguridad, Tráfico de red, Niveles de servicio y Disponibilidad de la red, etc.

5. El IMSS, llevará a cabo la supervisión directiva de los niveles de servicio de red solicitados, quedando a cargo del proveedor, la instalación, monitoreo proactivo y reactivo, administración operativa y mantenimiento; entendiéndose por esto, la responsabilidad permanente por parte del proveedor sobre la

continuidad, seguridad y calidad de los servicios de la red incluyendo la solución de fallas presentadas en los equipos asociados de comunicación, así como la reparación y corrección a los problemas en los enlaces contratados en cumplimiento con los niveles de servicio.

4.3 ESQUEMAS PROPUESTOS Y/O ESCENARIOS PROPUESTOS (VOZ, DATOS, VIDEO Y OTROS)

VOZ

Con el fin de lograr una comunicación más dinámica entre oficinas del IMSS, se propone conectar los conmutadores telefónicos entre si con enlaces E1 y E&M, la decisión del tipo de enlace que se utilizara en cada caso depende de las facilidades que se quieran mantener en un determinado punto de la red, esto se debe a que el mantener servicios como identificador de llamadas, despliegue de nombre y otros servicios en red requieren de equipar los conmutadores con enlaces E1 dedicados entre si, además de equipar los conmutadores con software avanzado.

El utilizar enlaces E&M (Estos enlaces analógicos se utilizan para conectar varias centrales entre si de manera que pueden enviarse llamadas de una a otra). Ello nos permitirá manejar un plan de numeración coordinado, pero se perderán facilidades como identificador de nombre y numero en las llamadas, manejo de operadora centralizada entre otras facilidades. Los enlaces E1 y E&M se conectaran de los conmutadores telefónicos a los equipos multiservicio que se instalen como infraestructura de la red WAN. La conmutación de las llamadas de voz en este tipo de solución es realizada por los switches de datos, con la ventaja de que disminuye el tráfico que llega a los conmutadores de voz, ya que la llamada se direcciona automáticamente hasta su destino final optimizando la utilización del ancho de banda y canales disponibles.

Otro punto importante que se debe tener en cuenta en el diseño de la red de voz es el considerar las marcas de los conmutadores telefónicos con que se cuenta en el instituto, esto debido a que para mantener la mayor cantidad de facilidades en la red además de requerir enlaces E1 dedicados, los equipos deberán ser del mismo fabricante, ya que al hacer mezclas de equipos de diferentes proveedores se pierden las facilidades (solo queda el numero de identificación de llamada, utilizando protocolos como Qsig o Euro-ISDN).

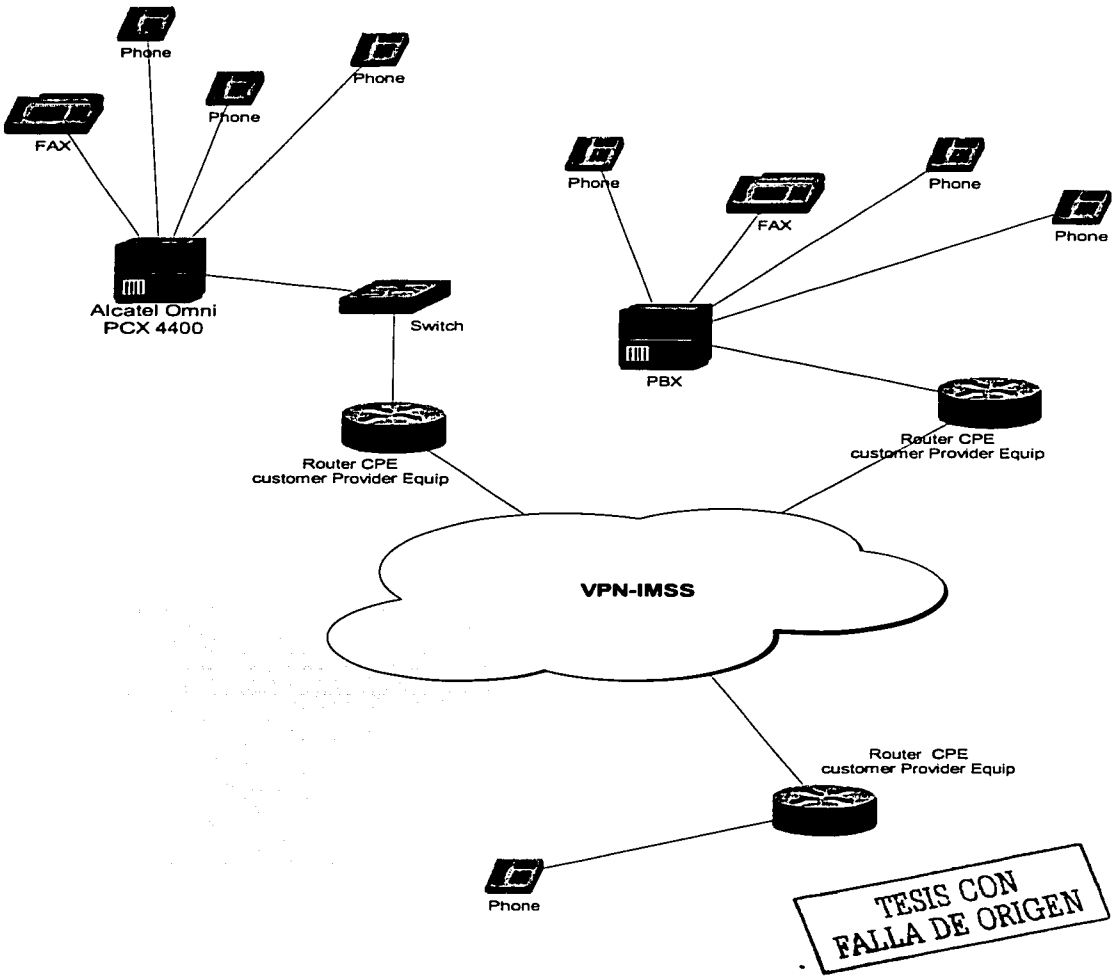
El servicio de correo de voz que se sugiere implantar, es una solución no propietaria de los PBX, esto con la finalidad de que los correos de voz se puedan comunicar entre si sin importar la marca del conmutador al que estén conectados. El servicio de correo de voz se recomienda para el grueso de la población y servicios más avanzados como son fax y mensajería unificada, solo para ciertas áreas en específico. Aunque cabe mencionar que el servicio de mensajería unificada incrementara el trafico IP en la red. Esto a su vez requiere que los servidores de e-mail que se tengan actualmente incrementen su capacidad de almacenamiento, ya que en este esquema los mensajes de e-mail, voz y fax se almacenan en el servidor de correo. Otro de los servicios que se pueden manejar a través del correo de voz es la operadora automática, este servicio además de permitir marcar a un usuario del que se conoce su extensión permitirá hacer una búsqueda por nombre, manejar mas de un lenguaje en caso de ser necesario y en caso de que se requiera atención personalizada hacer la transferencia a una operadora. Por lo que una red de este tipo independientemente del tipo de enlace con que cuente (E1 o E&M) permitirá manejar funciones básicas como son:

- Retención
- Transferencia
- Conferencia

Ahora bien para crear una red privada de uso exclusivo de funcionarios solo se dependería de las facilidades de los PBX y para mantener la privacía dentro de este circulo de usuarios podemos manejar clases de servicio donde dependiendo del usuario se tiene acceso o no a un determinado plan de numeración. El grafico de la figura (4.3-a) nos muestra el esquema propuesto para los servicios de voz en la VPM-IMSS.

Grafica (4.3-a) esquema de voz.

ESQUEMAS DE VOZ PROPUESTOS PARA LA VPN-IMSS



SERVICIOS DE DATOS

En este punto nos abocaremos a describir el esquema propuesto para los servicios de datos en la VPN, a su vez esto implica la necesidad de plantear como deberán operar los dispositivos en el nuevo esquema de comunicaciones dispuesto para los CENATIS's (antes CIZ's), así como la topología y los anchos designados para dichos servicios. En el capitulo 3 dimos una descripción de la gran cantidad de aplicaciones con las que se trabaja en la institución para acceder a las bases de datos, pues bien hemos de citar que después de un análisis se toma la decisión de conservar el entorno main frame con la plataforma SNA, el esquema TCP/IP, así mismo se adicionan nuevas variantes en cuanto a equipamiento y la manera de operar de estos nuevos equipos de comunicaciones, todo ello con el objeto de tener una plataforma lo suficientemente robusta que asegure la conectividad y la operación al 100 % entre los CENATI's mismos que ahora solo estarán emplazados en las ciudades de México y Monterrey, dejando fuera de este nuevo esquema de comunicaciones al CIZ Guadalajara que durante el proceso de migración saldrá de operación, con ello se termina el esquema de la delta que formaban los CIZ's Mex, Mty y Gdl. Ahora bien la topología entre los dos CENATI's quedara con solo 2 nodos punto a punto los cuales contaran con las siguientes características técnicas y de equipamiento:

- Para el replicamiento directo entre las bases de datos del CENATI Mex y el CENATI Mty la institución contara con un en lace inicial de 8 E1's mismos que pudieran ser incrementados dependiendo de las necesidades de operación del mismo instituto.

- Sobre el backbone SNA Guadalajara México y Guadalajara Monterrey estará operando con un enlace de 512 Kbps, el cual dobla su capacidad en ancho de banda (antes 256Kbps) para enlazar el main frame del CIZ Gdl el cual será reubicado en la ciudad de Mty. Adicionalmente se tendrá un E1, sobre el backbone entre México y monterrey.

- La capacidad de procesamiento será incrementada en los dos CENATI's quedando de la siguiente manera 480 mips (mips = millones de instrucciones por segundo) para el CENATI México y 360 mips para el CENATI Mty.

- Por lo que corresponde al backbone TCP/IP se incrementa con un enlace E3 (BW de un E3 = 32.768 Mbps) para soportar los servicios de voz, datos y video.

- El equipamiento en Main Frame se moderniza con los modelos Z series 2066-003 para el CENATI Mex y Z series 2006-001 para el CENATI Mty, con sistema operativo OS/390 V.2.10 (en prueba).

- Unidades de almacenamiento Symetrix multiplataforma con capacidades de 12 Teras en el CENATI Mex y 8 Teras en el CENATI Mty.

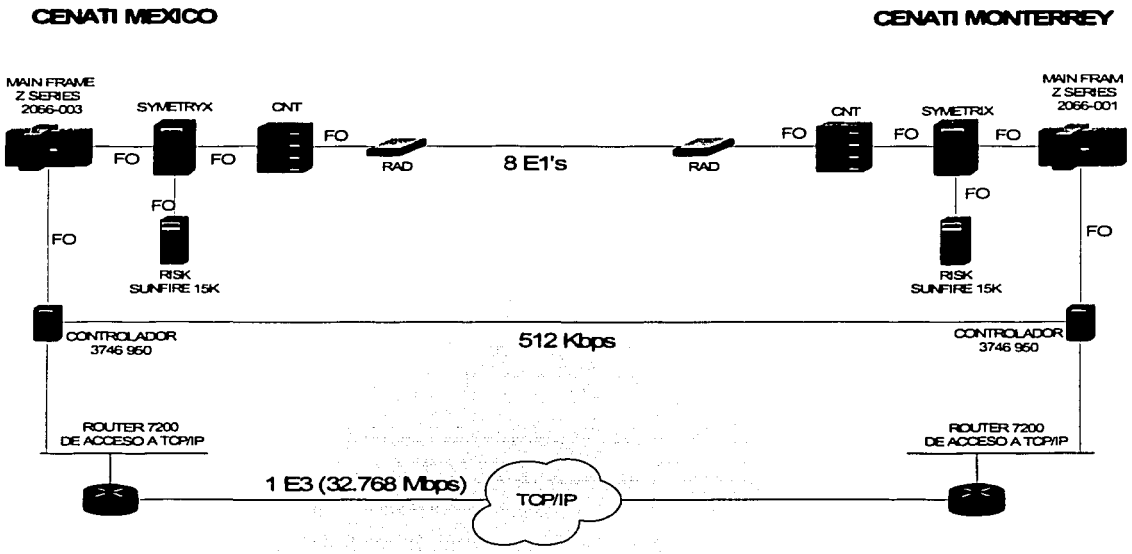
- El equipamiento dispuesto para el desarrollo de las aplicaciones institucionales lo comprenden equipos Risk Sunfire 15K de SUN Systems.

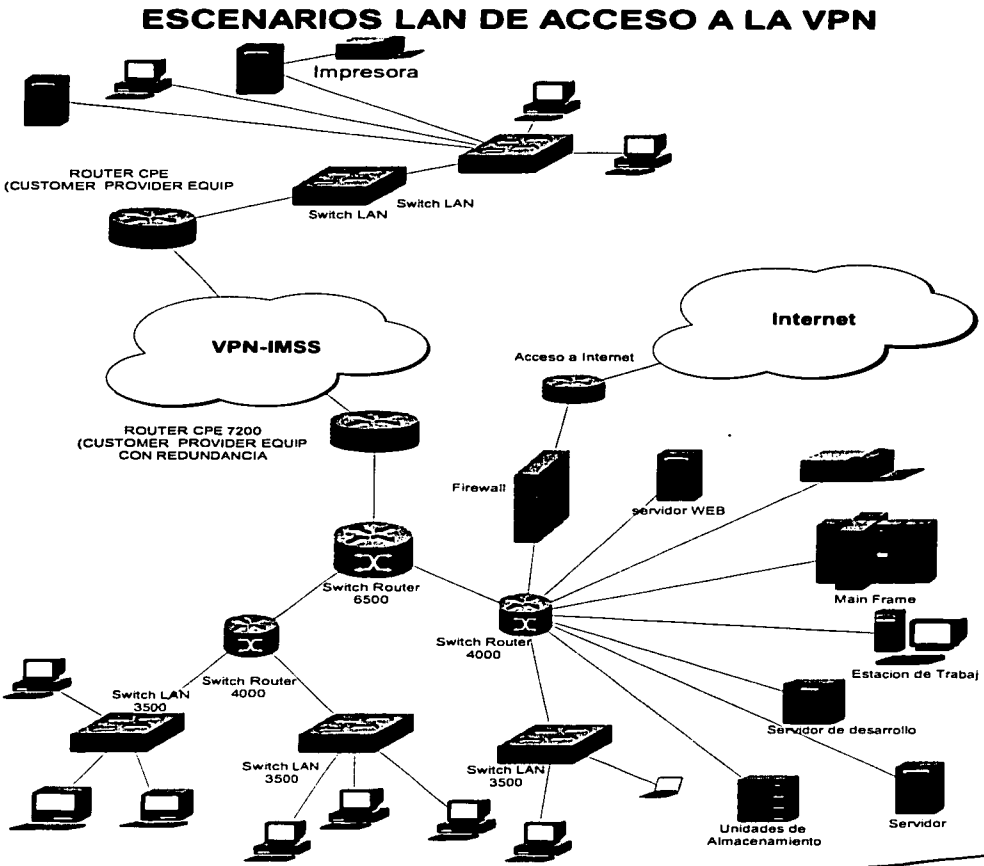
- Los accesos hacia los diferentes nodos como son los campus y demás sitios (UMF, Hospitales, Almacenes, Centros Médicos, etc.) de la VPN-IMSS, dentro del equipamiento de comunicaciones de la institución se cuenta con Switches de las familias 6000, 4000, 3000de Cisco para los diferentes servicios LAN que operen en cada sitio de la VPN.

De todo lo anteriormente descrito damos el detalle en las graficas (4.3-b) y (4.3-c)

Graficas (4.3-b) y (4.3-c)

Esquema nuevo de replicamiento en la VPN-IMSS





SERVICIOS DE VIDEO

El objetivo de esta propuesta de solución esta basada en la creación de una red de videoconferencia para el IMSS, considerando que debe ofrecer una solución confiable que permita la integración de los servicios de audio, video, datos así como su factibilidad para la expansión, y la convivencia con sus aplicaciones futuras. De acuerdo a las necesidades expuestas por el IMSS se propone una solución que cumpla con funcionalidad, tecnología de punta, seguridad e integridad de los mismos. Es decir, se propone un esquema donde los servicios de voz, datos y video,

sean confiables y seguros a través de una misma infraestructura de LAN/WAN. Los criterios y consideraciones de diseño sobre los que se ha conceptualizado esta solución están basados en los siguientes requerimientos del cliente:

- Integrar una infraestructura de conectividad de servicios de videoconferencia para escritorio (para las subdelegaciones).
- Integrar una infraestructura de conectividad de servicios de videoconferencia para salas (Delegaciones, Centros Médicos Nacionales y oficinas de Nivel Central).
- Integrar una infraestructura de conectividad de servicios de videoconferencia para telemedicina (para los hospitales de alta especialidad).
- Los medios que se contemplaron para los servicios de transmisión de estas videoconferencias es por H.320(ISDN) y H.323(IP).
- Servicio de unidad de control multipunto para los medios de transmisión H.320 y H.323.

Esta propuesta contempla equipos de compresión y descompresión de audio, video y datos para tres diferentes aplicaciones de uso, que son: videoconferencia para escritorio, videoconferencia para salas, videoconferencia para telemedicina y servicio de multipunto entre ellos. La propuesta para la integración de audio, video y datos del IMSS entre el nodo central y los sitios remotos se plantea mediante el uso de su misma infraestructura LAN/WAN.

Los criterios y consideraciones de diseño sobre los que se ha conceptualizado esta solución hacen necesario la integración de una plataforma con equipo Picturetel (Equipos de escritorio Picturetel 550, Equipos de sala Picturetel 900, Equipos de telemedicina Medlink y equipos de unidad multipunto accord). En cuanto al sitio central es necesario considerar por lo menos un equipo de telemedicina Medlink y/o Picturetel 900 y equipo multipunto accord, ya que tiene la capacidad de manejar controlar y administrar todos los nodos remotos.

Por otro lado, respecto al equipamiento de los sitios remotos se ha considerado que para video conferencia de escritorio:

- Se utilicen equipos Picturetel 550 que se instalan en una computadora personal y se conecten a un nodo de la red WAN (hasta 384 Kbps) para poder ofrecer la misma calidad en velocidad de conexión que el nodo central.

Para video conferencia en salas:

- Se contemplaron equipos Picturetel de la serie 900 los cuales tienen un puerto Ethernet y se conectan a un nodo de la red WAN (velocidades de hasta 768 Kbps):

Y para la videoconferencia de telemedicina:

- Se contemplaron equipos Picturetel Medlink los cuales tienen la facilidad de poder trabajar por un puerto Ethernet (hasta 768 Kbps).

Algo que ofrece también estos equipos es el hecho de que son fáciles de manejar, amigables en su configuración (por medio de iconos), autoprueba de hardware y conexión.

Los equipos propuestos cumplen con los estándares de la ITU-T H.320(px64), H.323 así como protocolos de audio y video (G.728, G.722, G.711, H.261, anenex D, H.263+ respectivamente), los cuales tienen la capacidad de interoperar con otros equipos de diferentes marcas existentes en el mercado actual, tales como Polycom, Vtel, aterra, Sony, etc. Cabe recalcar o reiterar que una de la ventajas de estos equipos, es precisamente que cuando no se esta ocupando el ancho de banda con aplicaciones de video conferencia como en equipos ATM, por ejemplo, el ancho de banda se puede utilizar por otras aplicaciones, sin ningún problema haciendo de esto una excelente ventaja.

En el diagrama (4.3-d), se muestra la topología propuesta para el IMSS: para conexiones punto a punto y multipunto.

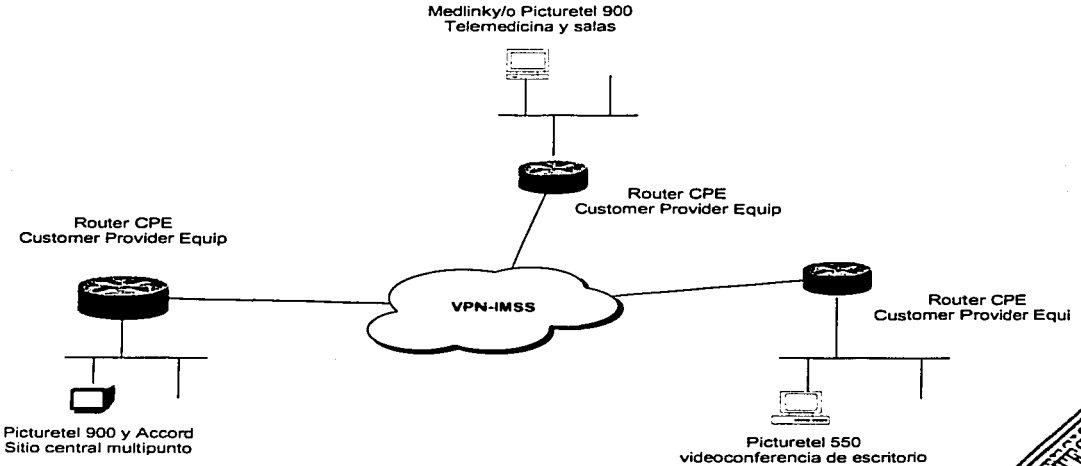
En el nodo central adicionalmente hemos dimensionado la red con un equipo multipunto Accord MGC-100 el cual nos permite tener en video conferencia a más de dos sitios al mismo tiempo y poderlos administrar fácilmente, al mismo tiempo tener en este mismo lugar un equipo Picturetel de la serie 900 para poder comprimir y descomprimir la información de audio, video y datos que se quieran transmitir o recibir de los puntos remotos, estos equipos cumplen con los estándares de la ITU-T lo cual les permite con mucha

facilidad conectarse con equipos de cualquier marca, pero como es una red WAN propia estos equipos deben estar dentro de la misma red del IMSS.

En los nodos remotos se planteo la colocación de equipos Picturetel de la serie 900 para videoconferencia en salas (Delegaciones) para tener las misma facilidades y ventajas de compartición y colaboración de audio, video y datos con el nodo central. En la videoconferencia de escritorio se colocaran equipos más sencillos que son los Picturetel 550 los cuales se instalan en una PC. Ahora bien de los equipos Picturetel que se contemplaron para esta red, aunque algunos sean para escritorio y otros para salas o aplicaciones especiales (telemedicina)todos pueden conectarse punto a punto o multipunto entre ellos mismos, ya que tanto los equipos del nodo central como los remotos, cuentan con interfaz de red Ethernet 10/100 por la cual se conectaran a la red LAN/WAN del IMSS en la VPN.

Grafica (4.3-d)

INTEGRACION DE VIDEOCONFERENCIA EN LA VPN-IMSS



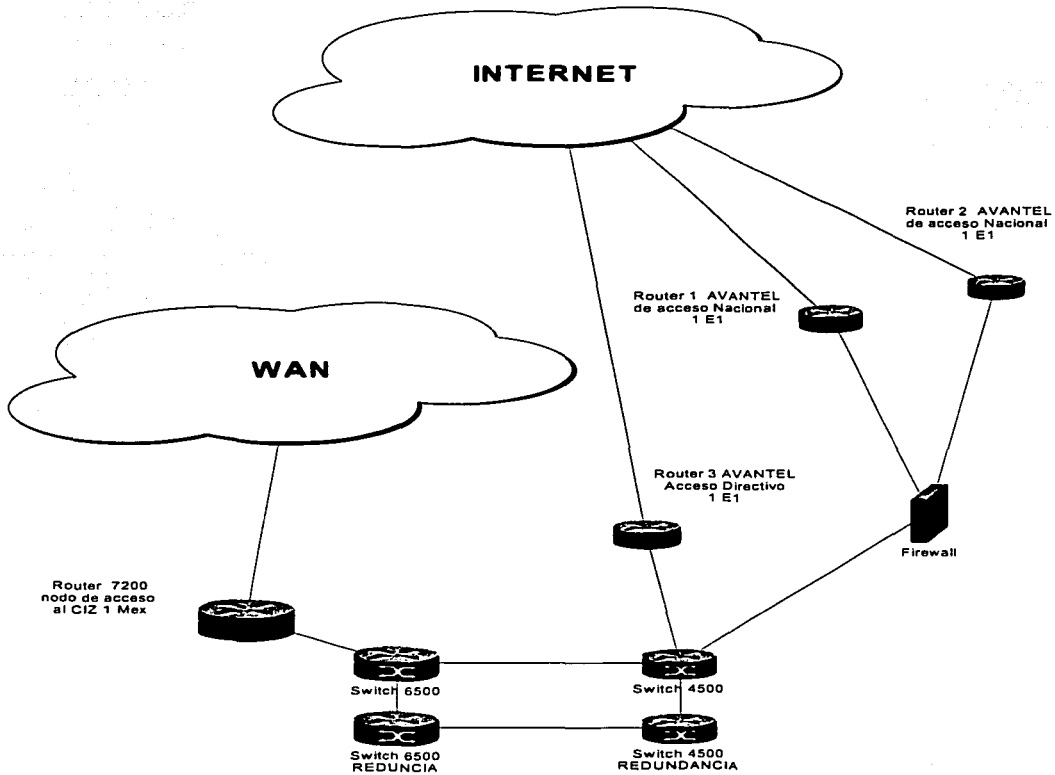
OTROS

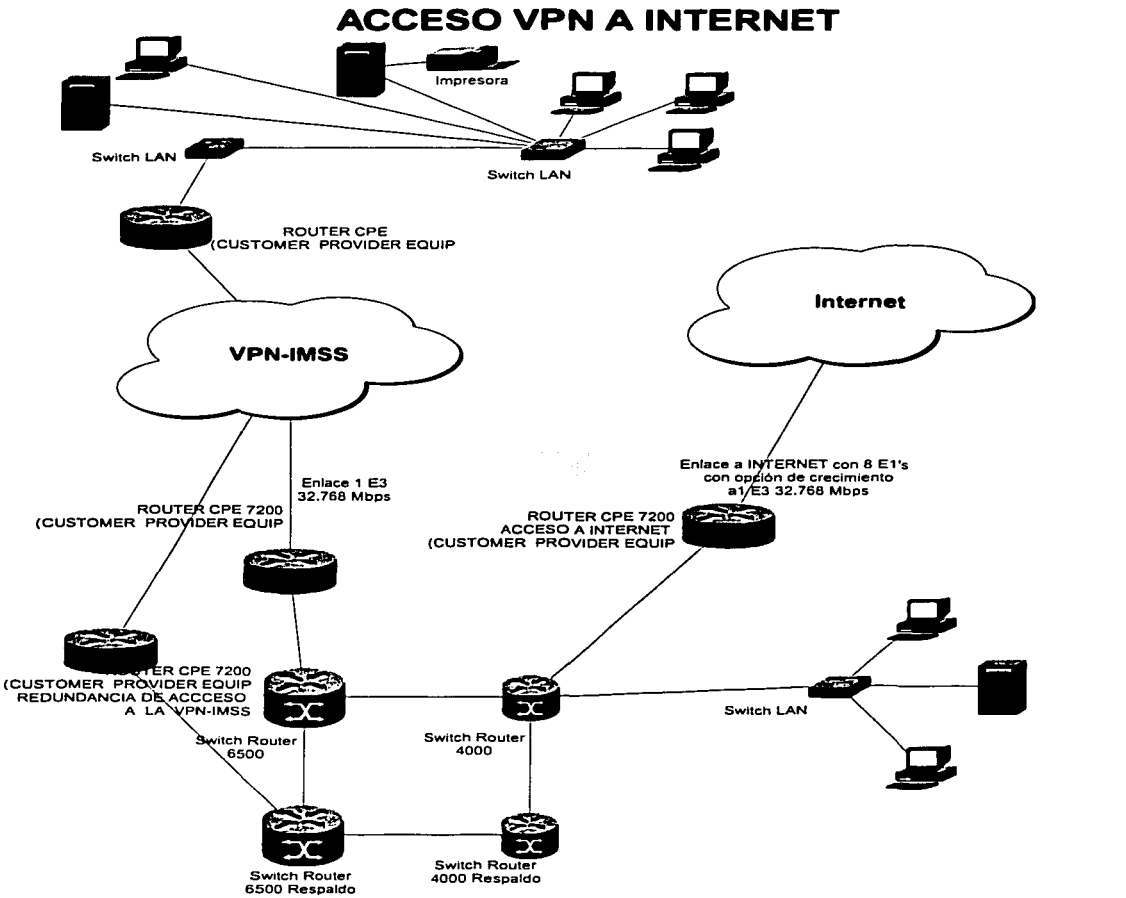
El acceso a internet para la VPN-IMSS será más robusto ya que habrá acceso por el CENATI México y el CENATI Monterrey con un enlace de 8 E1's de inicio y con infraestructura de crecimiento a 1 E3 en ambos CENATI's. Esquema que además Contemplara una solución de seguridad idéntica por cada una de las salidas hacia Internet, una en el nodo CENATI México y otra en el Nodo CENATI Monterrey. Cabe mencionar que lo anterior se desprende del hecho de que la cantidad, de usuarios concurrentes, estimada por el Instituto, con acceso a Internet

será de 40,000. Las graficas (4.3-e) y (4.3-f) nos describen más ampliamente los esquemas de acceso a Internet actualmente en la RITEL y el esquema de acceso propuesto para la VPN-IMSS.

Graficas (4.3-e) y (4.3-f)

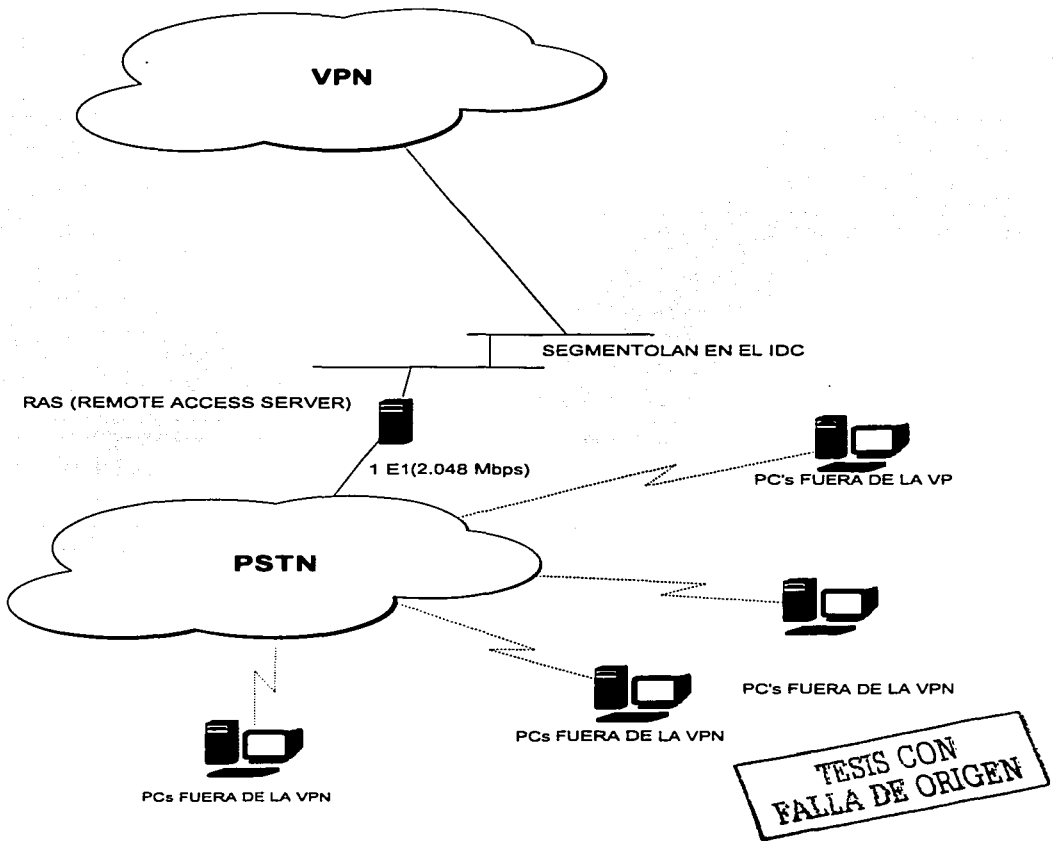
ESQUEMA DE ACCESO A INTERNEL EN LA RITEL IMSS





Otro escenario contemplado por el instituto para implantarse sobre el esquema de la VPN-IMSS es el acceso por RAS (Remote Access Server). Aunque dicho esquema no esta solicitado al proveedor como parte de los servicios requeridos en la VPN, ni en los costos de este proyecto. Se ha considerado como una solución que la institución pondrá en marcha e integrara con recursos propios como parte de otro escenario de acceso ala VPN. Como nota adicional podemos mencionar que este servicio solo será para usuarios con permiso de acceso a la VPN. El acceso a la VPN estará dado por un enlace E1 que conectara la red PSTN hacia el servidor RAS, mismo que a su vez este estará emplazado de cara hacia el segmento LAN del CENATI México o Monterrey. Para ello damos el esquema (4.3-g).

ESQUEMA DE ACCESO RAS A IMPLEMENTARSE COMO OTRO ESCENARIODE ACCESO A LA VPN



Una vez que hemos descrito el panorama general de los nuevos escenario sobre la VPN-IMSS, pasaremos al hecho de plantear en el siguiente capítulo, los aspectos económicos que sustentan la magnitud de este proyecto de carácter nacional para la institución, haciendo hincapié en que el escenario de acceso RAS no esta contemplado en los costos ni en las soluciones requeridas al proveedor.

ANÁLISIS COSTO BENEFICIO

Para este capítulo nos ayudaremos de un comparativo hecho con la VPN de la Secretaría de Hacienda y Crédito Público, y la actual RITEL del IMSS ello nos servirá como marco de referencia para evaluar los costos de este proyecto con el fin de asentar bases firmes que sustenten el costo del proyecto denominado como VPN-IMMS. Esto es con el objetivo firme de poder constatar realmente todos los beneficios que obtendrá la institución de la mejora tecnológica, así como la propuesta económica aprobada para dicho proyecto. El tope del presupuesto asignado para cubrir el proyecto de la VNP-IMSS es del orden de $ 1000 millones de pesos con una proyección a 3 años con el proveedor ganador de la licitación.

Para la cuantificación de E1's por cada red se tomo la siguiente relación:
Ancho de banda en E1's = ancho de banda total /2.048
1E = 2.048 Mbps

Para empezar a dar un esbozo de las cifras, las ventajas y el ahorro en términos económicos de este proyecto, empezaremos con el hecho de plantear un pequeño análisis comparativo como punto de partida que dando de la manera siguiente:

Como primer punto de comparación se tomaron datos que involucran el números de nodos, ancho de banda total medido en E1's así como los costos calculados en la VPN de la SHCP, ahora bien para esta red de la SHCP los costos proyectados a 3 años se describen en la tabla 4.

En las tablas 1, 2, y 3 solo detallamos numero de nodos, ancho de banda total y ancho de banda medido en E1's.

Tabla 1 parámetros de la VPN SHCP.

280590	**Ancho de Banda Total de Voz / Datos / Video (kbps)**
137.006836	**Ancho de Banda Total de Voz / Datos / Video (E1's)**
NODOS	**330**

El segundo punto de comparación fue el hecho de medir, comparar y cuantificar los mismos parámetros tomados en la red anterior, pero con los datos que aporta la RITEL IMSS (red actual). Todo ello con el objeto de tener mas referencias y datos que nos ayuden a evaluar la proyección de los costos de la VPN-IMSS, y con el fin de sacar conclusiones que justifiquen la magnitud y los alcances de este proyecto institucional de carácter nacional. Así que de la misma manera que en el caso anterior, mostramos en la tabla 2 los mismos parámetros tomados en consideración como son números de nodos, ancho de banda total medido en E1's. Los costos de la RITEL están plasmados de igual manera en la tabla 4.

Tabla 2 parámetros de la RITEL IMSS.

95108	**Ancho de Banda voz / datos / video (kbps)**		
46.4394531	**Ancho de Banda voz / datos / video (E1's)**		
NODOS	**317**		

Ahora bien, una vez que tenemos algunos parámetros analizados en dos redes diferentes y que también se conoce que ambas operan en esquemas de comunicaciones diferentes, con diferencias en cuanto al número de nodos, ancho de banda utilizado y costos a tres años. Pasamos al hecho de hacer el mismo análisis con los parámetros del proyecto de la VPN-IMSS. Así mismo de la misma forma que en los casos anteriores asentamos los costos de este proyecto a tres años en la tabla 4 y solo detallamos el números de nodos, ancho de banda total medido en E1's en la tabla 3.

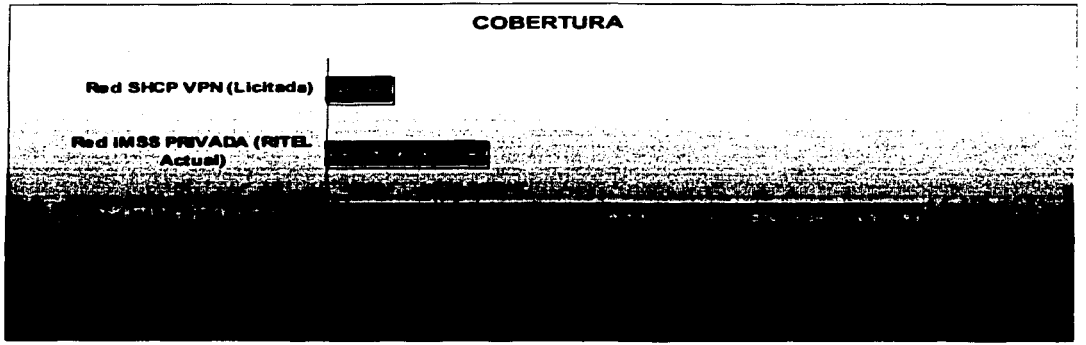
Tabla 3 parámetros de la VPN-IMSS.

491056	**Ancho de Banda Total de Voz / Datos / Video (kbps)**			
239.7734375	**Ancho de Banda Total de Voz / Datos / Video (E1´s)**			
NODOS	**2930**			

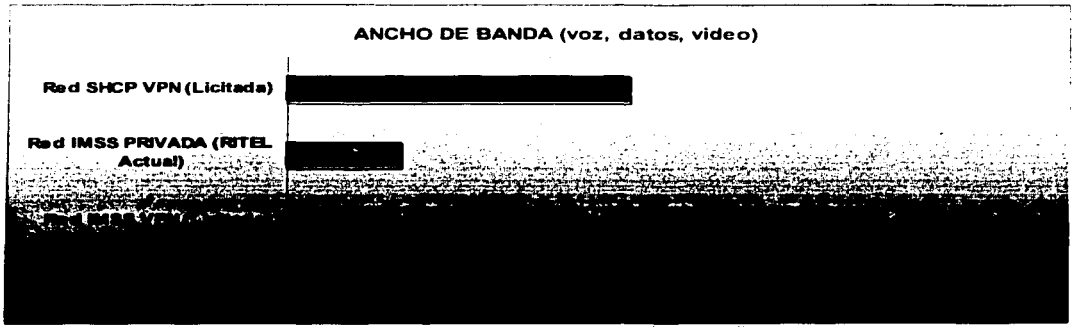
La tabla 4 hace referencia de el numero de sitios contemplados en cada una de las tres redes, así como también detalla el ancho de banda ocupado por cada red medido en E1's y por ultimo se hace una descripción sobre el costo de cada uno de estas redes con proyección a tres años de servicio.

RED	No. Sitios	Total E1's	Costo a 3 años
Red IMSS VPN (Licitada)	2,930	239	669,321,000
Red IMSS PRIVADA (RITEL Actual)	795	46	298,000,000
Red SHCP VPN (Licitada)	330	137	226,428,660

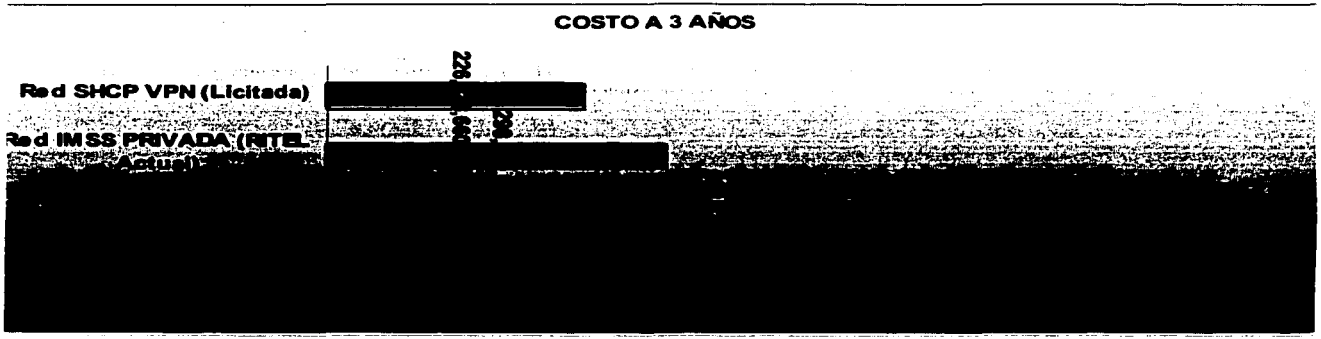
La grafica (5a) nos describe el alcance en términos de cobertura por el número de nodos asignados a nivel nacional en cada una de estas redes.



Ahora bien, en cuanto a los anchos de banda utilizados por estas redes la grafica (5b) nos hace referencia del ancho de banda total cuantificado en E1's en cada uno de estos tres proyectos.



Y por ultimo detallamos en el grafico (5c) los costos reales calculados a tres años para cada unos de los proyectos.



El proyecto de modernización de la red IMSS VPN IP/MPLS, podemos citar que es un buen proyecto en el país a nivel institucional y de gran magnitud a nivel Latinoamérica, en lo que se refiere a aspectos como su cobertura geográfica, mejoras tecnológicas en sus nodos IDC principales, en la modernización con nuevas tecnologías, nuevos escenarios de operación, nuevos esquemas de acceso WAN , en la asignación e implementación de mayores anchos de banda, en la disminución de tiempos de operación, y por supuesto con una disminución considerable de costos en un proyecto de esta índole.

Como observación final de este trabajo de tesis tenemos que este proyecto nos aporta las siguientes conclusiones:

- Es un proyecto de magnitud nacional que aporta nuevos elementos para la transformación y crecimiento del IMSS.
- Se perfila como uno de los proyectos más grandes en su género y de su tipo, ya que hoy en día son muy pocas las instituciones que han implantado VPN's en México.
- La institución se transforma de nueva cuenta con nuevos e innovadores esquemas en las áreas de telecomunicaciones e informática a nivel latinoamérica.
- Se asegura un proyecto sustentable para el corto y mediano plazos con tecnologías que no serán obsoletas en poco tiempo.
- El nuevo proyecto contribuye en el mejoramiento y desempeño de todas las áreas informáticas de la institución.
- Se incrementa la cantidad de nodos a nivel nacional en más del triple de los existentes.
- Los accesos a internet por la VPN también son mejorados en servicio y ancho de banda con la nueva propuesta.
- Se incorporan e implementan tecnologías informáticas ya usadas en países de primer mundo como son las videoconferencias, la telemedicina y la telefonía IP.
- Se elimina la problemática de lentitud y tráfico excesivos acumulados en el último par de años.
- Desaparece la topología jerárquica que ocasionaba cuellos de botella, y se establece conectividad todos contra todos.
- Con esto la institución se sitúa dentro del país, con una gran plataforma de comunicaciones, procesamiento de datos, replicamiento de datos, almacenamiento de los mismos y con una gran cantidad de vínculos con otras instituciones a nivel nacional.
- Se amplían los anchos de banda en de todos los sitios a nivel nacional
- Se logra otro de los objetivos o cometidos más importantes para la institución, que es obtener una reducción bastante considerable en los costos del proyecto, hecho que justifica al proyecto como viable términos económicos.

Academia de Networking de Cisco Systems:
Guía del primer año
John Wait Ed al
Segunda Edición 2002
Pearson Educación, S.A.

Configuración de routers Cisco
Allan Leinwand y Bruce Pinsky
Segunda Edición 2001
Pearson Educación, S.A.

Redes de Computadoras
Michael J. Palmer
Primera Edición 2001
Thompson Learning

Comunicaciones y redes de computadoras
William Stallings
Sexta Edición 2000
Pearson Educación, S.A.

Fundamentación técnica para justificar la compra por asignación directa para la renovación tecnológica de los centros informáticos de Zona 1998
Instituto Mexicano de Seguro Social
Coordinación general de informática, área de telecomunicaciones

Bases para la: Licitación pública nacional IMSS 00641149-037-2002,
para la contratación de la red privada virtual para el Instituto Mexicano del Seguro Social
MEXICO, D.F., a 21 de noviembre del 2002

Propuesta técnica preliminar de la red integral de telecomunicaciones IMSS
Telmex-Uninet-Red Uno
Mayo 2001

Consultas en internet:

http://www.cisco.com

http://www.pue.udlap.mx/~electro/REDES/lane/Antecentes.html - 11k

http://www.ldc.lu.se/natverk/je/sida/glossary/glosario_a.pdf

http://www.internetcampus.com/recomm22.htm

http://mailweb.udlap.mx/~electro/REDES/lane/Resumen.html

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

http://www.atm-forum.com

cursos.uacj.mx/ATM/atm54.htm

http://www.ptg.es/liru/tema3.ppt

http://lovecraft.die.udec.cl/Redes/disc/trabajos/atm/Atm.html

http://www.comunicaciones.unitronics.es/tecnologia/atm.htm

http://informatica.uv.es/doctorado/SST/3

http://www.iespana.es/infotutoriales/redes/redes.htm

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

http://www.monografias.com/trabajos3/voip/voip.shtml#arriba

http://www.recursosvoip.com/tutoria1/teleip.php

http:// www.blackbox.com.mx/page.asp?bc=techoverviews/framerelay&cc=MX&pc=7#top

http:// www.blackbox.com.mx/page.asp?cc=MX&pc=7&tc=10&bc=techoverviews/cat5

http://www.geocities.com/Eureka/Plaza/2131/redes.html

http://www.geocities.com/CapeCanaveral/Lab/6800/P97_JDSR.HTM#intro

http://www.cisco.com/warp/public/cc/pd/rt/12000/tech/posdh_wp.pdf

http://www.aramark.com.mx/alestra/pages/resenahistorica.html

http://iio.ens.uabc.mx/~jmilanez/escolar/redes/01040000.html

http://espanol.geocities.com/redes_ntechnology/redes.htm

http://www.usuariosenred.com.ar/consulta.php?palabra=A-Z

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

100BaseT : Especificación Fast Ethernet de banda base de 100 Mbps que utiliza cableado UTP. Al igual que la tecnología 10BaseT en la que se basa, 100BaseT envía impulsos de enlace a través del segmento de la red cuando no se detecta tráfico. Sin embargo, estos impulsos de enlace contienen más información que los utilizados en 10BaseT. Se basa en el estándar IEEE 802.3. Ver también 10BaseT, Fast Ethernet e IEEE 802.3.

100BaseT4 : Especificación Fast Ethernet de banda base de 100 Mbps que utiliza cuatro pares de cableado UTP de Categoría 3, 4 ó 5. Para garantizar una correcta temporización de la señal, un segmento 100 BaseT4 no puede superar los 100 metros de longitud. Se basa en el estándar IEEE 802.3. Ver también Fast Ethernet e IEEE 802.3.

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

100BaseX : Especificación Fast Ethernet de banda base de 100 Mbps que se refiere a los estándares 100BaseFX y 100BaseTX para Fast Ethernet sobre cableado de fibra óptica. Se basa en el estándar IEEE 802.3. Ver también 100BaseFX, 100BaseTX, Fast Ethernet e IEEE 802.3.

100VG-AnyLAN : Tecnología de medios Fast Ethernet y Token Ring de 100 Mbps que utiliza cuatro pares de cableado UTP de Categoría 3, 4 ó 5. Esta tecnología de transporte de alta velocidad, desarrollada por Hewlett-Packard, puede operar en redes Ethernet 10BaseT existentes. Se basa en el estándar IEEE 802.12. Ver también IEEE 802.12.

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

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

10BaseF : Especificación Ethernet de banda base de 10 Mbps que se refiere a los estándares 10BaseFB, 10BaseFL y 10BaseFP para Ethernet a través de cableado de fibra óptica. Ver también 10BaseFB, 10BaseFL, 10BaseFP y Ethernet.

10BaseFB : Especificación Ethernet de banda base de 10 Mbps que utiliza cableado de fibra óptica. 10BaseFB forma parte de la especificación 10BaseF de IEEE. No se utiliza para conectar estaciones de usuario, sino para establecer un backbone de señalización síncrona que permite que se conecten segmentos y repetidores adicionales a la red. Los segmentos 10BaseFB pueden tener hasta 2000 metros de largo. Ver también 10BaseF y Ethernet.

10BaseFL : Especificación Ethernet de banda base de 10 Mbps que utiliza cableado de fibra óptica. 10BaseFL forma parte de la especificación 10BaseF de IEEE y, aunque puede interoperar con FOIRL, se encuentra diseñada para reemplazar a la especificación FOIRL. Los segmentos 10BaseFL pueden tener una longitud de hasta 1000 metros si se los utiliza con FOIRL y de hasta 2000 metros si se utiliza exclusivamente 10BaseFL. Ver también 10BaseF y Ethernet.

10BaseFP : Especificación Ethernet de banda base de fibra pasiva de 10 Mbps que utiliza cableado de fibra óptica. 10BaseFP forma parte de la especificación 10BaseF de IEEE. Organiza varios

computadores en una topología en estrella sin el uso de repetidores. Los segmentos 10BaseFP pueden tener una longitud de hasta 500 metros. Ver también 10BaseF y Ethernet.

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

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

AEP (Protocolo de eco AppleTalk, AppleTalk Echo Protocol) Protocolo utilizado para probar la conectividad entre dos nodos AppleTalk. Un nodo envía un paquete a otro nodo y recibe un duplicado, eco, de ese paquete.

Algoritmo de Enrutamiento por Vector Distancia Clase de algoritmo d enrutamiento que se basa en el numero de saltos en una ruta para encontrar el árbol de extensión de ruta mas corta. Los algoritmos de enrutamiento por vector de distancia piden a cada router que envié su tabla de enrutamiento completa en cada actualización, pero solamente a sus vecinos.

Ancho de Banda Diferencia entre las frecuencias mas alta y mas baja disponibles para las señales de red. También se utiliza para describir la capacidad de rendimiento medida de un medio o protocolo de red especifico.

Anillo Conexión de dos o más estaciones en una topología circular lógica. La información se pasa de forma secuencial entre estaciones activas. Token Ring, FDDI y CDDI se basa en esa topología.

ANSI (Instituto Nacional Americano de Normalización, American Nacional Standards Institute) Organización compuesta por empresas, organismos del gobierno de los EE.UU. y otros miembros que coordinan las actividades relacionadas con los estándares. Ayuda a desarrollar estándares internacionales relacionados entre otras cosas con las comunicaciones y el Internetworking.

API (Interfaz de programa de aplicaciones, Aplication Programming Interface) Especificación de convenciones de llamadas a funciones que definen una interface para un servicio.

AppleTalk Serie de protocolos de comunicaciones diseñada por Apple Computer.

APPN (Red avanzada de igual a igual, Advanced peer to peer Networking) Versión mejorada de la arquitectura SNA de IBM. APPN manipula el establecimiento de una sesión entre nodos iguales, el calculo de rutas transparentes y dinámicas y la priorización del trafico APPC.

ARP (Protocol de Resoluciones de Direcciones, Address Resolution Protocol) Protocolo de Internet utilizado para asignar una dirección IP a una dirección MAC, definido en la RFC 826.

ARPA (Advanced Research Projects Agency) Agencia de Proyectos de Investigación Avanzada.

ARPANET A finales de los 60's, Internet es ahora una gran conexión que tiene redes independientes en todo el mundo creando una gran red global.

ASCII (Código Normalizado Americano para el intercambio de información, American Nacional Standar Code for Information Interchange) Código de 8bits.

ATM (Modo de transferencia Asíncrono, Asynchronous Transfer Mode) Estándar internacional para la retransmisión de celdas en la que múltiples tipos de servicios (como voz, datos o video) se transmiten celdas de longitud fija 53 bytes.

Backbone Parte de una red que actúa como una ruta primaria para el tráfico que se origina en, y se destina a otras redes. En una red pequeña el Backbone esta definido por el cableado principal o columna vertebral de dicha red.

Baud-(Baudio) En el uso común el "baud rate" de un módem es la cantidad de bits que puede enviar y recibir en un segundo. Técnicamente, un baudio es el número de veces por segundo que el carrier cambia de valor – por ejemplo un módem de 1200 bits por segundo corre normalmente a 300 baudios, pero este mueve 4 bits por baudio (4 X 300 = 1200 bits por segundo).

Binario Sistema de numeración caracterizado por unos y ceros(1= encendido y 0= apagado). Bit*(Binary DigIT)* Un solo dígito o número en base-2, en otras palabras, es o un 1 ó un cero. La unidad más pequeña de almacenamiento de datos en un sistema computarizado. El ancho de banda *(Bandwith)* es comúnmente medido en bits- por- segundo.

Bps(Bits-por–segundo)*(Bits- Per- Second)* Una medida de velocidad de transmisión de datos de un lugar a otro. Un módem de 28.8 puede transferir 28,800 bits por segundo.

Byt Un conjunto de bits que representan un solo carácter. Comúnmente son 8 en un byte de pendiendo de cómo se esta realizando la medición.

Canal ESCON Canal de IBM para conectar mainframes con periféricos tales como dispositivos de almacenamiento, controladores de comunicaciones.

DCE (Equipo de Circuito de Datos, Data Circuit Equipment) Los dispositivos y las conexiones de una red de comunicaciones que comprenden el extremo de la red de la interfaz de red del usuario.

DTE (Equipo Terminal de Datos, Data Terminal Equipment) Dispositivo en extremo del usuario de una interfaz de red de usuario que sirve como origen de datos, destino de datos o ambo.

E1 Sistema de transmisión digital de área amplia, utilizado predominantemente en Europa. Enlace de acceso que opera a 2,048 Mbps, que se encuentra subdividido en 32 canales.

ELAN LAN emulada. Red ATM en la cual se emula una LAN Ethernet o Token Ring utilizando un modelo cliente servidor.

ESCON (Enterprise System Connection) Conexión del sistema corporativo. Arquitectura de canal IBM que especifica un par de cables de fibra.

Ethernet Un método muy común de establecer redes en una LAN *(red no muy grande "local area network)* Ethernet maneja aproximadamente 10,00,000 bits – por –segundo y puede ser usado con casi todo tipo de computadora.

FDDI *(Fiber Distributed Data Interface)* Un estándar de transmisión de datos empleando fibra óptica con un rango de 100,000,000 bits – por –segundo *(10 veces más rápido que una red ethernet, alrededor del doble de rápido que un T-3)*

FTP *(File Transfer Protocol)* Un método muy común de transferir archivos a través de sites Internet. FTP es una manera especial de establecer contacto *(login)* con otros sites Internet con propósito de obtener ó enviar archivos. Existen muchos sites Internet que ofrecen archivos publicitarios ó con otras intenciones que pueden ser obtenidos mediante FTP, estableciendo contacto *(login)* con el nombre de usuario anónimo *(anonymous)*, es por esto que estos sites son llamados "anonymous ftp servers".

G.114 Esta norma recomienda menos de 150 ms de retraso máximo entro los nodos extremos(bordes de la red), para tráfico en tiempo real, como la voz.

G.711 Modulación por Codificación de Pulsos (PCM) de las Frecuencias de Voz La recomendación G.711 describe la codificación de audio de 3.1 khz en un canal digital de 64 kbps.

G.722 Codificación de Audio de 7 khz en 64 kbps La recomendación G.722 describe el uso de la modulación adaptativa diferencial de pulsos para transmitir audio de alta calidad 7 khz en 48, 56 o 64 kbps. Esta recomendación también permite la transmisión de datos a 16 kbps sobre un canal de 64 kbps, con los 48 kbps restantes para audio.

G.723.1 Describe una técnica de compresión para ser utilizada en transmisiones de componentes de audio a una muy baja tasa de bits como parte del estándar H. 324. Este CODEC, tiene asociada solo dos tasas de bits: 5.3 y 6.3 kbps con muestreos de voz de 30 milisegundos. La tasa más alta, esta basada en tecnología MP-MLQ, que provee una mayor

G.728 16 kbps/Low Delay CELP La recomendación G.728 describe el método para la codificación de audio que permite una calidad próxima a 3.1 khz (PCM), usando 16 kbps de ancho de banda. EL MCS soporta los estándares de audio G.711, G.722 y G.728. El algoritmo G.728 usa sólo 16 kbps para compresión de audio, lo cual da mayor espacio para el vídeo y opcionalmente para los datos. El resultado es una significativa mejor calidad de vídeo que cuando se utilizan algoritmos de audio convencionales. Es especialmente recomendable cuando se trabaje sobre líneas de 128 kbps.

G.729 La norma especifica que se requiere que el número de paquetes perdidos sea menor del 1% para evitar errores perceptibles. Idealmente no debe de producirse perdida de paquetes.

Gateway El significado técnico se refiere a un hardware o software que traduce dos protocolos distintos o no compatibles, por ejemplo Prodigy tiene un gateway que traduce su formato interno de correo electrónico a el formato Internet del e-mail. Otro significado menos correcto de gateway es el describir cualquier mecanismo para proveer acceso a otro sistema por ejemplo, AOL puede ser llamado un gateway hacia Internet.

H.320 Equipos Terminales y Sistemas de Telefonía Visual de Banda Estrecha La recomendación H.320, un paraguas de estándares, se refiere a muchas otras recomendaciones que en conjunto describen un sistema de conferencias multimedia el cual permite a un número de usuarios compartir voz, datos y vídeo en tiempo real sobre un medio digital con capacidad desde los 56 kbps hasta los 2 Mbps. El H.320 defino los términos, proporciona una supervisión del equipo, enumera los modos de operación y las velocidades de transmisión, y describe los procedimientos para establecer una llamada, terminarla y controlar la conferencia.

H.221 Estructura de trama para un canal de 64 a 1920 kbits/s en Teleservicios Audio Visuales La recomendación H.221 define un protocolo de trama que permite la división de un canal de transmisión en subcanales para voz, vídeo, datos y señales de control. El MCS soporta todo el espectro de velocidades de transferencia para los actuales entornos de conferencia, desde 56 kbps a 2 Mbps, incluyendo agregación de canales B.

H.230 Control de Sincronismo de Trama e Indicación de Señales para Sistemas Audiovisuales La recomendación H.230 proporciona un mecanismo para el control del canal o indicación del estatus del canal entre dos dispositivos audiovisuales.

H.231 Unidad de Control Multipunto para Sistemas Audiovisuales usando Canales Digitales de hasta 2 Mbps La recomendación H.231 describe la configuración de red para una MCU y proporciona un esquema de la misma con una breve descripción de cada elemento.

H.242 Sistema para Establecer la Comunicación entre Terminales Audiovisuales usando Canales Digitales de hasta 2 Mbps La recomendación H.242 describe el procedimiento para establecer comunicaciones punto a punto entre dos terminales audiovisuales.

H.243 Procedimiento MCU para Establecer la Comunicación entre Tres o Más Terminales Audiovisuales usando Canales Digitales de hasta 2 Mbps La recomendación H.243 describe el procedimiento y funcionamiento para comunicaciones multipunto.

H.261 Codificación de Vídeo para Servicio Audiovisuales a p x 64 kbps La recomendación H.261 describe el método de compresión de la señal de vídeo para transmisión sobre medios digitales. El H.261 también especifica el rango de velocidades utilizables para transportar la información de vídeo.

Host Cualquier computadora en una red que es fuente de servicios disponibles a otras computadoras en cierta red. Es muy común el tener una máquina host que provee diversos servicios, tal como WWW y USENET.

Hub Dispositivo que integra distintas clases de cables y arquitecturas o tipos de redes de área local. Concentradores de cableado en estrella integrados por microprocesadores, memoria y protocolos como SNMP, características que lo convierten en un nodo inteligente en la red capaz de controlar y diagnosticar, incluso por monitoreo remoto

Internet La vasta colección de redes en todo el mudo interconectadas entre si. Es la red de redes. Resultado del experimento del ministerio de defensa americano, con difusión más amplia en el ámbito científico-universitario. Internet no tiene una autoridad central, es descentralizada. Cada red mantiene su independencia y se une cooperativamente al resto respetando una serie de normas de interconexión. La familia de protocolos TCP/IP es la encargada de aglutinar esta diversidad de redes.

Intranet Una red privada dentro de una organización que emplea el mismo tipo de software que se encontrara en la red pública Internet, pero es de uso interno exclusivamente. A medida que Internet se ha hecho más famoso, muchas de las herramientas empleadas en Internet están siendo empleadas ahora en redes privadas, por ejemplo, muchas compañías tienen servidores de red que están disponibles solo para sus empleados y/o clientes.

ISDN *(Integrated Services Digital Network)* Básicamente es la manera de mover datos en líneas telefónicas regulares. ISDN esta siendo rápidamente disponible a la mayoría de Estados Unidos y en muchos mercados esta costeando muy similarmente a circuitos estándar analógicos. Provee una velocidad mínima de 128,000 bits – por – segundo en líneas telefónicas regulares. En la práctica, la mayoría de las personas serán limitadas a 56,000 ó 64,000 bits – por –segundo

ISP *(Internet Service Provider)* Una institución que provee acceso a Internet de alguna forma con intenciones lucrativas.

LAN *(Local Area Network)* Una red de computadoras limitados por el área que rodea a la red, comúnmente un edificio un piso de un edificio.

Línea de 56K Una conexión a través de una línea teléfono digital capaz de llevar 56,000 bits- por segundo. A esta velocidad, un Megabyte se llevara aproximadamente 3 minutos en transferirse. Esta velocidad es 4 veces, más rápido que un módem de 14,000bps.

Mainframe Microcomputador que en la actualidad se utiliza esta palabra para referirse a los grandes ordenadores.

MAN (Metropolitan Area Networks/MAN) redes computacionales de tamaño medio situadas en una misma área geográfica.

MIP (Million Instructions Per Second). Millones de Instrucciones por Segundo. Se utiliza como unidad de medida procesamiento en dispositivos como mainframe.

MODEM *(Modulator, DEModulator)* Un dispositivo que conecta una computadora a una línea telefónica y permite a la computadora comunicarse con otras computadoras mediante el sistema telefónico. Básicamente, los módem son para las computadoras como los teléfonos para los humanos.

Networking Conexión de cualquier conjunto de computadoras, impresoras, routers, switches, y otros dispositivos.

NIC *(Networked Information Center)* Generalmente, cualquier oficina que maneje información de una red. El más famoso de estos en Internet es el InterNIC, que es donde los nuevos Domain Names son registrados.

Node (nodo) Cualquier computadora por si sola conectada a una red o punto en donde se producen dos ó más conexiones en una red de comunicaciones.

OC (Optical Carrier) Portadora óptica. Serie de protocolos físicos (OC-1, OC-2, OC-3, etc.), definidos para las transmisiones.

OSI (Interconexión de Sistemas Abiertos, Open System Interconection) programa internacional de estandarización creado por ISO y la ITU-T para desarrollar estándares de Networking de datos que faciliten la interoperabilidad de equipos de varios fabricantes.

PBX (Private branch exchange) Central telefónica. Tablero de conmutación telefónico digital o analógico ubicado en las instalaciones de telefonía del conmutador.

POP Dos significados comunes: Point of Presence y Post Office Protocol. La primera, Point of Presence, se refiere a una ciudad o localidad donde una red puede conectarse comúnmente con líneas dial-up. Entonces si una compañía anuncia que pronto tendrá un POP en Monterrey, significa que ellos tendrán pronto un teléfono local en Monterrey y/o un lugar donde líneas dedicadas podrán conectarse a su red. El segundo significado, Post Office Protocol, se refiere a la manera en que el software del correo electrónico como el Eudora recibe el correo de un servidor. Cuando se obtiene un SLIP, PPP ó una cuenta shell casi siempre se obtiene una cuenta POP junto, y esta cuenta POP será la que se le indicara a el software del correo electrónico que use.

PPP Point to Point Protocol) El protocolo conocido como aquel que permite a una computadora el usar un teléfono común y un módem para hacer conexiones TCP/IP y entonces accesar Internet.

Q.931 Señalización inicial de llamada. Especificación de la capa 3 de la interfaz usuario-red de la red digital de servicios integrados para el control de llamada básica. Q.931 maneja lo concerniente a la instalación de la llamada, manejo y desconexión de los canales B ISDN y FR y ATM se encargan de las mismas funciones en circuitos virtuales.

QSIG (Q Interface SIGnaling protocol) Protocolo estándar de señalización normalizado a nivel europeo para conectar Sistemas Telefónicos Privados (PBX) y evitar los problemas que surgen a causa de la proliferación de numerosos procedimientos de señalización propietarios incompatibles entre sí. La base de esta señalización radica en la estandarización del punto de referencia Q (el nombre de señalización Q-SIG le viene en relación a su punto de referencia "punto Q", que es el "punto S/T" definido en la RDSI pública), con la que se pretende poner de acuerdo a distintos fabricantes y administraciones en procedimientos de señalización que permitan la interconexión y provisión de servicios complementarios entre equipos de distinta procedencia. La Señalización Q-SIG proporciona unos servicios suplementarios superiores a los ofrecidos por la red pública, debido a que los requerimientos de las redes privadas pasan por obtener a nivel de red un grado de servicio similar al existente en las PBX a nivel local. Básicamente, la señalización Q-SIG pretende una serie de ampliaciones sobre la señalización de canal "D" definida por CCITT para la RDSI, para potenciar las posibilidades de dicha señalización en entornos de redes privadas de empresa.

Red (Network) Cualquier vez que se conecten 2 o más computadoras de tal manera que puedan compartir recursos, se tiene entonces una red. Si se conectan 2 o más redes y se tienen una internet.

Redundancia En Internetworking, la duplicaron de dispositivos, servicios o conexiones de forma que, en caso de fallo, los dispositivos, servicios o conexiones redundantes pueden realizar el trabajo de aquellos en los que se produce el fallo.

Router Dispositivo LAN/WAN que opera en la Capa 1 (física), en la 2 (enlace de datos) y en la 3 (red) del OSIRM. Se distingue de los puentes por su capacidad de conmutar y enrutar datos basados en los protocolos de redes como el IP. Los ruteadores pasan todo el tiempo observando las direcciones de destino de los paquetes que pasan por ellos y deciden por que ruta serán enviados.

Server (servidor) Una computadora, o un paquete de software, que provee un tipo específico de servicio a un software de cliente ubicado en otras computadoras. El término se puede referir a una pieza específica de software, como es el caso del servidor de WWW, o a la máquina en donde el software este corriendo, por ejemplo; un servidor de correo esta fuera de servicio el día de hoy, es por eso que no hay correo saliente. Un solo servidor puede contener distintos tipos de paquetes de software corriendo, esto provee muchos servidores a los clientes de la red.

SLIP *(Serial Line Internet Protocol)* Un estándar para emplear una línea telefónica común (*una linea Serial)* y un Modem para conectar una computadora a un site Internet. SLIP esta siendo gradualmente reemplazado por el PPP.

SMDS *(Switched Multimegabit Data Service)* Un nuevo estándar para transmisores de datos de alta velocidad.

Switch Divide la LAN en varios segmentos limitando el trafico a uno o más segmentos en vez de permitir la difusión de los paquetes por todos los puertos. Dentro del Switch, un circuito de alta velocidad se encarga del filtrado y de permitir el transito entre segmentos de aquellos segmentos que tengan la intención de hacerlo.

T.120 La recomendación T.120 define la tecnología de conferencia de documentos que puede existir dentro de la trama H.320. El T.120 está basado en una aproximación multicapa, la cual define los protocolos y servicios entre niveles. Cada nivel dentro de la arquitectura asume la existencia de los otros.

T.123 La recomendación T.123 es el protocolo específico de red par T.120 y define cómo el T.120 comparte los recursos de comunicaciones con el tráfico audiovisual H.320.

T.122, T.125 Servicios de Comunicaciones Multipunto las recomendaciones T.122 y T.125 para los Servicios de Comunicaciones Multipunto, el mecanismo de control de conferencias. En una conferencia, se conectan lógicamente varios puntos dentro de un dominio. Un dominio, es en la mayor parte de los casos, equivalente a los múltiples nodos que participan en una conferencia. Las aplicaciones pueden ser añadidas a más de un dominio a la vez.

T.124 Control Genérico de la Conferencia (GCC) El control Genérico de la Conferencia proporciona una estructura de alto nivel para el manejo de la conferencia. Se acompaña de funcionas tales como:

- Establecimiento y terminación de la conferencia.
- Manejo de la lista de conferenciantes.
- Manejo de la lista de aplicaciones
- Servicio de registro de aplicaciones
- Conducción de la conferencia

El GCC también proporciona coordinación entre los aspectos del tiempo real del vídeo y audio, con los datos en tiempo no real dentro de la multiconferencia.

T.126 Anotación e Intercambio de Imágenes Estáticas La recomendación T.126 define el protocolo para aplicaciones de pizarra electrónica compartida y la conferencia con imágenes fijas que incluyan anotaciones. Utiliza los servicios proporcionados por el T.122 y T.124 (GCC). Se incluyen la señalización remota y el intercambio de mensajes entre teclados, de forma que los terminales remotos pueden implementar dichas funciones para la compartición de aplicaciones, incluso cuando la aplicación esta corriendo en una plataforma o sistema operativo diferente.

T.127 Transferencia Multipunto de Ficheros Binarios. La recomendación T.127 soporta el intercambio de ficheros binarios dentro de la conferencia interactiva. Proporciona un mecanismo que facilita la distribución y la recepción de uno o más ficheros simultáneamente.

T-1 Una línea arrendada o dedicada capaz de transferir datos a 1,544,000 bits – por-segundo. Teóricamente una T-1 a su máxima capacidad de transmisión transporta un megabyte en menos de 10 segundos. Sin embargo, esto no es lo suficiente rápido para pantallas completas con movimiento general, para las cuales se requiere al menos 10,00,000 bits- por-segundo. Una T-1 es el medio más rápido comúnmente usado para realizar conexiones a Internet.

T1 canalizado Enlace de acceso que opera a 1,544 Mbps, que se encuentra subdividido en 24 canales

T-3 Facilidad de portadora de WAN digital. T3 transmite datos formateados en DS-3 a 44,736 Mbps por la red.

TCP/IP (Transmission Control Protocol/Internet Protocol) El protocolo que mejor describe a internet. Originalmente diseñado para sistemas operativos UNIX, el software TCP/IP es ahora disponible para cualquier sistema operativo mayor. Para poder tener una conexión a Internet una computadora requiere TCP/IP.

Telnet El comando empleado para realizar un login de un site Internet a otro. El comando/software telnet da acceso a el prompt login del servidor al que de se desea conectar.

Terminal Un dispositivo que permite enviar comandos a una computadora ubicada en otro lugar. Como mínimo esto es un teclado y una pantalla y un conjunto sencillo de circuitos. Comúnmente se usa el software de una terminal en una computadora personal—el software pretende ser (emular) una terminal física y permite teclear comandos a una computadora lejana.

Transmisión Asíncrona Término que describe las señales digitales que se transmiten sin una sincronización precisa.

Transmisión Síncrona Término que describe las señales digitales que se transmiten con una precisa sincronización.

UPS (Uninterrumpible Power Supply). Fuente de alimentación ininterrumpible. Energía de seguridad.

VLAN (virtual LAN) LAN virtual. Grupo de dispositivos en una LAN que se configuran (utilizando software de gestión).

VPN (Virtual Private Network) Red privada virtual. Red de comunicaciones de área amplia.

WAN *(Wide Area Network)* Una red internet que cubre un área mayor a un solo edificio, edificio o campus.