



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
"CAMPUS ARAGÓN"

"ADMINISTRACIÓN ÓPTIMA DE
UNA RED ATM/MPLS"

T E S I S

QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN

PRESENTA
MARÍA DEL CARMEN REYES SÁNCHEZ

Asesor:

M. en C. DAVID M. TÉRAN PÉREZ

MÉXICO

2004



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

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

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



UNIVERSIDAD NACIONAL
AUTÓNOMA DE
MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
ARAGÓN
DIRECCIÓN

MARÍA DEL CARMEN REYES SÁNCHEZ
Presente

Con fundamento en el punto 6 y siguientes, del Reglamento para Exámenes Profesionales en esta Escuela, y toda vez que la documentación presentada por usted reúne los requisitos que establece el precitado Reglamento; me permito comunicarle que ha sido aprobado su tema de tesis y asesor.

TÍTULO:

"ADMINISTRACIÓN ÓPTIMA DE UNA RED ATM/MPLS"

ASESOR: Ing. DAVID MOISÉS TERÁN PÉREZ

Aprovecho la ocasión para reiterarle mi distinguida consideración.

Atentamente
"POR MI RAZA HABLARÁ EL ESPÍRITU"
San Juan de Aragón, México, 28 de mayo de 2003.

LA DIRECTORA

ARQ. LILIA TURCOTT GONZÁLEZ



C p Secretaria Académica
C p Jefatura de Carrera de Ingeniería en Computación
C p Asesor de Tesis

LTG/AIR/IIa

Hoy termina una etapa más en mi vida, he llegado al final de este camino y en mi han quedado grandes recuerdos de este largo recorrido. Quiero dedicar este espacio a quienes lo han compartido con migo, quienes me dieron la oportunidad de vivir, quienes me han heredado el tesoro más valioso que pudiera recibir para continuar con mi superación, mis padres:

Claudia Sánchez Bravo y Othón Reyes Montes

Agradezco la confianza que han depositado en mi, su comprensión al compartir con migo logros y tropiezos, el cariño que en cada segundo de mi vida me han brindado y el apoyo que me han dado no solo a lo largo de mi vida como estudiante sino cuando más lo he necesitado.

Gracias por todo el tiempo que les robé pensando en mí, por enseñarme a que el éxito y la felicidad dependen de mi habilidad para alcanzar las cosas que yo quiero en la vida, por inculcarme a renunciar al fracaso y la mediocridad, pero sobre todo porque han sacrificado gran parte de su vida para reforzar la mía, moldearla y dirigirla a triunfar, con cualquiera que sea el significado del triunfo en mi vida.

Haciendo de éste un triunfo más suyo que mío, porque su esfuerzo ha sido mucho más grande que el mío, quiero que sepan que mis logros e ideales han sido también suyos e inspirados en ustedes, porque su presencia ha sido y será siempre el motivo más grande que me ha impulsado para seguir adelante.

Hoy, la vida me desafía a sobresalir y solo me queda decir que me esforzare por ser mejor cada día, mantendré viva mi capacidad de soñar grandes sueños, aunque sé que soñar e inspirarme es vital pero poner en práctica lo soñado en fundamental, trabajare con más inteligencia, más creatividad, más ambición y más exigencia para mi y por ustedes.

Sé que nunca existirá una forma de agradecer y pagar todo lo que me han brindado a lo largo de mi existencia, por darme mucho más de lo que merezco, por hacer de mi lo que soy ahora, por esto y mucho más.....Gracias!!.

"Papás los amo"

Sinceramente

María del Carmen Reyes Sánchez

Como un testimonio de la gratitud ilimitada, porque dan lo mejor de sí mismos sin esperar nada a cambio, porque saben escuchar y brindar ayuda cuando es necesario, a quienes hicieron posible la realización de éste trabajo, con admiración y respeto:

Ing. David Bernardo Estopier Bermúdez:

Gracias, por la confianza y apoyo que siempre me brindo, compartiéndome su valioso tiempo y sus conocimientos al dirigir mi tesis cuidando hasta el más mínimo detalle de principio a fin, y sobre todo por darme la oportunidad de descubrir en ésta experiencia parte de mi capacidad e ingenio. Ha sido un gran reto trabajar con usted y ahora me deja una gran satisfacción y un gran orgullo

M. en C. David Moisés Téran Pérez:

Gracias, por todo el tiempo que me dedico, por su apoyo incondicional, por ayudarme a alcanzar mis objetivos por medio de conocimientos y motivación, por brindarme sus consejos que siempre fueron útiles, porque simple y sencillamente, sin su ayuda todo hubiera sido más difícil.

Gracias a su guía y apoyo he llegado a realizar uno de los anhelos más grandes de mi vida por lo cual viviré eternamente agradecida. A los dos mil gracias por compartir ésta inolvidable experiencia, por ser un ejemplo en mi vida y por enseñarme que no hay grandeza sin pasión por ser grande.

Agradezco a la Universidad Nacional Autónoma de México por darme la oportunidad de ser parte de su comunidad y haber hecho posible mi formación profesional.

Administración óptima de una red ATM/MPLS

Reyes Sánchez María del Carmen

ÍNDICE

Índice.....	I
Introducción.....	VIII
Justificación.....	XII
Antecedentes al trabajo.....	XVI
Plan propuesto.....	XVIII
Objetivos.....	XIX

CAPÍTULO I: CONCEPTOS GENERALES

I.1 Introducción.....	1
I.2 Definición de red.....	2
I.2.1 Componentes de una red.....	3
I.2.2 Clasificación de las redes de computadoras de acuerdo a su propietario...	4
I.2.2.1 Redes privadas.....	4
I.2.2.2 Redes públicas.....	5
I.2.2.3 Redes comerciales.....	5
I.2.3 Clasificación de las redes de computadoras de acuerdo a su cobertura geográfica.....	5
I.2.3.1 Redes de Área Local.....	6
I.2.3.2 Redes de Área Metropolitana.....	6
I.2.3.3 Redes de Área Extensa.....	7
I.2.3.4 Red de Área Global.....	7
I.3 Topologías de redes.....	7
I.3.1 Topologías básicas.....	9
I.3.1.1 Topología en bus (horizontal).....	9
I.3.1.2 Topología en estrella.....	10
I.3.1.3 Topología en anillo.....	11
I.3.1.4 Topología en malla.....	12
I.3.1.5 Topología en árbol (jerárquica).....	12
I.3.2 Topologías híbridas.....	13
I.3.2.1 Topología bus-estrella.....	13
I.3.2.2 Topología estrella-anillo.....	14
I.3.2.3 Topología estrella-estrella.....	15
I.4 Medios de transmisión.....	16
I.4.1 Medios de transmisión guiados.....	16
I.4.1.1 Par trenzado.....	16
I.4.1.2 Cable coaxial.....	17
I.4.1.3 Fibra óptica.....	17
I.4.2 Transmisión inalámbrica.....	17
I.4.2.1 Microondas.....	18
I.4.2.2 Satélites.....	18
I.4.2.3 Ondas de radio.....	19
I.4.2.4 Infrarrojos.....	19

I.5	Concepto de conmutación.....	19
I.5.1	Conmutación de circuitos.....	20
I.5.2	Conmutación de mensajes.....	20
I.5.3	Conmutación de paquetes.....	20
I.6	Concepto de arquitectura de red.....	21
I.6.1	TCP/IP.....	21
I.6.2	Modelo OSI.....	22
I.7	Interfases.....	25
I.8	Concepto de protocolo y señalización.....	26
I.9	Concepto general de Internet.....	28
I.10	Conceptos básicos de la administración de redes.....	29
I.10.1	El administrador de redes.....	30
I.10.2	Funciones del administrador.....	30
I.10.2.1	Proceso para la administración de redes.....	30
I.10.2.2	Documentación del flujo operativo de la red.....	30
I.10.2.3	Control de los usuarios, los grupos y sus derechos.....	31
I.10.3	Puntos importantes para el administrador de redes.....	31
I.10.4	Administración de la configuración de la red.....	32
I.10.5	Administración de fallas.....	32
I.10.6	Administración de rendimiento.....	32
I.10.7	Administración de seguridad.....	33
I.10.7.1	Organización de la seguridad.....	33
I.10.7.2	Seguridad de los datos.....	33
I.10.7.3	Seguridad del “hardware”.....	33
I.10.7.4	Seguridad en conexiones remotas.....	34

CAPÍTULO II: TECNOLOGÍAS DE REDES

II.1	Introducción.....	36
II.2	Conmutación de circuitos.....	36
II.2.1	Redes conmutadas.....	36
II.2.2	Redes de conmutación de circuitos.....	37
II.2.3	Conceptos de conmutación de circuitos.....	40
II.2.3.1	Conmutación por división en el espacio.....	41
II.2.3.2	Conmutación por división en el tiempo.....	43
II.2.4	Encaminamiento en redes de conmutación de circuitos.....	45
II.2.5	Señalización de control.....	46
II.2.5.1	Funciones de señalización.....	46
II.2.5.2	Localización de la señalización.....	48
II.2.5.3	Señalización por canal común.....	48
II.2.5.4	Sistema de Señalización Número 7.....	51
II.3	Conmutación de paquetes.....	54
II.3.1	Principios de conmutación de paquetes.....	54
II.3.1.1	Técnicas de conmutación.....	55
II.3.1.2	Funcionamiento externo e interno.....	56
II.3.2	Encaminamiento.....	57

II.3.2.1 Ruteador (“router”).....	57
II.3.2.2 Características.....	58
II.3.2.3 Estrategias de encaminamiento.....	60
II.3.3 X.25.....	62
II.3.3.1 Servicio de circuito virtual.....	63
II.3.3.2 Multiplexación.....	63
II.3.3.3 Control de flujo y de errores.....	64
II.3.3.4 Secuencias de paquetes.....	64
II.3.3.5 Reinicio y reordenamiento.....	64
II.4 Evolución de los conceptos de redes de datos (de X.25 a Frame Relay).....	65
II.4.1 Fundamentos.....	65
II.4.2 Concepto de Frame Relay.....	66
II.4.3 Diferencias entre Frame Relay y X.25.....	66
II.5 Evolución de la telefonía digital a RDSI.....	69
II.5.1 Redes analógicas.....	69
II.5.2 La digitalización.....	70
II.5.3 RDSI.....	70
II.6 Problemas de dos tecnologías separadas: voz y datos.....	72
II.6.1 Problemas en la transmisión de voz.....	73
II.6.2 Problemas en la transmisión de datos.....	73
II.7 Video y sus problemas en redes integradas.....	75
II.8 Problemas de las limitantes de ancho de banda.....	77

**CAPÍTULO III:
CONCEPTOS DE REDES DE ALTA VELOCIDAD**

III.1 Introducción.....	79
III.2 Sincronización en redes.....	79
III.2.1 Transmisión asíncrona.....	79
III.2.2 Transmisión síncrona.....	80
III.2.3 Transmisión isócrona.....	80
III.3 Jerarquía Digital Plesiócrona (PDH).....	81
III.4 Jerarquía Digital Síncrona (SDH).....	84
III.5 Modo de Transferencia Asíncrono (ATM).....	86
III.6 Aparición de RDSI-BA.....	88
III.6.1 Concepto de RDSI-BA.....	88
III.6.2 Modelo ATM.....	88
III.7 Red Óptica Síncrona (SONET).....	90
III.8 Fast Ethernet.....	92
III.8.1 Tipos de Fast Ethernet.....	93
III.8.1.1 100Base-T.....	93
III.8.1.2 100VG-AnyLan.....	94
III.9 Gigabit Ethernet.....	94
III.9.1 Características de Gigabit Ethernet.....	95
III.9.2 Especificaciones técnicas.....	95
III.10 Interfase de Datos Distribuida por Fibra Óptica (FDDI).....	97
III.10.1 Componentes de la red.....	97

III.10.2 Funcionamiento de FDDI.....	98
III.10.3 Trama FDDI.....	98
III.10.4 FDDI II.....	100
III.11 Cola Distribuida en Doble Bus (DQDB)	101
III.11.1 Características.....	101
III.12 Multiplexación en Longitud de Onda (DWDM)	103
III.13 Problemas de las redes.....	105

**CAPÍTULO IV:
 APLICACIONES DE LA ADMINISTRACIÓN DE REDES A LAS
 TELECOMUNICACIONES**

IV.1 Introducción.....	107
IV.2 Conceptos de Centros de Operación de Red (NOC)	107
IV.2.1 Actividades del NOC.....	107
IV.3 Conceptos de “Call Center”.....	109
IV.3.1 Arquitectura Integración Computador-Teléfono (CTI).....	109
IV.3.2 Componentes de un “Call Center”	110
IV.3.3 Tipos de “Call Center”	112
IV.4 Administración de Redes TCP/IP.....	116
IV.5. Sistema de Administración de Redes (NMS).....	117
IV.5.1 Protocolo Simple de Administración de Red (SNMP).....	119
IV.5.2 Concepto de MIB I.....	121
IV.5.2.1 Árbol MIB I.....	122
IV.5.2.2 RFC 1156.....	123
IV.5.3 Concepto de MIB II.....	124
IV.5.3.1 Árbol de MIB II.....	124
IV.5.3.2 RFC 1213.....	126
IV.5.4 Categorías de MIB.....	126
IV.6 Plataformas de administración de redes.....	127
IV.6.1 Open View, de Hewlett-Packard.....	129
IV.6.1.1 Características de Open View.....	129
IV.6.2 SunNet Manager, de SUN Microsystems.....	130
IV.6.2.1 Características de SunNet Manager.....	130
IV.6.3 SistemView para AIX, de IBM.....	130
IV.6.3.1 Características de SystemView.....	131
IV.6.4 Tivoli NetView, de IBM.....	131
IV.6.4.1 Características de Tivoli NetView.....	131
IV.6.5 Spectrum, de Cabletron	131
IV.6.5.1 Características de Spectrum.....	132
IV.6.6 CiscoWorks, de Cisco.....	132
IV.6.6.1 Características de CiscoWorks.....	132

**CAPÍTULO V:
PROBLEMAS ACTUALES DE LAS REDES DE
TELECOMUNICACIONES**

V.1	Introducción.....	134
V.2	El pasado.....	134
V.2.1	T1/E1 y X.25.....	134
V.2.2	Interconexión de redes de área local.....	135
V.3	Características fundamentales de las redes tradicionales.....	136
V.3.1	Medio físico compartido.....	136
V.3.2	Ancho de banda compartido.....	136
V.4	El futuro se ha convertido en el presente.....	138
V.4.1	La necesidad de mayor capacidad para comunicarse.....	138
V.4.2	Lo que las aplicaciones van a necesitar.....	139
V.5	Limitaciones de las actuales LAN.....	141
V.5.1	Interconectividad de Redes de Área Local.....	142
V.6	Nuevas implementaciones de Redes de Área Local.....	142
V.6.1	LAN conmutadas.....	142
V.6.2	Metas de las nuevas tecnologías de comunicaciones.....	142
V.7	Interconexión de redes LAN y WAN.....	144
V.7.1	Costos de conectar LAN dispersas.....	145
V.7.2	La Red Privada Virtual (VPN).....	145
V.8	Soluciones propuestas.....	147
V.8.1	Consideraciones de desempeño y distancia.....	150
V.8.2	Redes de banda ancha.....	151
V.8.3	Obtención de servicios para redes: ancho de banda por demanda.....	152
V.8.4	Dónde se proporcionan los servicios.....	153
V.9	Tendencias en la tecnología.....	154
V.9.1	“Hardware” y “software”.....	155
V.9.2	Computadoras.....	155
V.9.3	Canales de transmisión.....	156
V.9.4	Ethernet.....	156
V.9.5	Aplicaciones multimedia.....	157
V.9.5.1	Voz y video en la red.....	157
V.9.5.2	“Voice LAN”.....	158
V.9.6	Ideas recientes sobre RDSI.....	159
V.10	Problemática en redes de voz.....	159
V.10.1	Calidad de voz.....	160
V.10.2	Percepción de la calidad de voz.....	161
V.10.3	Retraso de paquetes y sus variaciones.....	162
V.10.4	Almacenamiento momentáneo de paquetes (“buffering”) y pérdida de paquetes.....	163
V.10.5	Retrasos en VoIP.....	164
V.10.6	Retrasos en la Red Telefónica Pública Conmutada (PSTN).....	164
V.11	Problemática en la administración de redes.....	165
V.11.1	Tendencias.....	165
V.11.2	Avances en la administración de redes LAN.....	166

V.12 Seguridad en redes.....	166
V.13 Desarrollo de Internet.....	167
V.13.1 Limitaciones del modelo de direcciones IP.....	167
V.13.2 IP: La Siguiete Generación (IPnG)	168
V.13.3 IP Versión 6 (IPv6)	169
V.14 Limitaciones de la Internet actual.....	169
V.14.1 Internet 2 como solución.....	170
V.14.1.1 Ventajas que ofrece Internet 2.....	170
V.15 Carencias de Internet y MPLS como solución.....	171
V.16 Servicios Diferenciados.....	173

CAPÍTULO VI:

ANÁLISIS E IMPLEMENTACIÓN DE UNA RED ACTUAL

VI.1 Introducción	174
VI.2 Descripción de la red.....	174
VI.2.1 Topología de la red.....	175
VI.2.2 Servicios que proporciona la red.....	176
VI.3 Análisis y diseño de la red.....	177
VI.3.1 Red de Área Local.....	177
VI.3.1.1 Análisis de la red.....	178
VI.3.1.2 Descripción de las funciones de la red.....	179
VI.3.1.3 Diseño físico de la red.....	180
VI.3.1.4 Topología física de la red LAN	181
VI.3.1.5 Equipos de interconectividad en la red.....	182
VI.3.2 Red del Campus.....	183
VI.3.2.1 Descripción de la red.....	183
VI.3.2.2 Diseño de la red.....	185
VI.3.2.3 Topología física de la red	186
VI.3.2.4 Especificaciones de Frame Relay	187
VI.3.3 Red WAN.....	188
VI.3.3.1 Descripción de la red.....	188
VI.3.3.2 Diseño de la red.....	188
VI.3.3.3 Topología física de la red.....	189
VI.3.3.4 Especificaciones de ATM.....	191
VI.3.3.5 Modo de operación de ATM.....	192
VI.3.3.6 Dispositivos ATM.....	195
VI.4 Implementación de MPLS.....	196
VI.4.1 Conceptos fundamentales de MPLS.....	197
VI.4.2 Beneficios de MPLS.....	198
VI.4.3 Arquitectura de MPLS.....	201
VI.4.3.1 Tipos de nodos MPLS.....	201
VI.4.3.2 Transporte de la etiqueta.....	202
VI.4.3.3 Pila de etiquetas.....	203
VI.4.3.4 Protocolos de distribución de etiquetas.....	203
VI.4.4 Funcionamiento de MPLS.....	204
VI.4.5 Aplicaciones de MPLS.....	205

VI.4.5.1 Ingeniería de tráfico.....	206
VI.4.5.2 Clases de servicio.....	207
VI.4.5.3 Redes Virtuales Privadas.....	207
VI.5 Propuesta de implementación de MPLS.....	209
VI.5.1 Estructura de una red con MPLS.....	209
VI.5.2 Elementos MPLS en una red ATM WAN.....	210
VI.5.3 Estructuras de red para la implementación de MPLS en una red ATM..	211
VI.5.4 Formas de implementación de MPLS.....	213
VI.5.5 Propuesta para implementar MPLS en la red.....	214
Conclusiones.....	217
Simbología de equipos de interconexión.....	219
Apéndice A: Equipos de interconexión.....	220
Apéndice B: Glosario de términos.....	226
Apéndice C: Acrónimos.....	232
Bibliografía.....	235

Introducción

El término *telecomunicaciones* proviene de las palabras *tele* de origen griego y que significa distancia y de *comunicare*, del latín, que significa hacerlo común. Las telecomunicaciones se encargan del transporte de la información a grandes distancias a través de un medio o canal de comunicación por medio de señales. La misión de las telecomunicaciones es transportar la mayor cantidad de información en el menor tiempo de una manera segura, (Martínez, 2002).

El origen de la comunicación parte de la necesidad del hombre por transmitir ideas, sentimientos e información que le permitan desarrollarse en sociedad. Desde que el hombre existe ha buscado la manera de satisfacer la necesidad de comunicarse con sus semejantes. Al principio lo hizo por medio de signos y señas hasta que formó códigos de información y finalmente estableció un lenguaje (Castro, 2002).

En la historia de la humanidad siempre ha existido la necesidad de transmitir información a distancia. Se puede decir que las telecomunicaciones nacieron en el momento en que se concibió la transmisión de esta información.

A mediados del siglo XIX los telégrafos conformaban las primeras redes de comunicaciones de la era moderna, la codificación en Morse constituía un método simple y eficaz para la transmisión de información a grandes distancias. Tal era la aceptación de la que gozaba la telegrafía que la invención del teléfono en 1876, fue considerada como un instrumento útil para las comunicaciones más que una curiosidad tecnológica. Aunque el telégrafo se siguió utilizando durante mucho más tiempo, el teléfono acabó por imponerse junto con las redes analógicas que fueron mayoritarias durante casi un siglo. Hubo una notable excepción: el télex, inventado en 1935, fue la primera red digital y que aún hoy sigue utilizándose prácticamente en su formato original.

Los estudios teóricos y matemáticos de los sistemas de telecomunicaciones comenzaron en los años veinte (1920-1928) con la teoría de la transmisión de señales y del ruido, abreviadamente Teoría de la Señal, cuyos padres son Carson y Nyquist, entre otros. En esta época fue cuando comenzaron a considerarse con más rigor los estudios en el dominio de la frecuencia, así como la importancia del ancho de banda de las señales y los sistemas.

Sin embargo, el gran desarrollo práctico de las telecomunicaciones vino tras la Segunda Guerra Mundial (1945), al practicar al mundo comercial los avances en múltiples áreas de la electrónica que se produjeron en esta época en el terreno militar.

La Teoría Estadística de la Comunicación tuvo su origen en los estudios de Rice, de 1944 a 1947. Rice consiguió desarrollar una representación matemática del ruido desde el punto de vista estadístico. Por la misma época, Wiener, Kolmogoroff y Kotelnikow ya aplicaron métodos estadísticos para la detección de señales.

De 1948 a 1950 se sentaron las bases de la Teoría de la Información y la Codificación. Así, en 1948, Claude Shannon publicó su Teoría Matemática de la Comunicación, donde planteó el modelo más comúnmente utilizado en sistemas de telecomunicaciones, con básicamente un *Transmisor* de la información, un *Canal* para la transmisión, y un *Receptor*, además de las señales asociadas y las perturbaciones sufridas por éstas. También en esta época, Hamming y Golay desarrollaron métodos de codificación de la información con capacidad para detectar errores y corregirlos.

La aparición del transistor de germanio en 1948 permitió la miniaturización de los dispositivos electrónicos en telecomunicaciones. De 1954 es el primer transistor de silicio, desarrollado por Texas Instruments con el fin de abaratar su costo de fabricación a la sexta parte. En 1959 apareció el primer ordenador transistorizado; y la producción comercial de circuitos integrados comenzó en 1961. Gracias a esto, los ordenadores evolucionaron muy rápidamente, lo cuál provocó más tarde una nueva revolución en el mundo de las telecomunicaciones. Las aplicaciones de los semiconductores a los sistemas de alta frecuencia (microondas) no aparecieron hasta 1963 con el oscilador de microondas de estado sólido, del físico egipcio-británico John Battiscombe Gunn.

La carrera espacial también proporcionó nuevos avances en los sistemas de telecomunicaciones. La primera propuesta para utilizar satélites geoestacionarios para la comunicación a larga distancia es de J.R. Pierce en 1955. Pero hasta 1962 no se lanzó el primer satélite exclusivamente para comunicaciones, el Telstar I, propiedad de la AT&T. Previamente, en 1960 la NASA (Aeronáutica Nacional y Administración Espacial) hizo pruebas de reflexión pasiva de señales de radio en una esfera metálica de 30 metros situada en órbita: El Echo 1. De 1963 es el primer satélite geoestacionario. Pero la revolución vino con la serie de satélites INTELSAT, que comenzó en 1965, que son propiedad de un consorcio Internacional.

Las comunicaciones ópticas tienen su origen en el láser, perfeccionado por el físico norteamericano Theodore Maiman en 1960, tras los trabajos de R. Gordon Gould tres años antes, y las publicaciones de Charles Hard Townes y Arthur Leord Schawlow. Su aplicación a las telecomunicaciones comenzó en los años sesenta tras el desarrollo de la fibra óptica.

Otra rama de las telecomunicaciones a tener en cuenta es la comunicación digital de alta velocidad. Aunque los primeros sistemas de transmisión de datos digitales se desarrollaron hacia 1958 con fines militares, su comercialización no empezó hasta mediados de los sesenta, cuando aparecieron los canales de banda ancha especialmente diseñados para señalización digital. En estos años se empezó también a aplicar la Modulación por Pulsos Codificados (PCM) para transmisión de audio y vídeo, su origen se remonta a la idea de Alec Reeves en 1937.

La aplicación de la transmisión de datos a las comunicaciones entre ordenadores, es decir, la Telemática, ha supuesto un paso más en la evolución de las telecomunicaciones. La primera red transcontinental de ordenadores que aparece es ARPANET en 1969, financiada por el Departamento de Defensa de los Estados Unidos y origen de la actual red Internet, (Ortega, 1999).

Por otro lado, la historia de los ordenadores arranca en los años cuarenta cuando fueron desarrolladas las primeras calculadoras automáticas, que en principio fueron dedicadas a realizar cálculos simples aunque muy repetitivos como la aplicación para el censo norteamericano. Pronto se observó la necesidad de acceder a aquellas máquinas desde puntos remotos, necesidad que se resolvió utilizando módems conectados a las líneas telefónicas existentes.

En los años sesenta las comunicaciones informáticas se empezaron a estructurar en protocolos e interfaces estandarizados con lo que se seguían unos soportes independientes de las máquinas, de los fabricantes y de las infraestructuras utilizadas. Esta tendencia aceleró, a mediados de los sesenta, el SNA (la primera arquitectura de comunicaciones que, posteriormente, inspiraría el Modelo de referencia OSI). A partir de este momento los soportes de comunicaciones vinieron a configurarse de modo más genérico y abstracto en torres de niveles.

Las primeras redes públicas diseñadas específicamente para el intercambio de información entre ingenios informáticos fueron las redes de paquetes que datan también de la década de los setenta. Gracias a sus mecanismos de encaminamiento, control de errores y control de flujo, resultaban más indicadas para la transmisión de datos que las redes de circuitos utilizadas hasta entonces que, en realidad, habían sido concebidas con el único objetivo de transmitir voz.

Este fue el panorama que dominó la escena de las redes públicas durante casi veinte años, hasta que apareció la Red Digital de Servicios Integrados (RDSI) que unificaba las redes de circuitos y de paquetes bajo una misma red, proporcionando simultáneamente los servicios de voz y datos. La RDSI, a pesar de no proporcionar servicios realmente nuevos, ha sido el primer estándar de aceptación universal en su seno han aparecido nuevas tecnologías de comunicaciones avanzadas como el Modo de Transferencia Asíncrono (ATM) o Frame Relay.

Pero desde que se formuló la RDSI hasta que se puso en marcha pasaron muchos años. Tanto que la informática rompió el equilibrio histórico entre capacidad de proceso de los ordenadores y capacidad de transmisión de las redes. Durante esos años, mientras la RDSI se ponía en marcha, tuvo lugar el nacimiento de la informática distribuida (LAN) y un aumento espectacular de la capacidad de proceso de las estaciones de trabajo (PC).

Los avances en las telecomunicaciones que posibilitaron la conexión entre ordenadores han incrementado, en forma inimaginable, al permitir el flujo de información entre millones de ordenadores en todos los rincones del mundo.

La interconexión de redes de ordenadores se ha comparado con una infraestructura de autopistas que se enlazan. Esta metáfora hizo surgir el término supercarretera de información, que se utiliza en forma común hoy en día. El aspecto más destacable que se le atribuye a esta tecnología es que, al posibilitar la transmisión y la consulta de información ubicada en distintos continentes, en forma casi instantánea, permite el acceso al acervo creciente de conocimientos del mundo.

Por esta razón adquiere gran importancia contar con una infraestructura de redes de datos que permita satisfacer las actuales necesidades del país y prepare a los usuarios para los desafíos que traerán los avances tecnológicos que se perfilan, (Instituto Nacional de Estadística, Geografía e Informática, 2002).

Dentro de los acontecimientos de las telecomunicaciones más importantes en México se tiene lo siguiente:

En 1968 la Secretaría de Comunicaciones y Transportes (STC) realizó con apoyo en la estación terrena Tulancingo I, el primer enlace vía satélite para transmitir los juegos de la XIX Olimpiada por medio del satélite llamado el "Pájaro Madrugador", fue este hecho el que permitió el ingreso de México a las comunicaciones espaciales.

Posteriormente pudo aliviar el congestionamiento en el tráfico intercontinental vía cable submarino y sustituir parcialmente los servicios de telecomunicación radioeléctrica en la frontera norte del país. Más tarde inició la operación del servicio telefónico internacional por satélite gracias al consorcio Intelsat, del que México formaba parte, y en 1981 transmitió la primera señal de televisión por ese medio.

En el año de 1980 se inició el estudio para crear un sistema de satélites y mientras tanto se rentó un "transponder" de Intelsat. En noviembre de 1982, luego de un concurso, se eligió a la empresa Hughes Aircraft Communications International como proveedor de los satélites Morelos I y II, cuya construcción comenzó en 1983, a tiempo que se iniciaba la instalación del centro de control en Iztapalapa. Ambos satélites fueron lanzados al espacio en 1985: el 17 de junio el Morelos I y el 26 de noviembre el Morelos II.

Entre los años 1994 y 1995 se puso en órbita la segunda generación satelital, con los satélites Solidaridad I y II. Estos satélites debían ser puestos en órbita poco antes que los satélites del sistema Morelos terminasen su vida útil.

En 1997 se privatizó Satmex. Con este hecho la empresa telefónica Autrey junto con Loral Space & Communications adquirieron el 75% del capital de Satélites Mexicanos S.A. de C.V.

En el año 1998 se lanza por primera vez un satélite comercial mexicano bajo la inversión privada: Satmex V. De esta manera se duplica la capacidad de la flota mexicana y se amplía la cobertura a todo el continente.

Entre otros aspectos importantes cabe mencionar que el 7 de junio de 1985 se publica la Ley Federal de Telecomunicaciones en México y en Enero de 1997 comienza la apertura telefónica (de larga distancia) en nuestro país, (Martínez, 2002).

Justificación

A manera de justificación del presente trabajo de tesis se menciona la importancia que tiene hoy en día el tener una red de ordenadores, así como la administración de redes jugando uno de los papeles más importantes para obtener un alto índice de rendimiento y rentabilidad, de igual forma la evolución gradual de nuevas tecnologías de red con el fin de optimizar las redes actuales.

Muchas personas utilizan los ordenadores prácticamente a diario en sus relaciones personales y profesionales. Esta tendencia se va acelerando a medida que la gente va descubriendo la potencia de los ordenadores y de las redes de comunicación para uso profesional y doméstico. Hoy en día la importancia de tener una red se ha convertido en una necesidad tanto para las empresas u organizaciones como para las personas, ya que han aumentado su productividad y rendimiento significativamente con el uso de los ordenadores y las redes de ordenadores. Gracias a la existencia de una red existe la posibilidad de que ordenadores ubicados en diferentes partes geográficas puedan intercambiar información y datos, de manera rápida a cualquier hora.

Sin embargo, el explosivo desarrollo de las telecomunicaciones ha incrementado enormemente la complejidad de las redes y la gama de servicios disponibles, lo cual resalta la importancia de la administración de redes como uno de los componentes esenciales para maximizar la relación costos/prestaciones. La importancia de la administración de una red radica en las enormes ventajas que una empresa puede obtener de esta disciplina. El propósito del establecimiento de una red no es sólo tener una forma de comunicación más, sino obtener de ella productividad y eficiencia. Por lo tanto, el gasto realizado, ya sea en mantener un equipo encargado del correcto funcionamiento de la red o del pago a una compañía especializada, permite a la empresa contratante aumentar su rendimiento y funcionalidad.

Hace algún tiempo, las redes servían solamente para soportar algunos procesos específicos en las empresas, ahora son la fuerza impulsora de la mayoría de las operaciones y servicios centrales de una organización. Cuando una red falla o funciona en forma ineficiente, se obstaculizan las comunicaciones, los datos críticos no se pueden compartir, las transacciones se vuelven lentas, y se pierde productividad y dinero.

Las redes de comunicaciones han evolucionado con el paso del tiempo ante la necesidad de satisfacer las demandas de los diferentes servicios de telecomunicaciones, que día a día necesitan un mayor ancho de banda y una mejor calidad de servicio para las nuevas aplicaciones que se han venido desarrollando hasta la actualidad. La tecnología de redes ha incrementado su complejidad generándose la necesidad de contar con una mejor administración de los recursos de estos sistemas, lo cual ha favorecido la evolución conjunta de la administración de redes. La administración de redes tiene como propósito la utilización y coordinación de los recursos para planificar, organizar, mantener, supervisar, evaluar y controlar los elementos de las redes de comunicaciones para adaptarse a la calidad de servicio necesaria, a un determinado costo.

Su campo de aplicación es amplio y de gran importancia dadas las características tecnológicas que poseen los sistemas de telecomunicaciones y los servicios que ofrecen, mantiene un cierto grado de complejidad al interactuar con sistemas heterogéneos que involucran diversos fabricantes, así como productos apegados a estándares en forma total o parcial. Además de estas presiones, existen muchas demandas sobre las redes. Con el crecimiento del número de usuarios, tamaño y complejidad, las redes tienen que soportar una nueva generación de aplicaciones complejas de gran ancho de banda, enlaces inalámbricos y bases de datos cada vez más masivas.

Al mismo tiempo, el crecimiento y el cambio constante en diversas áreas obligan al desarrollo de nuevas tecnologías. Por ejemplo, a principios de la década de 1980, la red internacional (Internet) únicamente contaba con doscientos ordenadores (“host”), en los últimos años, el número de ordenadores conectados creció drásticamente, las últimas estimaciones indican que existen más de 3,200,000. Algunos de estos ordenadores pertenecen a gobiernos, universidades, grandes empresas, empresas comerciales que se encargan de proporcionar acceso a usuarios particulares entre otros. La Internet, así como la inmensa mayoría de las redes corporativas de datos (“intranets”), basan su funcionamiento en diversas tecnologías que han ido apareciendo desde principios de los años ochenta y continúan apareciendo hoy en día.

Dentro de la aparición gradual de nuevas tecnologías de red, a principios de los años noventa vio la luz una tecnología muy prometedora. Se trató del Modo de Transferencia Asíncrono mejor conocido como ATM por sus siglas en Inglés “Asynchronous Transfer Mode”, estas redes permitieron que las velocidades de transmisión mediante las cuales accedían los usuarios, pasasen de 128 Kbps a 2 Mbps, a valores de 34 Mbps y de 155 Mbps.

Las redes ATM se diseñaron no solo para transportar datos sino también voz y vídeo, es decir, multimedia. Lo que ATM significó fue el aumento en varios órdenes la capacidad de las redes para transferir datos, permitió dar servicio a un mayor número de usuarios y ejecutar aplicaciones en red con un mayor atractivo para el usuario.

ATM, es una tecnología plenamente implantada en la Internet y en las redes de las distintas corporaciones. Se trata de una tecnología que alcanzó el grado de madurez necesario para su implantación alrededor del año 1994. ATM es hoy en día, el principal soporte de datos sobre el que se ofrecen multitud de servicios.

Al mismo tiempo, la influencia de Internet en el dinámico mercado de las telecomunicaciones ha generado una gran demanda de flexibilidad y a la vez un mayor control sobre los costos. Esta influencia provoca una necesidad importante de replantear la arquitectura de las próximas generaciones de redes, los conceptos fundamentales en esta nueva mentalidad de red son convergencia, consolidación, migración y simplificación.

También está aumentando el tipo de aplicaciones que corren por la red, como las que se realizan en entornos corporativos (por ejemplo, la videoconferencia, entre otros) que requieren un tratamiento distinto.

Es evidente que el crecimiento de Internet es imparable, el número de usuarios que se conectan a la red no termina de incrementar, el éxito de la Internet actual está vinculado al soporte de las aplicaciones y los servicios que existen sobre ella, pero hoy en día no es capaz de satisfacer las nuevas necesidades que están surgiendo. Una carencia fundamental de esta red es la imposibilidad de seleccionar diferentes niveles de servicio para los distintos tipos de aplicaciones de los usuarios, (González, 2002).

La idea original de Internet es proveer acceso a las distintas ubicaciones y distribuir contenidos. En su inicio, no era tan importante el servicio de transporte de datos, conocido como "Best Effort". Hoy en día, no debe tratarse de la misma manera un paquete de voz que necesita muy poco ancho de banda, donde el retardo está muy acotado y es menos importante la pérdida de paquetes, que una transmisión de archivos con unos requerimientos de ancho de banda mucho mayores, con una necesidad de pérdida de paquetes muy baja pero relativamente poco estricta en el retardo. Es necesario, proveer a Internet de herramientas que permitan ofrecer distinto tratamiento a diferentes tipos de tráfico.

Una de las soluciones propuestas por la Fuerza de Trabajo de Ingeniería en Internet (IETF) con el objetivo de proporcionar Calidad de Servicio (QoS) a una red de datos es la Conmutación por Etiquetas Multiprotocolo (MPLS) del Inglés "Multi Protocol Label Switching". Se trata de un estándar, capaz de soportar cualquier tipo de tráfico y capaz de ofrecer una gran eficiencia a la hora de realizar la transmisión de paquetes de un extremo a otro de la red.

Cada vez más, el desarrollo de la tecnología MPLS está revalidando las cualidades de ATM desafiando muchas de sus características y funciones hasta tal punto que la convergencia de MPLS y ATM es ahora técnicamente factible.

La tecnología ATM continúa soportando muchas y muy amplias redes multiservicio en el mundo. Desde las primeras que surgieron y hasta la nueva generación de redes de voz sobre paquetes, ATM ha demostrado ser la tecnología preferida en el mundo de los negocios y de los operadores de red.

El despliegue de redes multiservicio ATM ha permitido a los proveedores de servicio consolidar varias redes dispares en una infraestructura común con una gran reducción de costos. Como resultado, los proveedores de servicio ahora buscan que los servicios de datos sean una de sus operaciones más rentables. (IDC, 2000).

Para obtener el mismo nivel de rentabilidad en las redes de próxima generación, los proveedores de servicios deben evolucionar su infraestructura de red rápidamente para adaptarse a la demanda explosiva de nuevos servicios y mayor ancho de banda. Deben hacer esto a la vez que protegen las fuentes de ingresos de los servicios actuales de telefonía y datos. En el mercado actual de las telecomunicaciones, donde escasea la financiación y el objetivo es construir fuentes de ingresos que generen rentabilidad, el mensaje clave es obtener resultados.

Para permanecer competitivos, los proveedores de servicios deben ajustar sus operaciones usando elementos que puedan transportar y administrar tráfico de múltiples tipos de servicio. Las redes superpuestas actuales deben sufrir un proceso continuo de consolidación y optimización de red. El protocolo Internet (IP) y el Modo de Transferencia Asíncrono (ATM) coexistirán en un núcleo multiprotocolo con MPLS como la tecnología unificadora que une los beneficios de ambos mundos.

La consolidación reducirá la complejidad y el costo de construir, configurar y operar redes separadas, y proporcionará la infraestructura necesaria para soportar nuevos servicios. Para permitir esta transición de arquitectura, los suministradores de equipos deben proporcionar soluciones escalables y a la vez, cumplir la demanda de menores costos a corto plazo.

Para las redes ATM existentes, donde se usan líneas alquiladas para transportar el tráfico y existe una significativa infraestructura en el núcleo de paquetes, es posible obtener un gran ahorro consolidando este tráfico en el núcleo de la red MPLS. Para algunos proveedores de servicio, adoptar esta estrategia puede suponer ahorrar millones de pesos en costos, impactando directamente en la rentabilidad del negocio.

Antecedentes al Trabajo

Los orígenes de las redes de ordenadores se remontan a los primeros sistemas de tiempo compartido, al principio de los años sesenta, cuando un ordenador era un recurso caro y escaso. La idea que encierra el tiempo compartido es simple. Puesto que muchas tareas requieren solo una pequeña fracción de la capacidad de un gran ordenador, se sacaría mayor rendimiento de éste, si presta servicios a más de un usuario al mismo tiempo. Del tiempo compartido a las redes hay solo un pequeño escalón.

Una vez demostrado que un grupo de usuarios más o menos reducido podía compartir un mismo ordenador, era natural preguntarse si muchas personas muy distantes podrían compartir los recursos disponibles (discos, terminales, impresoras, e incluso programas especializados y bases de datos) en sus respectivos ordenadores de tiempo compartido.

Con el establecimiento de ARPANET, en Estados Unidos de Norteamérica en 1968, comenzó a entreverse el impacto social de la telemática. En 1987 la red ARPANET (dependiente del Departamento de Defensa norteamericano) utilizada al principio, exclusivamente para la investigación y desbordada por el interés demostrado por sus usuarios por el correo electrónico, necesitó transmitir datos que usaban gran ancho de banda (sonidos, imágenes y videos) y sufrió tal congestión que tuvo que declarar obsoletas sus redes de transmisión de 56.000 bits por segundo (5.000 palabras por minuto). Posteriormente, se convirtió en la espina dorsal (“backbone”) de las telecomunicaciones en Estados Unidos de América bajo su forma actual de Internet.

A medida que las redes de ordenadores fueron captando mas adeptos, compañías tales como XEROX e IBM comenzaron a desarrollar su propia tecnología en redes de ordenadores, comenzando por lo general, con Redes de Área Local. Las Redes de Área Amplia entonces, pasaron a ser usadas no solo para la comunicación entre ordenadores conectados directamente sino también para comunicar las Redes de Área Local.

Los servicios prestados por las redes de ordenadores se han difundido ampliamente y alcanzan ya a la mayoría en las naciones. El crecimiento imparable de la Internet, así como la demanda sostenida de nuevos y más complejos servicios, supone cambios tecnológicos fundamentales respecto a las prácticas habituales desarrolladas en los años anteriores, se tiene por ejemplo; la aparición y desarrollo de ATM.

La primera referencia sobre el Modo de Transferencia Asíncrono (ATM) surgió en los años sesenta cuando un norteamericano de origen oriental perteneciente a los laboratorios Bell describió y patentó una forma de transferencia no síncrona. Sin embargo, en un principio, todo su esfuerzo sólo conllevó a ciertos experimentos entre los años setenta y ochenta. ATM no se popularizó sino hasta 1988 cuando el Comité Consultivo Internacional en Telegrafía y Telefonía (CCITT), actualmente Unión Internacional para Telecomunicaciones (ITU), decidió que sería la tecnología de conmutación de la futura Red Digital de Servicios Integrados de Banda Ancha (RDSI-BA), (Guijarro, 2000).

En aquel entonces se produjo una denotada lucha de intereses y los favorecedores del ATM tuvieron primero que persuadir a algunas de las compañías propietarias de las redes de comunicaciones existentes de los beneficios del cambio de tecnología, puesto que éstas hubieran preferido una simple amplificación de las capacidades de RDSI de banda estrecha, solución que aparentemente parecía más económica.

Por otro lado, nuevas tecnologías de transmisión sobre fibra óptica, proporcionan una eficaz alternativa al ATM para multiplexar múltiples servicios sobre circuitos individuales. Además, los tradicionales conmutadores ATM están siendo desplazados por una nueva generación de ruteadores ("routers") con funciones especializadas en el transporte de paquetes en el núcleo de las redes. Esta situación se complementa con una nueva arquitectura de red de reciente aparición, conocida como Conmutación de Etiquetas Multiprotocolo del Inglés "Multi Protocol Label Switching" (MPLS), la cual se considera fundamental en la construcción de los nuevos cimientos para la Internet del próximo siglo, (Barberá, 2001).

Una de las principales cuestiones que originaron el MPLS fue el hecho de utilizar las redes ATM para conseguir un rápido envío de paquetes IP, (Lucent Technologies, 2002). MPLS es un estándar de arquitectura multinivel capaz de soportar cualquier tipo de tráfico en Internet, (González, 2002).

De la misma manera que ATM ha sido usado para transportar tráfico multiservicio sobre una Red de Área Amplia, ahora existe la oportunidad de utilizar MPLS para transportar tráfico ATM a través de un núcleo MPLS, (Castro, 2002).

La Conmutación de Etiquetas Multiprotocolo, permite construir en una red una ruta señalada entre un punto de salida y un destino, o entre un grupo de salida y un grupo de destino. Esta tecnología está basada en la colocación de "etiquetas" en los paquetes que entran en una red y que van a avanzar a lo largo de un trayecto llamado trayecto conmutado por etiquetas mediante la conmutación de etiquetas. Éstas contienen información de encaminamiento específica que puede indicar varias cosas: Un trayecto predefinido, la identidad del emisor (una fuente), la identidad del destinatario (un destino), una aplicación, una calidad de servicio, etcétera.

Los equipos intermedios están configurados para que a partir de esa información, deducir un tratamiento muy simple, ya que se trata esencialmente de enviar el paquete hacia el ruteador siguiente tomando un trayecto específico y predefinido. En primer lugar, la creación de trayectos señalados de extremo a extremo mejora mucho la rapidez de conmutación de los equipos del núcleo, ya que sus listas de rutas se limitan a una colección restringida de instrucciones simplificadas, (RISQ, 2003).

Un punto fuerte de ATM es que puede proporcionar diferentes niveles de calidad de servicio a diferentes clientes. Esta habilidad se mantiene y se mejora en la red convergente ATM/MPLS. Los servicios ATM de tiempo real pueden ser ajustados para encajar en los recursos reservados dentro del trayecto conmutado por etiquetas, y los servicios ATM sin calidad garantizada ("Best Effort") pueden estar autorizados a expandirse más allá de estos límites para aprovechar la capacidad no utilizada dentro de la red MPLS, (Castro, 2002).

Plan Propuesto:

Para obtener un buen aprovechamiento del presente trabajo de tesis, se recomienda asumirlo y asimilarlo de la siguiente manera:

Capítulo I: Se presentan los conceptos generales de las redes de computadoras con la exposición de definiciones básicas, se desarrollan las clasificaciones de redes de acuerdo a su propietario y cobertura geográfica, las diversas topologías y medios de transmisión utilizadas en el diseño de redes, se definen los conceptos de conmutación, arquitectura de red, interfases, protocolos, la idea general de Internet y por último los conceptos básicos de la administración de redes.

Capítulo II: Se definen los detalles de la conmutación de paquetes y su aplicación con X.25, detalles de la conmutación de circuitos y su aplicación a la telefonía, la evolución de la telefonía digital hacia la Red Digital de Servicios Integrados (RDSI), así como los diversos problemas que se presentan en la transmisión de voz, datos y video.

Capítulo III: Se exponen los conceptos de sincronía en redes y la evolución de las tecnologías de redes hacia su nueva generación, presentando conceptos generales de las redes de alta velocidad.

Capítulo IV: Se establecen los conceptos básicos de los Centros de Operación de Red y Centros de Atención de Llamadas Telefónicas como parte de la aplicación de la administración de redes a las telecomunicaciones, se definen los elementos (protocolos) más importantes que intervienen en la administración de redes y se proporciona una idea muy breve de las plataformas de administración existentes en el mercado.

Capítulo V: Se presenta una idea general de los problemas actuales existentes en las redes de telecomunicaciones, contrastando los problemas que existían en el pasado con los que se presentan hoy en día, de la misma forma se pretende dar una idea de las diferentes tendencias en el futuro.

Capítulo VI: Se presenta el proyecto de aplicación que sustenta el presente trabajo de tesis.

Como apoyo al lector se presenta un anexo con definiciones básicas de los equipos de interconexión mencionados en el presente trabajo, un glosario de términos con definiciones básicas para el mejor entendimiento de los conceptos presentados y por último un anexo de acrónimos en Inglés/Español para mejorar su comprensión.

Objetivos:

Objetivo general:

- ✦ Presentar una visión general sobre los principios, tecnologías, arquitecturas, plataformas y estándares de las redes, para su posterior aplicación a una red actual con el fin de optimizar su operación y administración.

Objetivos particulares:

- ✦ Presentar los conceptos básicos y generales de las redes.
- ✦ Conocer las diversas tecnologías que han surgido para su utilización en las redes.
- ✦ Analizar la evolución de las redes hacia redes de mayores prestaciones, requeridas por la emergente sociedad de la información.
- ✦ Proporcionar los conceptos generales de las nuevas tecnologías de comunicación a alta velocidad.
- ✦ Conocer los aspectos fundamentales y las distintas áreas funcionales de la administración de redes aplicados a las telecomunicaciones.
- ✦ Presentar de forma general la problemática existente en las redes actuales y sus servicios.
- ✦ Analizar e implantar los conceptos y elementos inherentes a la administración en una red actual.

CAPÍTULO 1:

CONCEPTOS GENERALES

I.1 Introducción

Una red de computadoras es un conjunto de computadoras, equipos de comunicaciones y otros dispositivos que se pueden comunicar entre sí, a través de un medio en particular, es decir, consiste en un tipo de telecomunicaciones, a su vez, el concepto de telecomunicaciones consiste en la comunicación a distancia. Las redes de telecomunicaciones nacen de las necesidades básicas de la sociedad humana y una de ellas es: “la comunicación”, a continuación se presentan los elementos esenciales de la comunicación de datos [Figura 1.1], posteriormente se definirá el concepto de red de computadoras y como intervienen los elementos aquí mencionados.

La comunicación es el proceso de transmitir información, en esta definición se destacan dos palabras:

1. Transmitir: Es pasar algo.

2. Información: Son contenidos simbólicos que representan: hechos, ideas, cosas, sentimientos, palabras, números, dibujos, etcétera.

En consecuencia, los elementos esenciales de la comunicación de datos son los siguientes:

- Fuente o mensaje.
- Emisor.
- Medio o canal.
- Receptor.
- Destino.

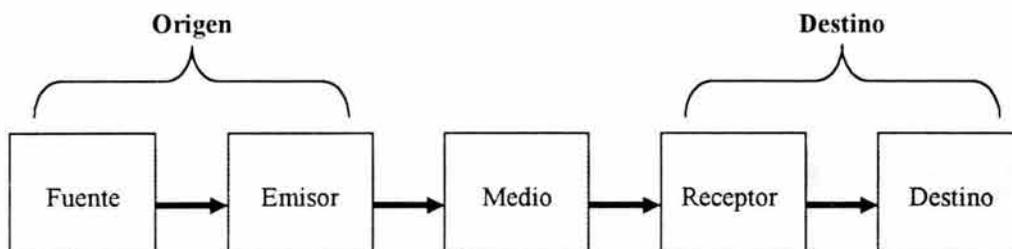


Figura 1.1 Elementos de la comunicación de datos.

Fuente o mensaje: Es la información que se trata de transmitir, constituye el primer elemento de la comunicación entre dos entidades, el cual puede revertirse de varias formas y con una duración variable. Lo más importante es que llegue íntegro y con fidelidad.

Emisor: Es el elemento que da origen al mensaje, prepara la información para que pueda ser enviada por el canal, tanto en calidad (adecuación a la naturaleza del canal) como en cantidad (amplificando la señal). El emisor puede ser una persona, una aplicación o una máquina dotada de una “inteligencia” capaz de elaborar un mensaje o proporcionar una respuesta sin que haya intervención humana alguna.

Medio o canal: Es el elemento a través del cual se envía la información del emisor al receptor. En ocasiones es factible utilizar varios medios para transmitir el mensaje.

Desafortunadamente el medio puede introducir en la comunicación: distorsiones, atenuaciones (pérdidas de señal) y ruido (interferencias). Dos características importantes del medio son:

1. Velocidad de transmisión, se mide en bits por segundo.
2. Ancho de banda, es el rango de frecuencias en el que opera la señal.

Receptor: Es el elemento al cual va dirigido el mensaje, tendrá que demodular la señal, limpiarla y recuperar de nuevo el mensaje original. Si hubiera un emisor y un mensaje pero se careciera de un receptor, la comunicación no se realizaría.

Destino: Es el elemento que toma los datos del receptor, dicho de otra forma, es a quien va dirigido el mensaje enviado por el emisor.

I.2 Definición de red

El Comité Consultivo Internacional en Telegrafía y Telefonía (CCITT) define una red como: un numero determinado de estaciones radiodifusoras o de televisión conectadas por cable coaxial, radio o línea alámbrica de tal forma que todas las estaciones puedan emitir el mismo programa simultáneamente.

Por otro lado, la Unión Internacional para Telecomunicaciones (ITU), anteriormente CCITT define una red de telecomunicaciones como un conjunto de nodos y enlaces que proporcionan conexiones entre dos o más puntos definidos para facilitar la telecomunicación entre ellos.

Sin embargo, para Black, U (1995) una red es un conjunto de computadoras conectadas mediante una o mas vías de trasmisión para la transferencia e intercambio de datos entre computadoras y terminales, la vía de transmisión es a menudo la línea telefónica, debido a su comodidad y su presencia universal.

De igual forma, Palmer, M (2001) menciona que una red es un sistema de comunicaciones que permite a los usuarios de computadoras compartir los recursos de una computadora, un programa y sus datos, la voz, imágenes y las transmisiones de video. Adicionalmente este mismo autor dice que una red de computadoras es un sistema de computadoras, dispositivos de red, impresoras y aplicaciones de “software” interconectados mediante comunicaciones por cable, fibra o radio.

Objetivos de una red:

- Entregar la información de manera confiable y sin pérdidas o modificaciones en los datos de forma lógica,
- compartir recursos e información,
- aumentar la disponibilidad de los datos,
- permitir el acceso a información a una gran cantidad de usuarios (Internet),
- permitir la comunicación,
- reducir costos.

Entre otras cosas:

Los equipos que forman la red deben ser capaces de identificarse entre sí. Además la red puede proporcionarnos un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre sí.

I.2.1 Componentes de una red

Una red de computadoras está compuesta tanto por “hardware” como por “software”. El “hardware” incluye tanto las tarjetas de interfase de red como los cables que las unen, y el “software” incluye los controladores (programas que se utilizan para administrar los dispositivos y el sistema operativo, el “software” que administra la red).

Los elementos esenciales que integran una red de computadoras son los siguientes:

- Estaciones de trabajo.
- Servidor.
- Sistema de cableado.
- Tarjetas de interfase.
- Sistema operativo.
- Recursos y periféricos compartidos.

Estaciones de trabajo: Son computadoras personales (que pueden no disponer de discos duros ni discos flexibles). Las utiliza el usuario para procesar la información, el usuario puede hacer uso de los recursos de su computadora o acceder a la red para utilizar unidades de memoria, impresoras, módems, etcétera. Las estaciones de trabajo pueden ser computadoras personales con DOS, Macintosh, Unix, etcétera.

Servidor: Es un ordenador de alto rendimiento que tiene uno o varios discos duros de alta velocidad, gran capacidad de memoria y varios puertos para conectar periféricos, ejecuta el sistema operativo de red y ofrece los servicios de red a las estaciones de trabajo, por ejemplo: unidades de disco, impresoras, bases de datos, etcétera.

Puede haber uno o varios servidores en la misma red, se tienen los siguientes tipos de servidores:

- A) Dedicado o no dedicado.
- B) Centralizado o distribuido.

Las funciones del servidor dedicado son exclusivamente administrar los recursos de la red y controlar el acceso a datos y programas de aplicación por parte de los usuarios de la red. Por otra parte, un servidor no dedicado es aquel que además, se utiliza también como una estación de trabajo de la red. Es poco recomendable utilizar el servidor en modo no dedicado, ya que hace más lento el funcionamiento de la red.

Las redes con servidor centralizado, utilizan una sola computadora como servidor de archivos, servidor de impresoras y administrador de la red. Las redes con varias estaciones de trabajo y gran tráfico de información, utilizan como servidor distribuido dos ó mas ordenadores en donde alguno de ellos se encarga de administrar el uso de impresoras, otro para administrar archivos y proporcionar programas de aplicación y posiblemente un tercero, para comunicación con otras redes.

Sistema de cableado: Es el medio físico que se utiliza para enviar o recibir mensajes de un ordenador a otro y conectar los demás componentes de la red, el cable puede ser coaxial, de par trenzado o de fibra óptica.

Tarjetas de Interfase (NIC): Es una pieza de la arquitectura (“hardware”) que va dentro del ordenador y que provee la conexión física de la red, toma los datos del ordenador, los convierte a un formato apropiado para poder ser transportados y los envía por el cable, a otra tarjeta de interfase. Esta tarjeta los convierte nuevamente al formato original y los envía al ordenador.

Sistema Operativo: Debe soportar el intercambio de información a nivel “software”, reside en clientes como en servidores, se encargan de comunicar a las estaciones de trabajo entre sí, garantizando la integridad de la información y controlando el uso de los recursos de la red.

Recursos y periféricos compartidos: Se incluyen los dispositivos de almacenamiento ligados al servidor, las unidades de discos ópticos, las impresoras y el resto de equipos que puedan ser utilizados por cualquier usuario en la red, puede ser tan amplio como se necesite ya que puede incluir procesadores de palabra, paquetes integrados, sistemas administrativos de contabilidad y áreas afines, sistemas especializados, correo electrónico, etcétera.

I.2.2 Clasificación de las redes de computadoras de acuerdo a su propietario

- Redes privadas.
- Redes públicas.
- Redes comerciales.

I.2.2.1 Redes privadas

Una red privada es aquella que se utiliza para la prestación de servicios de telecomunicaciones no disponibles para el público. Es una solución capaz de resolver las necesidades de servicios de las empresas, utilizando medios alternativos al uso de las redes públicas. El Instituto Europeo de Telecomunicaciones Estándares (ETSI) define el concepto de red privada como aquella red que puede ser constituida por estructuras dedicadas, por la utilización de medios de las redes públicas o por un mezcla de ambos tipos de medios.

Una red de comunicaciones pertenece al dominio privado cuando es ofertada únicamente para uso interno. Estas redes solo abarcan a los usuarios que pertenezcan a una determinada organización y solo se pueden comunicar con miembros de la misma organización.

I.2.2.2 Redes públicas

Una red de comunicaciones se denomina red pública cuando se utiliza, total o parcialmente, para la prestación de servicios de telecomunicaciones disponibles para el público. A este tipo de redes puede acceder cualquier usuario y comunicarse con cualquier otro que esté conectado a ella, sin ningún tipo de limitación.

Las redes públicas son de libre utilización por cualquier usuario pertenecientes a las operadoras y ofrecidos a los usuarios a través de suscripción, por ejemplo:

- Compañías de servicios de comunicación local,
- compañías de servicios de comunicación a larga distancia,
- proveedores de servicios de valor añadido.

I.2.2.3 Redes comerciales

Los proveedores de redes comerciales tienden a ofrecer una variedad de servicios como conferencias por computadora y en muchos casos acceso directo o indirecto a servicios de bases de datos en línea.

Características generales de las redes comerciales:

- Los usuarios vienen de una diversidad de contextos.
- Pueden ser muy costosas para los países en desarrollo.
- Pueden ser excelentes fuentes de información sobre ciencia, tecnología o políticas gubernamentales publicadas en revistas comerciales.
- En muchos casos son accesibles utilizando redes de conmutación.
- Las redes comerciales son ampliamente utilizadas por personas en los países industrializados, donde su acceso es económico.

Podemos dividir las redes comerciales en dos tipos:

1. Proveedores de servicios de correo electrónico.
2. Proveedores de servicios de base de datos.

I.2.3 Clasificación de las redes de computadoras de acuerdo a su cobertura geográfica

- Redes de Área Local (LAN).
- Redes de Área Metropolitana (MAN).
- Redes de Área Extensa (WAN).
- Red de Área Global (GAN).

I.2.3.1 Redes de Área Local (LAN)

Una Red de Área Local es una red privada que se define como un sistema de comunicaciones que proporciona interconexión a una variedad de dispositivos en una área restringida, su finalidad principal es la de intercambiar información entre grupos de trabajo y compartir recursos tales como impresoras y discos duros, sus características son:

- Alcance: Las distancias abarcan desde metros hasta pocos kilómetros (distancia < 10 Km), tienen baja tasa de errores.
- Su medio de transmisión: cable de par trenzado o coaxial, fibra óptica, portadoras con infrarrojo o láser, radio y microondas.
- Velocidad: Las velocidades de transmisión cubren un rango desde 10 Mbps hasta 100 Mbps.
- Conectividad: Permiten la comunicación de igual forma en los dispositivos conectados, independientemente de que se trate de grandes procesadores o de computadoras personales.
- Interconexión: Ofrecen la posibilidad de conexión con otras redes mediante la utilización de puertas de enlace (“gateways”).

Ejemplos: IEEE 802.3 (Ethernet), IEEE 802.4 (Token Bus), IEEE 802.5 (Token Ring).

I.2.3.2 Redes de Área Metropolitana (MAN)

Una Red de Área Metropolitana es una versión más grande de una LAN en cuanto a topología, protocolos y medios de transmisión, que por ejemplo puede cubrir un conjunto de oficinas corporativas o empresas en una ciudad. En general, cualquier red de datos, voz o video con una extensión de una a varias decenas de kilómetros puede ser considerada una MAN. Los medios considerados para este tipo de red son la fibra óptica y el cable de par trenzado.

La arquitectura utiliza dos buses; cada uno es unidireccional, lo cual significa que la transmisión de datos se hace en un sentido sobre un bus y en otro sobre el segundo bus, por lo tanto, cada nodo debe estar enlazado a los dos buses. El índice de velocidad varía según el medio utilizado. Así, un cable coaxial puede soportar una velocidad de 45 Mbps y un cable de fibra óptica 156 Mbps.

Una Red de Área Metropolitana puede ser pública o privada:

- Privadas que son implementadas en áreas tipo campus debido a la facilidad de instalación de fibra óptica.
- Públicas de baja velocidad (menor a 2 Mbps) como Frame Relay, Red Digital de Servicios Integrados (ISDN) T1 o E1, etcétera.

El estándar IEEE 802.6 Cola Distribuida y Bus Dual (DQDB) es un ejemplo típico de las redes MAN este estándar utiliza dos cables “half-duplex” por los cuales se recibe y transmiten voz y datos entre un conjunto de nodos.

I.2.3.3 Redes de Área Extensa (WAN)

Una Red de Área Extensa es un sistema de redes de largo alcance que cubre una amplia superficie o área geográfica para conectar Equipos Terminales de Datos (DTE), a distancias que pueden llegar a miles de kilómetros. Utiliza medios de telecomunicación suministrados por operadores externos, a la infraestructura que une los nodos de usuarios se le llama subred y abarca diversos aparatos de red (llamados “routers” o ruteadores) y líneas de comunicación que unen las diversas redes.

En la mayoría de las WAN se utilizan una gran variedad de medios de transmisión para cubrir grandes distancias y tienen topologías irregulares. La transmisión puede efectuarse por microondas, por cable de cobre, fibra óptica o alguna combinación de los anteriores.

Se pueden distinguir dos componentes: Las líneas de transmisión y los elementos de intercambio (conmutación). Las líneas de transmisión se conocen como circuitos, canales o troncales. Los elementos de intercambio son computadoras especializadas utilizadas para conectar dos ó mas líneas de transmisión.

Una red extendida debe soportar la transmisión de voz, datos digitales, video, imágenes gráficas y de fax. Un aspecto importante de las redes extendidas es la conectividad con las redes locales. Los servicios de transmisión no pueden ser eficaces si la infraestructura de las redes extendidas no cuenta con dispositivos de interconexión perfeccionados y técnicas de transmisión modernas.

Ejemplos: X.25, Red Telefónica Conmutada (RTC), RDSI, etcétera.

I.2.3.4 Red de Área Global (GAN)

Esta compuesta de diferentes redes de computadoras interconectadas, es accesible desde más de dos millones de nodos en todo el mundo y cubre una área geográfica ilimitada. Uno de los aspectos más importantes es que utiliza una base tecnológica y protocolos de comunicación que son abiertos (no tienen propietario exclusivo), permitiendo la comunicación integrada entre computadoras de distintos fabricantes.

I.3 Topologías de redes

La palabra topología es un término de origen griego que se refiere al estudio de las formas y se emplea en el diseño de redes de comunicación, es importante identificar que una red presenta dos tipos de topologías:

1. Topología Lógica: Corresponde al modo de operación de la red, es decir, el método que se usa para comunicarse con las demás estaciones de trabajo o la ruta que toman los datos entre los diferentes nodos de la misma red. Los dos tipos mas comunes de topologías lógicas son: “broadcast” (Ethernet) y transmisión de “tokens” (Token Ring).

La topología de “broadcast” significa que cada estación de trabajo envía sus datos hacia todas las demás estaciones de la red. Las estaciones de trabajo no siguen ningún orden para utilizar la red, el orden es: el primero que entra, es el primero que trabaja.

La transmisión de “tokens” controla el acceso a la red al transmitir una señal eléctrica (“token”) de forma secuencial a cada estación de trabajo. Cuando una estación recibe la señal significa que puede enviar datos a través de la red. Si la estación de trabajo no tiene ningún dato para enviar, transmite la señal hacia la siguiente estación y el proceso se vuelve a repetir.

2. Topología Física: Se refiere a la forma geométrica en que están distribuidas las estaciones de trabajo (“host”) y los cables (medios) que las conectan en la red.

Dependiendo del método de acceso al medio utilizado, el funcionamiento lógico de la red corresponderá a determinada topología pudiendo ser distinta a la topología física, además es uno de los parámetros básicos que condicionan fuertemente las prestaciones de la red, adicionalmente las topologías determinan:

- La complejidad de instalación y mantenimiento del cableado,
- la vulnerabilidad a fallos o averías,
- la administración del medio y la facilidad de localización de fallos,
- la capacidad de expansión y reconfiguración,
- el costo.

Objetivos:

- Proporcionar máxima fiabilidad que garantice la correcta recepción de todo el tráfico,
- encaminar tráfico entre Equipo Terminal de Datos transmisor y receptor a través del camino más económico y confiable,
- proporcionar un tiempo de respuesta óptimo,
- permitir un mejor control de la red,
- permitir de forma eficiente el aumento de las estaciones de trabajo.

Entre otros aspectos:

- Minimizar la longitud real para evitarnos componentes intermedios,
- proporcionar un canal más económico para cada actividad,
- tener un cuidado especial en tiempo de respuesta y un ancho de banda lo mas elevado posible.

1.3.1 Topologías básicas

Las cinco topologías físicas básicas son:

- Bus (horizontal).
- Estrella.
- Anillo.
- Malla.
- Árbol (jerárquica).

1.3.1.1 Topología en bus (horizontal)

Las estaciones de trabajo se conectan por un canal de comunicación en línea recta (“backbone”). Cuando una estación transmite, su señal se propaga a ambos lados hacia todas las estaciones conectadas al bus hasta llegar a los puntos de terminación donde la señal es absorbida; de aquí que el bus reciba también el nombre de canal de difusión, [Figura 1.2].

Solo una computadora a la vez puede mandar mensajes en esta topología, por esto, el número de computadoras conectadas al bus va a afectar el rendimiento de la red. Cuantas más computadoras están conectadas, más computadoras van a estar esperando para mandar datos por el bus y como consecuencia más lenta va a ser la conexión por red.

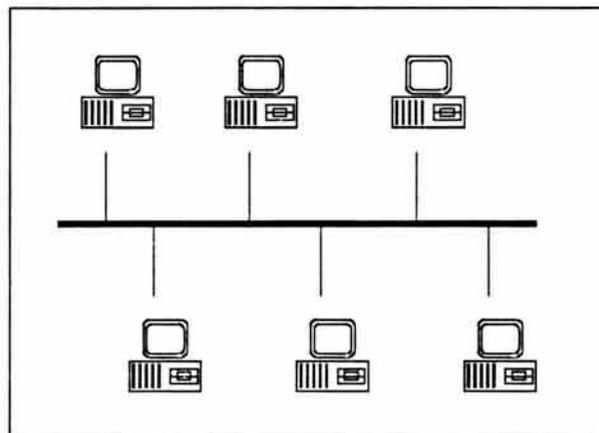


Figura 1.2 Topología en Bus.

Ventajas:

- La topología en bus es la más sencilla,
- funciona correctamente y el costo de implementación es barato para redes pequeñas,
- necesita menos cable,
- resulta fácil añadir nuevas estaciones de trabajo,
- maneja grandes anchos de banda,
- soporta de decenas a centenas de equipos.

Inconvenientes:

- Cuando el número de equipos es muy grande el tiempo de respuesta es más lento,
- dependiendo del vínculo puede presentar poca inmunidad al ruido,
- las distorsiones afectan a toda la red,
- como hay un solo canal, si este falla, toda la red falla,
- el cable central puede convertirse en un cuello de botella en entornos con un tráfico elevado, ya que todas las estaciones de trabajo comparten el mismo cable,
- es difícil aislar los problemas de cableado en la red y determinar que estación o segmento de cable los origina.

1.3.1.2 Topología en estrella

Todas las estaciones de trabajo están conectadas mediante enlaces bidireccionales a un nodo central, proporcionando un camino entre dos dispositivos que deseen comunicarse, [Figura 1.3]. Si se produce un fallo en una de las estaciones no repercutirá en el funcionamiento general de la red, pero si se produce un fallo en el servidor o en el computador central, la red completa se vendrá abajo.

Tiene un tiempo de respuesta rápido en las comunicaciones de las estaciones con el servidor o con el computador central, y lento en las comunicaciones entre las distintas estaciones de trabajo.

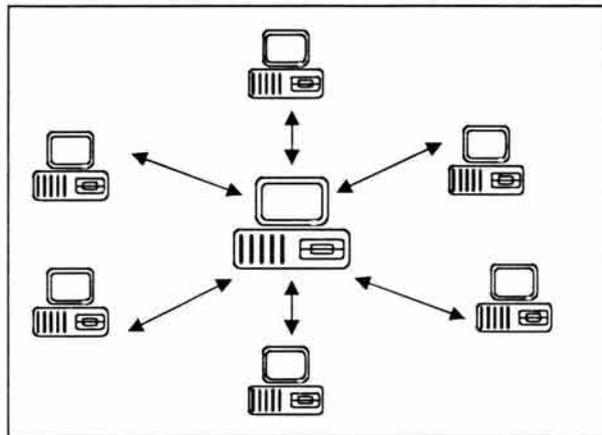


Figura 1.3 Topología en Estrella.

Ventajas:

- Estructura simple,
- es más fácil localizar los problemas en el cableado y en los nodos,
- permite incrementar y disminuir fácilmente el número de estaciones,
- cada estación de trabajo es independiente de las demás,
- fácil conexión a la red,
- la falta de una computadora no afecta a la red.

Inconvenientes:

- Limitación en rendimiento y confiabilidad,
- su funcionamiento y crecimiento depende del servidor central,
- es susceptible a fallar en un único punto (nodo central),
- no es muy conveniente para grandes instalaciones,
- su costo es caro debido a la gran instalación de cableado y a la complejidad de la tecnología que se necesita para el computador central o para el servidor.

I.3.1.3 Topología en anillo

Es un camino continuo para los datos, sin puntos lógicos de inicio ni final cuando se transmiten los datos por el anillo, van de nodo a nodo hasta que encuentran el nodo destino, [Figura 1.4]. A menudo los datos no pasan por todas las estaciones porque se puede alcanzar el nodo destino antes de que los datos hayan recorrido el círculo completo.

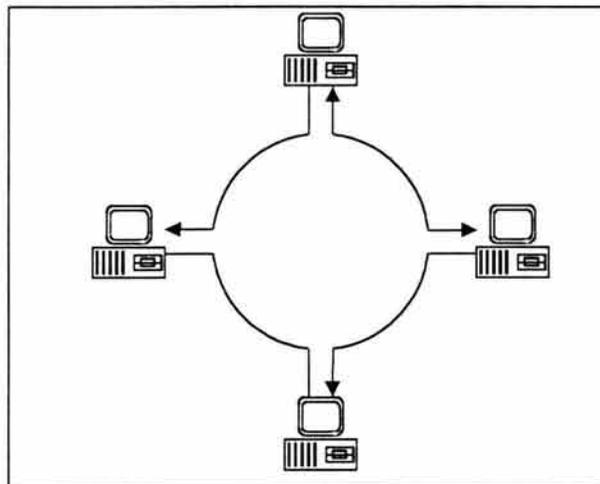


Figura 1.4 Topología en Anillo.

Ventajas:

- El sistema provee un acceso equitativo para todas las computadoras,
- el rendimiento no decae cuando muchos usuarios utilizan la red,
- es más fácil de localizar los problemas de los nodos y del cableado,
- esta topología es buena para distancias grandes,
- maneja de forma correcta los grandes volúmenes de tráfico,
- este tipo de redes permite aumentar o disminuir el número de estaciones sin dificultad,
- es muy fiable.

Inconvenientes:

- Las distorsiones afectan a toda la red,
- necesita más equipos de red y más cableado al principio que la topología de bus,
- a medida que aumenta el flujo de información, será menor la velocidad de respuesta de la red,
- un fallo en una estación o en un canal de comunicaciones dejara bloqueada la red en su totalidad.

I.3.1.4 Topología en malla

En esta topología todas las computadoras están interconectadas entre sí por medio de un tramado de cables, todos los nodos están conectados de forma que no existe una superioridad de un nodo sobre otros en cuanto a la concentración del tráfico de comunicaciones, [Figura 1.5]. En muchos casos la malla es complementada por enlaces entre nodos no adyacentes, que se instalan para mejorar las características del tráfico.

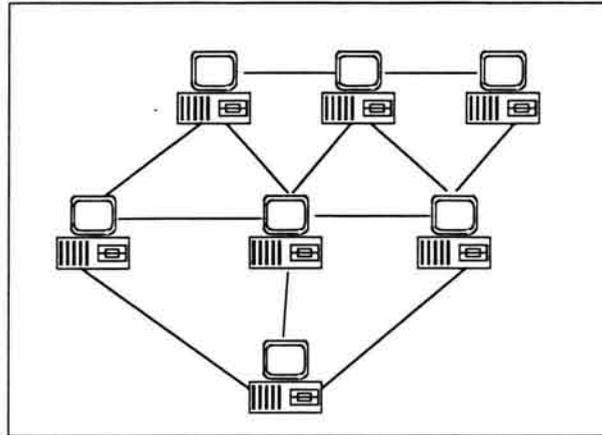


Figura 1.5 Topología en Malla.

Ventajas:

- Posibilita caminos alternativos para la transmisión de datos,
- maneja un grado de confiabilidad demasiado aceptable,
- inmunidad a problemas de fallos y cuellos de botella.

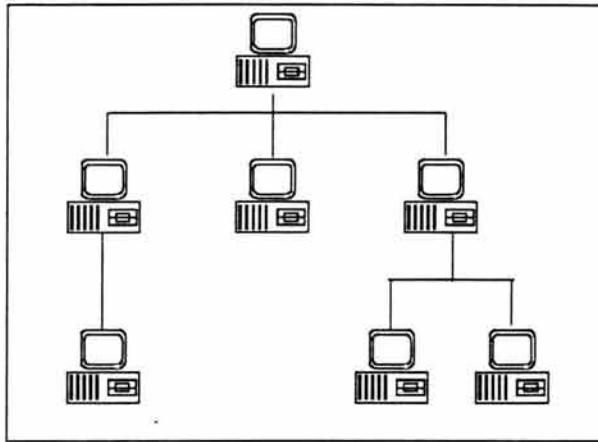
Inconvenientes:

- Baja eficiencia de las conexiones o enlaces, debido a la existencia de enlaces redundantes,
- poco económica debido a la abundancia de cableado,
- control y realización demasiado complejo.

I.3.1.5 Topología en árbol (jerárquica)

La topología en árbol o jerárquica es una de las más utilizadas, el cable se desdobra en varios ramales mediante el empleo de dispositivos de derivación, las transmisiones se propagan por cada ramal de la red y llegan a todas las estaciones, [Figura 1.6].

En la mayor parte de los casos, el nodo principal situado en la raíz de la jerarquía, que típicamente es un computador de altas prestaciones, controla todo el tráfico entre los nodos secundarios.



1.6 Topología en Árbol.

Ventajas:

- Esta topología es interesante especialmente para las redes de banda ancha,
- el “software” para controlar la red es relativamente simple,
- simplicidad de control,
- es muy sencillo añadir nuevos nodos.

Inconvenientes:

- Presenta problemas serios de cuellos de botella,
- en el caso de un fallo en la máquina situada en la raíz, la red queda completamente fuera de servicio, a no ser que otro nodo asuma las funciones del nodo averiado,
- es más difícil su configuración.

1.3.2 Topologías híbridas

Las topologías básicas pueden ser combinadas en una variedad de topologías híbridas más complejas:

- Bus – Estrella.
- Estrella – Anillo.
- Estrella – Estrella.

1.3.2.1 Topología en bus-estrella

Son varias redes de topología estrella unidas con un bus lineal, [Figura 1.7]. Si un computador se cae, éste no afecta el resto de la red. Los otros computadores serían habilitados para continuar comunicándose. Si un concentrador (“hub”) falla, todos los computadores conectados a ese concentrador son incapaces de comunicarse. Si un concentrador es vinculado con otros concentradores, esas conexiones serían rotas.

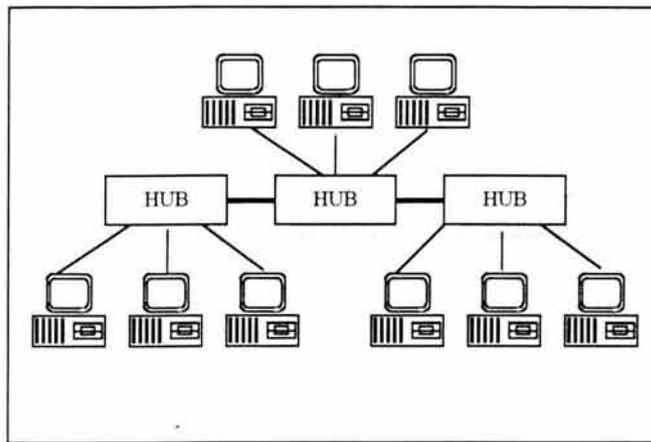


Figura 1.7 Topología en Bus – Estrella.

Ventajas:

- Es más fácil de administrar que el diseño de bus tradicional,
- es más sencilla la localización de problemas en el cableado que en un diseño de bus tradicional,
- dispone de muchas opciones para ampliarla,
- es adecuada para la ampliación en la interconexión a alta velocidad,
- hay disponibles muchos equipos.

Inconvenientes:

- Es susceptible de fallar en un único punto (el concentrador o “hub”),
- al comienzo necesita más cableado de red que una red de bus tradicional.

I.3.2.2 Topología en estrella – anillo

Configuración física de estrella, configuración lógica de anillo, [Figura 1.8]; las estaciones se conectan a través de una unidad de acceso, de tal manera que físicamente forman una estrella, si bien lógicamente constituyen un anillo.

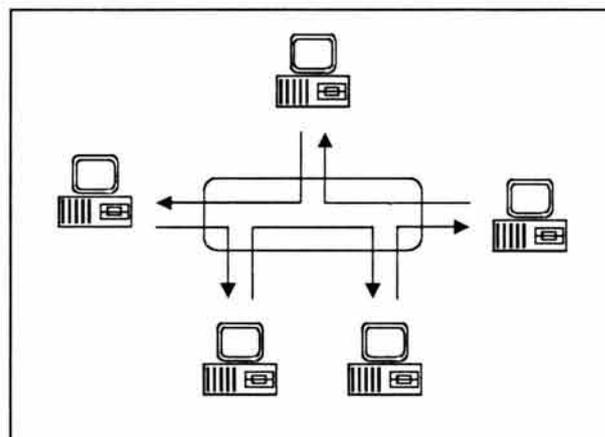


Figura 1.8 Topología en Estrella – Anillo.

En la topología estrella-anillo (algunas veces llamadas estrella cableada anillo) los concentradores son conectados en un modelo estrella por el concentrador principal.

Ventajas:

- Solventa los inconvenientes: de la escasa flexibilidad ofrecida por la topología en anillo en temas de instalación, mantenimiento o reconfiguración,
- puede disponer de varias unidades de acceso en serie.

Inconvenientes:

- En caso de que se averíe una estación de trabajo o un segmento del cable, la unidad de acceso puede cortocircuitar automáticamente esa estación o segmento del cable, de tal forma que el resto del anillo lógico puede permanecer inactivo.

I.3.2.3 Topología en estrella-estrella

Físicamente, la distribución consta de una o varias conexiones en estrella a través de unidades concentradoras (“hubs”), [Figura 1.9]. La estructura lógica puede mantenerse similar a la topología en bus, de tal manera que todas las estaciones accedan al mismo cable, a través de los concentradores.

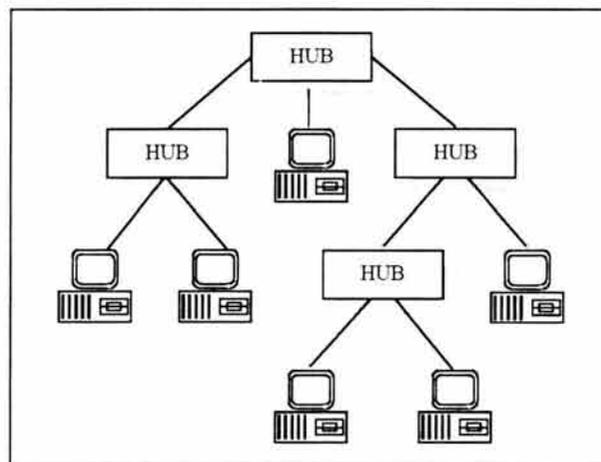


Figura 1.9 Topología Estrella – Estrella.

Ventaja:

- La avería en un segmento afecta normalmente sólo una estación.

Inconveniente:

- Puede afectar a todas las estaciones conectadas a un concentrador.

I.4 Medios de transmisión

De acuerdo a Stallings, W (2000), el medio de transmisión es el camino físico entre el transmisor y el receptor. Los medios de transmisión se clasifican en guiados y no guiados. En ambos casos la comunicación se lleva a cabo con ondas electromagnéticas. Los primeros son aquellos que utilizan un medio sólido (un cable) para la transmisión. Los medios no guiados utilizan el aire para transportar los datos: son los medios inalámbricos.

Las características y calidad de la transmisión están determinadas tanto por el tipo de señal, como por las características del medio. En el caso de los medios guiados, el medio en sí mismo es lo más importante en la determinación de las limitaciones de transmisión. En medios no guiados, el ancho de banda de la señal emitida por la antena es más importante que el propio medio a la hora de determinar las características de la transmisión.

I.4.1 Medios de transmisión guiados

Los tres medios guiados más utilizados para la transmisión de datos son el par trenzado, el cable coaxial y la fibra óptica.

I.4.1.1 Par trenzado

Es el medio guiado más económico y a la vez el más usado, consiste en dos cables de cobre embutidos en un aislante, cruzados en forma de espiral. Cada par de cables constituye sólo un enlace de comunicación. Normalmente se encapsulan varios pares mediante una envoltura protectora. Dependiendo del número de trenzas por unidad de longitud, los cables de par trenzado se clasifican en categorías. A mayor número de trenzas, se obtiene una mayor velocidad de transferencia:

- Categoría 3, hasta 16 Mbps.
- Categoría 4, hasta 20 Mbps.
- Categoría 5, hasta 100 Mbps.
- Categoría 6, hasta 1Gbps.

El par trenzado es mucho menos costoso que cualquier otro medio de transmisión guiado y a la vez es sencillo de manejar. Comparado con la fibra óptica y el cable coaxial está más limitado en términos de velocidad de transmisión y de distancia máxima. Este medio se caracteriza por su gran susceptibilidad a las interferencias y al ruido.

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

- Par trenzado no apantallado (UTP).
- Par trenzado apantallado (STP).

Los cables UTP son los más utilizados debido a su bajo costo y facilidad de instalación. El ruido inducido aumenta en forma considerable el porcentaje de error en la transmisión de datos.

Los cables STP son un tipo de cable blindado, el cual proporciona cierta inmunidad al ruido y permite extender la longitud del cable a instalar, proporciona mejores resultados a velocidades de transmisión bajas, reduce las interferencias y mejora las características de la transmisión. Sin embargo, tiene un costo elevado y al ser más grueso es más complicado de instalar, se utiliza únicamente para instalaciones muy exactas que requieran una calidad de transmisión muy alta.

I.4.1.2 Cable coaxial

Consiste en un conductor cilíndrico externo que rodea otro cable conductor. El conductor interior se mantiene a lo largo del eje mediante una serie de anillos aislantes o bien mediante un material sólido dieléctrico. El conductor exterior se cubre con una funda protectora. Es menos susceptible a interferencias y se puede usar para cubrir mayores distancias, así como para conectar un número mayor de estaciones en una línea compartida.

I.4.1.3 Fibra óptica

Un cable de fibra óptica tiene forma cilíndrica y está formado por tres secciones concéntricas: el núcleo, el revestimiento y la cubierta. El núcleo es la sección más interna, está constituido por una ó varias hebras o fibras muy finas de cristal o plástico. Cada fibra está rodeada por su propio revestimiento, que es otro cristal o plástico con propiedades ópticas distintas a las del núcleo.

La separación entre el núcleo y el revestimiento actúa como un reflector limitando el haz de luz que de otra manera escaparía del núcleo. La capa más exterior que envuelve a uno o varios revestimientos es la cubierta y está hecha de plástico y otros materiales dispuestos en capas para proporcionar protección.

I.4.2 Transmisión inalámbrica

En medios no guiados, tanto la transmisión como la recepción se lleva a cabo mediante antenas. En la transmisión, la antena radia energía electromagnética en el medio (normalmente el aire), y en la recepción la antena capta las ondas electromagnéticas del medio que lo rodea. Básicamente en las transmisiones inalámbricas hay dos tipos de configuraciones:

1. **Direccional:** la antena de transmisión emite la energía electromagnética concentrándola en un haz por lo tanto las antenas de emisión y recepción deben estar perfectamente alineadas.

2. **Omnidireccional:** la antena de transmisión emite en todas las direcciones pudiendo la señal ser recibida en varias direcciones.

I.4.2.1 Microondas

La antena más común en las microondas es la de tipo parabólico. El tamaño típico es de un diámetro de unos 3 metros. Estas ondas de frecuencia mayores a 100 Mhz viajan en línea recta, por lo que, el emisor y receptor deben estar alineados cuidadosamente.

Este tipo de señales son absorbidas por la lluvia y la tierra, por lo cual necesitan repetidoras terrestres o satélites y tienen dificultades para atravesar edificios. Debido a la propia curvatura de la tierra, la distancia entre dos repetidores no debe exceder de unos 80 kilómetros de distancia. Es una forma económica para comunicar dos zonas geográficas mediante dos torres de 100 metros de altura (suficientemente altas) para que sus extremos sean visibles.

Cuando mayor sea la frecuencia utilizada, mayor es el ancho de banda y por tanto, la velocidad de transmisión es mayor.

Por ejemplo: Las bandas de 2.4 Ghz a 2.484 Ghz se usan para transmisiones médicas, científicas e industriales. Las bandas de 902 Mhz a 928 Mhz y 5.725 Ghz a 5.850 Ghz se usan para teléfonos inalámbricos y controles remotos.

I.4.2.2 Satélites

Un satélite de comunicación puede ser pensado como un repetidor de microondas en el cielo, debido a que utiliza microondas de alta frecuencia y demanda una transmisión en línea, así las señales enviadas por un emisor llegan a la estación base (transmisores/receptores terrestres) y después se amplifican y retransmiten para cada estación de la ruta. En seguida, la información se puede proyectar hacia un satélite de comunicación que actúa como un reflector y funciona como un repetidor, las estaciones pueden ubicarse a 36 mil kilómetros en órbita sobre la tierra y a esa distancia tienen la propiedad de mantenerse sobre una misma área, lo cual es muy útil para enviar señales.

Las partes más importantes del satélite son sus "transponders", que se encargan de recibir la señal que viene de la tierra y de repetir la señal de regreso con una frecuencia diferente y sobre un área preprogramada.

El rango de frecuencias óptimo para la transmisión vía satélite está en el intervalo comprendido entre 1 y 10 Ghz. Se han destinado ciertas frecuencias para las transmisiones comerciales.

La banda C fue la primera y ya está saturada, la banda Ku no está saturada pero por su frecuencia es fácilmente interferida por la lluvia, por lo cual se instalan estaciones terrestres extras para darle la vuelta a las tormentas. La banda Ka es la más cara y menos usada y también se perjudica con la lluvia. Existen otras bandas pero son para uso militar. El costo de una transmisión es independiente de la distancia y tienen una tasa de error bajísima.

I.4.2.3 Ondas de radio

Las ondas de radio son omnidireccionales y no necesitan antenas parabólicas, el rango de frecuencias comprendido entre 30 Mhz y 1 GHz es muy adecuado para la difusión simultanea a varios destinos. La transmisión es posible cuando las antenas están alineadas, no produciéndose interferencias entre los transmisores debidas a las reflexiones con la atmósfera. Son capaces de recorrer grandes distancias, incluso atravesando edificios. Su mayor problema son las interferencias entre usuarios.

I.4.2.4 Infrarrojos

Son ondas direccionales incapaces de atravesar objetos sólidos, están diseñadas para transmisiones de corta distancia. Las comunicaciones mediante infrarrojos se llevan a cabo mediante transmisores/receptores (“transceivers”) que modulan luz infrarroja. Los “transceivers” deben estar alineados directamente o mediante la reflexión en una superficie coloreada como puede ser el techo de una habitación.

Las tarjetas de red inalámbricas utilizadas en algunas redes locales emplean esta tecnología: resultan muy cómodas para ordenadores portátiles; sin embargo, su velocidad es inferior a la que se puede conseguir mediante un cable par trenzado. No hay problemas de asignación de frecuencias, ya que en esta banda no se necesitan permisos.

I.5 Concepto de conmutación

Es el proceso que consiste en la interconexión de unidades funcionales, canales de transmisión o circuitos de telecomunicación, [Figura 1.10] por el tiempo necesario para transportar señales. En una red de conmutación los distintos equipos no están conectados entre sí directamente, sino que lo están a través de nodos de conmutación.

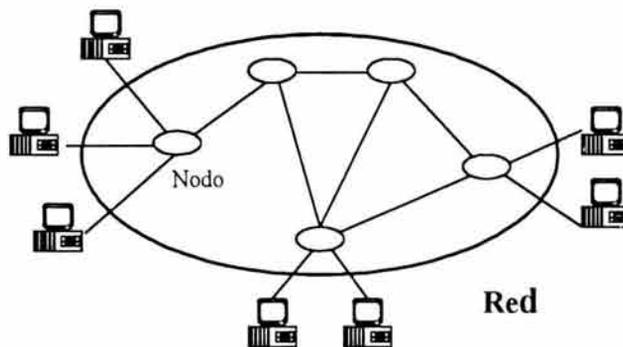


Figura 1.10 Red de conmutación.

Los nodos de conmutación transfieren información de sus entradas a sus salidas, comunicando unas con otras. Estos nodos pueden ser de dos tipos:

1. Nodo de tránsito: son aquellos nodos que no tienen ningún equipo conectado a ellos.
2. Nodo periférico: son aquellos que tienen conectados uno o más equipos terminales.

Si un nodo tiene conectados equipos, y además se comunica con otros nodos, entonces son simultáneamente nodos de tránsito y periféricos. Los nodos pueden llevar a cabo el control de errores y de flujo, además de encaminar (decidir por dónde debe ir un mensaje o un paquete) en algunos casos. La velocidad a la que los nodos procesan la información es muy importante, por lo tanto los nodos de tránsito son más rápidos.

No todos los nodos de conmutación están conectados entre sí. Debe existir por lo menos un camino posible entre dos nodos cualesquiera, y no tiene que ser directo. Por razones de fiabilidad (garantizar el servicio), es recomendable que existan al menos dos caminos.

La clasificación de este tipo de redes se hace en función de la tecnología utilizada por los nodos para conmutar:

- Conmutación de circuitos.
- Conmutación de mensajes.
- Conmutación de paquetes.

I.5.1 Conmutación de circuitos

Se establece un camino físico entre el origen y el destino durante el tiempo que dure la transmisión de datos. Este camino es exclusivo para los dos extremos de la comunicación: no se comparte con otros usuarios (ancho de banda fijo). Las comunicaciones a través de líneas telefónicas analógicas o digitales funcionan mediante conmutación de circuitos.

I.5.2 Conmutación de mensajes

Un mensaje que se transmite por conmutación de mensajes va pasando desde un nodo al siguiente, liberando el tramo anterior en cada paso para que otros puedan utilizarlo y esperando a que el siguiente tramo esté libre para transmitirlo. Esto implica que el camino origen-destino es utilizado de forma simultánea por distintos mensajes. Sin embargo, éste método no es muy útil en la práctica ya que los nodos intermedios necesitarían una elevada memoria temporal para almacenar los mensajes completos.

I.5.3 Conmutación de paquetes

Es la que realmente se utiliza cuando hablamos de redes. Los mensajes se fragmentan en paquetes y cada uno de ellos se envía de forma independiente desde el origen al destino. De esta manera, los nodos ("routers") no necesitan una gran memoria temporal y el tráfico por la red es más fluido. Nos encontramos aquí con una serie de problemas añadidos: la pérdida de un paquete provocará que se descarte el mensaje completo; además, como los paquetes pueden seguir rutas distintas puede darse el caso de que lleguen desordenados al destino. Esta es la forma de transmisión que se utiliza en Internet: los fragmentos de un mensaje van pasando a través de distintas redes hasta llegar al destino.

I.6 Concepto de arquitectura de red

La arquitectura de red es el conjunto de capas, protocolos y servicios que forman parte de una red de telecomunicaciones. Hay dos arquitecturas que han sido determinantes y básicas en el desarrollo de los estándares de comunicación: el conjunto de protocolos TCP/IP y el modelo OSI.

TCP/IP es la arquitectura más adoptada para la interconexión de sistemas, mientras que OSI se ha convertido en el modelo estándar para clasificar las funciones de comunicación.

I.6.1 TCP/IP

TCP/IP fue una de las primeras jerarquías de protocolos originalmente puesto en práctica por el Departamento de Defensa de los Estados Unidos de Norteamérica como un modo de unir los productos de red de varios vendedores. La parte IP proporciona una de las mejores definiciones para la interconexión entre redes y está siendo usada por muchos vendedores como una vía para interconectar áreas locales.

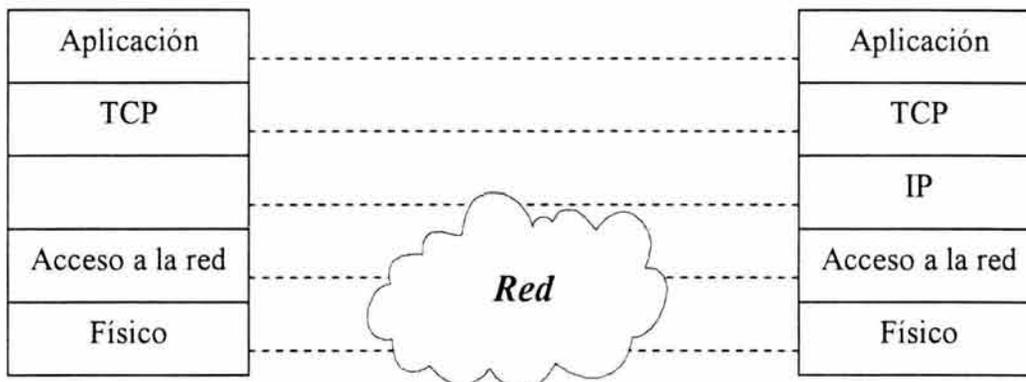


Figura 1.11 Arquitectura TCP/IP.

No hay un modelo oficial de referencia TCP/IP, sin embargo todas las tareas involucradas en la comunicación se pueden organizar en cinco capas, [Figura 1.11]:

Capa física: Es el nivel más bajo, aquí nos referimos al medio físico por el cual se transmite la información. Generalmente será un cable aunque no se descarta cualquier otro medio de transmisión.

Capa de acceso a la red: Determina la manera en que las estaciones de trabajo envían y reciben la información a través del soporte físico proporcionado por la capa anterior. El emisor debe proporcionar a la red la dirección del destino, de tal manera que la red pueda encaminar los datos hasta el destino apropiado.

El emisor puede requerir ciertos servicios, como por ejemplo solicitar una determinada prioridad, que pueden ser proporcionados por el nivel de red. El “software” en particular que se use en esta capa dependerá del tipo de red que se disponga; por ejemplo: Ethernet, Token Ring, entre otros.

Capa de red: Esta capa proporciona el direccionamiento IP y determina la ruta óptima (a través de los ruteadores) que debe seguir un paquete desde el origen al destino. En situaciones en las que los dos dispositivos estén conectados a redes diferentes, se necesitarán una serie de procedimientos que permitan que los datos atraviesen las distintas redes interconectadas. El Protocolo Internet (IP) se utiliza en esta capa para ofrecer el servicio de encaminamiento a través de varias redes. Este sistema se implementa tanto en los sistemas finales como en los ruteadores intermedios.

Capa de transporte: Independientemente de la naturaleza de las aplicaciones que están intercambiando datos, es usual requerir que los datos se intercambien de forma segura, es decir, sería deseable asegurar que todos los datos lleguen a la aplicación destino en el mismo orden en que son enviados. Los procedimientos que garantizan una transmisión segura están localizados en esta capa. El protocolo TCP es el más utilizado para proporcionar esta funcionalidad.

Capa de aplicación: Contiene la lógica necesaria para posibilitar las distintas aplicaciones de usuario, es decir, nos proporciona los distintos servicios de Internet: correo electrónico, páginas web, etcétera.

Las capas física y de acceso a la red proporcionan la interacción entre el servidor, destino y la red mientras que las capas de aplicación y transporte albergan los protocolos denominados “extremo a extremo”, ya que facilitan la interacción entre dos sistemas finales. La capa Internet tiene algo de las dos aproximaciones anteriores. En esta capa, los sistemas origen y destino proporcionan a la red la información necesaria para realizar el encaminamiento, pero a la vez deben proporcionar algunas funciones adicionales de intercambio entre los dos sistemas finales.

1.6.2 Modelo OSI

El modelo de Interconexión de Sistemas Abiertos (OSI) fue un intento de la Organización Internacional de Estándares (ISO) para la creación de un estándar que siguieran los diseñadores de nuevas redes. Se trata de un modelo teórico de referencia: únicamente explica lo que debe hacer cada componente de la red sin entrar en los detalles de implementación. El modelo divide las redes en capas, cada una de estas capas debe tener una función bien definida y relacionarse con sus capas inmediatas mediante interfases.

Esto debe permitir la sustitución de una de las capas sin afectar al resto, siempre y cuando no se varíen las interfases que la relacionan con sus capas superior e inferior. Los creadores del modelo OSI consideraron que era 7 el número de capas que mejor se ajustaba a sus requisitos, [Figura 1.12].

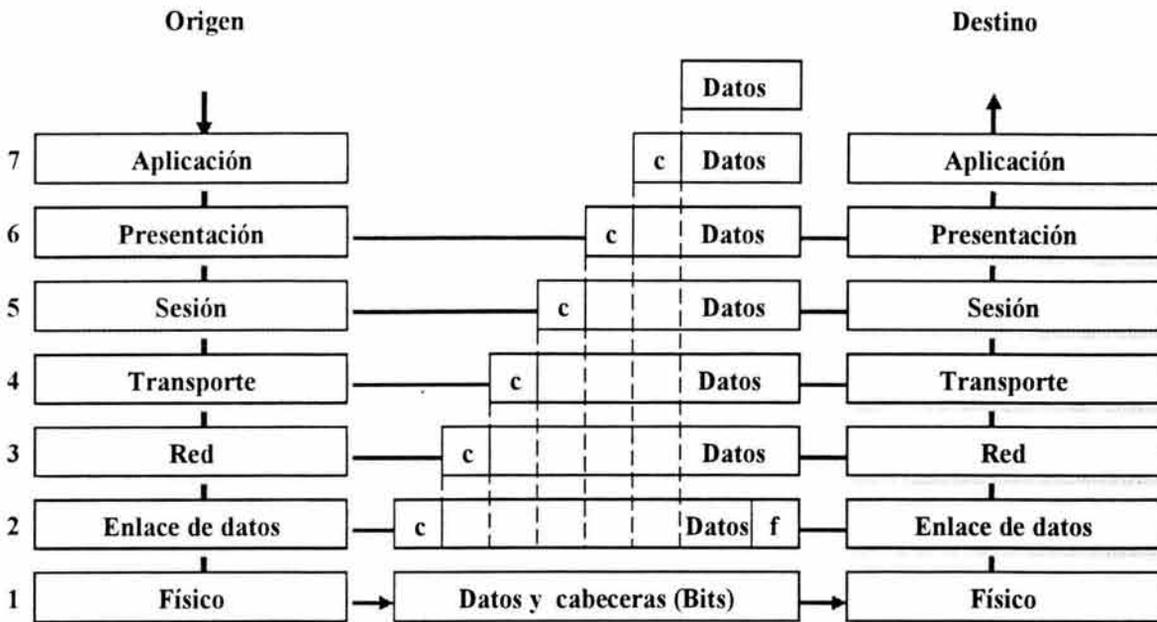


Figura 1.12 Capas del modelo OSI.

Si utilizamos este modelo para enviar datos del servidor origen hacia el servidor destino, los datos van descendiendo de capa en capa hasta llegar a la capa física del servidor origen. Cada capa añade un encabezado (c = cabecera) a los datos que recibe de la capa superior antes de enviárselos a su capa inferior.

En la capa de enlace de datos se ha añadido también una serie de códigos al final de la secuencia (f = final) para delimitar no sólo el comienzo sino también el final de un paquete de datos. La capa física no entiende de datos ni de códigos: únicamente envía una secuencia de bits por el medio de transmisión (un cable).

A medida que se van recibiendo secuencias de bits, se van pasando a las capas superiores. Cada capa elimina su encabezado antes de pasarlo a una capa superior. El mensaje que envía cada capa del servidor origen a su capa inferior es idéntico al que recibe la capa equivalente del servidor destino desde una capa inferior.

Finalmente, los datos llegarán a la capa de aplicación, serán interpretados y recibidos por el servidor destino.

La comunicación realmente se realiza descendiendo capas en el servidor origen, transmitiendo por el medio físico y aumentando capas en el servidor destino. Cada capa añade algo nuevo a la comunicación.

7. Capa de aplicación. Aquí se encuentran los protocolos y programas que utiliza el usuario para sus comunicaciones en red. Esta capa tendrá que ser adaptada para cada tipo de ordenador de forma que sea posible el envío de un correo electrónico (u otros servicios) entre sistemas heterogéneos como Macintosh, Linux o Windows.

6. Capa de presentación. Codifica los datos que recibe de la capa de aplicación a un sistema convenido entre emisor y receptor, con el propósito de que tanto textos como números sean interpretados correctamente. Una posibilidad es codificar los textos según la tabla ASCII y los números en complemento a dos.

5. Capa de sesión. Se encarga de iniciar y finalizar las comunicaciones. Además proporciona servicios mejorados a la capa de transporte como, por ejemplo, la creación de puntos de sincronismo para recuperar transferencias largas fallidas.

4. Capa de transporte. Únicamente se preocupa de la transmisión origen-destino. Podemos ver esta capa como una canalización fiable que une un proceso de un servidor con otro proceso de otro servidor (puede tener varios procesos ejecutándose). No se preocupa del camino intermedio que siguen los fragmentos de los mensajes. Integra control de flujo y control de errores, de forma que los datos lleguen correctamente de un extremo a otro.

3. Capa de red. Se encarga del encaminamiento de paquetes entre el origen y el destino, atravesando tantas redes intermedias como sean necesarias. Los mensajes se fragmentan en paquetes y cada uno de ellos se envía de forma independiente.

Su misión es unificar redes heterogéneas: todos los servidores tendrán un identificador similar a nivel de la capa de red (en Internet son las direcciones IP) independientemente de las redes que tengan en capas inferiores (Token Ring con cable coaxial, Ethernet con cable de fibra óptica, enlace submarino, enlace por ondas, etcétera).

2. Capa de enlace de datos. Envía tramas de datos entre servidores (o ruteadores) de una misma red. Delimita las secuencias de bits que envía a la capa física, escribiendo ciertos códigos al comienzo y al final de cada trama.

1. Capa física. Se encarga de la transmisión de bits por un medio de transmisión, ya sea un medio guiado (un cable) o un medio no guiado (inalámbrico).

Esta capa define, entre otros aspectos, lo que transmite cada hilo de un cable, los tipos de conectores, el voltaje que representa un 1 y el que representa un 0. La capa física será diferente dependiendo del medio de transmisión (cable de fibra óptica, cable par trenzado, enlace vía satélite, etcétera). No interpreta la información que está enviando: sólo transmite ceros y unos.

I.7 Interfases

Las interfases de nivel físico se utilizan para conectar los dispositivos a los circuitos de comunicaciones. Generalmente, los computadores y terminales no están capacitados para transmitir y recibir datos de una red de larga distancia, y para ello están los módem u otros circuitos parecidos. A los terminales y computadores se les llama Equipos Terminales de Datos (DTE) y a los circuitos (módem) de conexión con la red se les llama Equipos de Circuitos de Datos (DCE). Los DCE se encargan de transmitir y recibir bits uno a uno. Los DTE y DCE están comunicados y se pasan tanto datos de información como de control. Para que se puedan comunicar dos DTE hace falta que ambos cooperen y se entiendan con sus respectivos DCE. También es necesario que los dos DCE se entiendan y usen los mismos protocolos.

La interfase entre el DCE y el DTE debe tener una concordancia de especificaciones:

1. Eléctricos: Describen los niveles de tensión (o corriente) y la temporización de los cambios eléctricos que representan los valores binarios 0 y 1 (ambos deben trabajar con los mismos niveles de tensión).
2. Funcionales: Describen las funciones a ser realizadas por la interfase física. Muchos protocolos de nivel físico clasifican esas funciones como control, temporización, datos y tierra, (debe haber concordancia entre los eventos generados por uno y otro circuito).
3. Mecánicos: Describen los conectores y los hilos de interfase. Todos los hilos de control, señalización y datos se encuentran generalmente en un mismo cable y unidos a conectores en ambos extremos del mismo.
4. De procedimiento: Describen la función de los conectores y la secuencia de eventos que es necesario efectuar para la transmisión real de datos por la interfase, (ambos circuitos deben estar conectados con cables y conectores similares).

Existe una gran variedad de interfases físicas en el mercado. En la siguiente tabla se nombran algunas que se utilizan y otras que en su momento fueron usadas.

Serie V	Serie X
V.21	X.1
V.22	X.2
V.23	X.3
V.26	X.4
V.27	X.15
V.32	X.21
V.35	X.50

Tabla 1: Interfases físicas.

Entre otras:

- RS232C/V24: Para transmisiones síncronas o asíncronas, generalmente punto a punto (líneas telefónicas especializadas, unión de terminales a corta distancia).
- RS422A/V11: Permite la transmisión en entornos perturbados o a distancias importantes; también se emplea para uniones multipunto (máximo 10 receptores).
- RS485: De características equivalentes a la anterior, pero mejor adaptada a las redes locales industriales: hasta 32 emisores y otros tantos receptores.
- En el campo del control de procesos industriales, la oferta es también muy rica y jerarquizada.

El conector es el interfase entre el cable y el DTE o el DCE de un sistema de comunicación o entre dos dispositivos intermedios en cualquier parte de la red. En las Redes de Área Extensa la estandarización es muy importante, puesto que hay que garantizar que sea cual sea el fabricante de los equipos, los ordenadores conectados se puedan entender, incluso en el nivel físico.

Algunos de estos conectores son los siguientes:

- RJ11, RJ12, RJ45: Estos conectores se suelen utilizar con cables UTP, STP y con otros cables de pares.
- AUI, DB15: Se utilizan en la formación de topologías en estrella con cables de pares o para la conexión de transeptores a las estaciones.
- BNC: Se utiliza con cable coaxial fino, típico de Ethernet.
- T coaxial: Es el modo natural de conectar una estación en un bus de cable coaxial.
- DB25, DB9: Son conectores utilizados para transmisiones en serie.

I.8 Concepto de protocolo y señalización

Protocolo: Para que una computadora o equipo se entienda con otro equipo, e incluso una red se entienda con otra red, requieren de protocolos, los cuales son un conjunto de convenciones y reglas, que establecen como las computadoras deben comunicarse a través de las redes, reduciendo al mínimo los errores de transmisión. El objetivo del protocolo surgió a raíz de la incompatibilidad entre computadoras y equipos de diversos fabricantes, de allí vino la idea de estandarizar ciertas normas para la comunicación entre equipos de diferentes proveedores y tecnologías.

Un protocolo describe:

- El tiempo relativo al intercambio de mensajes entre dos sistemas de comunicaciones,
- el formato que el mensaje debe tener para que el intercambio entre dos computadoras, se pueda establecer,
- que acciones tomar en caso de producirse errores,
- las suposiciones hechas acerca del medio ambiente en el cual el protocolo será ejecutado.

Diferentes tipos de redes de computadoras se pueden comunicar a pesar de sus diferencias, porque los protocolos de cada una de ellas proveen formas y métodos para la comunicación.

Tipos de protocolos:

De bajo nivel: Son aquellos protocolos los cuales operan en el nivel dos del Modelo OSI, es decir en la capa de enlace y definen como se transmiten las señales por el cable.

De alto nivel: Se les conoce como protocolos de ruteo y operan en el nivel tres de OSI, es decir en la capa de red y definen como se comunican las aplicaciones.

Cuando un usuario envía un mensaje a otro usuario en la red, las reglas de cada nivel del protocolo transforman el mensaje. Cuando el mensaje está preparado para su transmisión y se le ha añadido la dirección, si es largo, puede ser dividido en paquetes más pequeños.

Los protocolos de bajo nivel aseguran que la otra estación de trabajo esté lista para recibir el mensaje, definiendo cómo se puede monitorizar la transmisión por parte de cada estación según pasa por el cable. En la estación receptora los distintos niveles del protocolo definen como reconstruir y desempaquetar el mensaje, y finalmente cómo presentarlo en la pantalla del usuario.

Señalización

La señal se define como la codificación eléctrica o magnética de los datos, la señalización proporciona la información necesaria sobre el emisor y los elementos de la red para poder establecer la conexión o garantizar su correcto funcionamiento. Permite la identificación del servicio solicitado y la selección de la ruta adecuada.

Técnicas de señalización:

Banda base: Es la técnica de señalización más difundida dentro de las redes de computadoras. Es una técnica de señalización digital. Las transmisiones se hacen por impulso, son pulsos discretos, el ancho de banda es utilizada en su totalidad. La comunicación utilizada es bidireccional.

Con las señales digitales eliminamos el problema de la pérdida de calidad, ya que en lugar de amplificadores se emplean repetidores. Los repetidores no se limitan a aumentar la potencia de la señal, sino que decodifican los datos y los codifican de nuevo regenerando la señal en cada salto; idealmente el enlace podría tener longitud infinita.

Banda ancha: La señalización es analógica y se puede representar como una curva ovalada, la comunicación es unidireccional. También necesita de un dispositivo para la regeneración de la señal cuando se llega al límite de distancia, este dispositivo se llama amplificador. El problema principal que presentan señales analógicas es la atenuación con la distancia lo que provocará que se tenga que intercalar una serie de amplificadores. Sin embargo estos amplificadores tienen un problema añadido y es que además de la señal se amplifica el ruido, por lo que cuanto más largo sea el enlace peor será la calidad de la señal en recepción.

I.9 Concepto general de Internet

La primera idea de lo que posteriormente sería Internet surgió en los sesenta por la necesidad militar de comunicarse y por la necesidad científica de compartir investigaciones. Fue en la Agencia de Proyectos Avanzados de Investigación (ARPA) donde surgió Internet, Dwight Eisenhower (1957) creó ARPA para asegurarse de que América no volviera a ser tomada con la guardia baja en la frontera tecnológica.

J.C.R. Licklider (1962) fue a trabajar a ARPA. Licklider, un psicólogo e informático, creía que los ordenadores se podrían utilizar para aumentar el pensamiento humano y sugirió que se estableciera una red de ordenadores para permitir a los investigadores de ARPA comunicar información de modo eficiente.

Licklider no construyó la red que propuso, pero su idea siguió viva cuando dejó ARPA en 1964, en este mismo año la red Internet surgió de la necesidad del gobierno de los Estados Unidos de resolver un problema de estrategia militar, en el periodo de la Guerra Fría (después de la Segunda Guerra Mundial), RAND Corporation, una de las empresas encargadas de la estrategia militar estadounidense propuso la creación de una red de comunicaciones que no dependiera del organismo central, integrado por nodos o puntos de enlace de igual rango y con la misma capacidad de originar, transmitir y recibir mensajes, y en caso de que alguno de los nodos recibiera un ataque o dejara de funcionar, el resto de la red siguiera en operación. Los mensajes de esta red se dividirían en paquetes, cada uno con su propia dirección, originado en algún punto de enlace en particular saltando de lado a lado y finalizando en otro nodo específico, de manera individual. La ruta no importaba, lo único que importaba era que llegaran, si su ruta hubiera sido destruida, el paquete encontraría otra para llegar a su destino.

Sin embargo, la primera experiencia nació en el año 1969, cuando varios científicos del Departamento de Defensa de los Estados Unidos crearon una red de computadoras que permitía transferir información secreta. Aquel invento rudimentario se llamó (ARPANET). Este proyecto fue diseñado con la finalidad de comunicar todos los centros militares para que sobrevivieran a un posible ataque nuclear.

Fue hasta 1972 cuando se comenzó a considerar a Internet como una red de redes. En 1973 tuvo lugar la primera conferencia Internacional de Comunicaciones entre computadoras (presentando ARPANET), con la demostración de 40 computadoras conectadas entre sí alrededor del mundo y sin ninguna pérdida de información, logrando un gran impacto, entonces se formó el Grupo de Trabajo de Redes (INWG) como foro de discusión para crear las bases de una gran red mundial. En 1983 ARPANET se dividió en ARPANET y MILNET, esta última formó la red de la Defensa de Estados Unidos.

Durante la década de 1983 a 1993, Internet pasó de un proyecto de investigación pequeño y experimental a ser la red de computación mas grande del mundo. En estos años el número de redes creció considerablemente, el ritmo de crecimiento al iniciar 1990 fue sorprendente.

Durante 1993 tenía un crecimiento del 20% mensual así Internet ha dejado sus orígenes en bases militares e instituciones gubernamentales para establecerse en escuelas, universidades, centros de investigación, bibliotecas públicas e incluso los sectores comercial e industrial. En la actualidad, Internet es una red de computadoras creada por miles de redes en todo el mundo, vinculadas mediante computadores especiales que pueden traducir información entre sistemas con formato de datos diferentes.

Entre otras cosas Internet ofrece:

- Acceso a vastos recursos de información,
- una manera de conectarse con más de 150 países,
- una manera de conectarse con más de 30 millones de usuarios en el mundo entero,
- un ambiente de cooperación para discutir, compartir ideas e investigar,
- un vínculo relativamente económico para intercambiar gran volumen de información en el mundo entero.

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.

Hoy en día Internet es una infraestructura informática extendida ampliamente, su influencia alcanza no sólo al campo técnico de las comunicaciones entre computadoras (redes), también a toda la sociedad en la medida en que su empleo se incrementa cada vez más para llevar a cabo procesos como el comercio electrónico, la adquisición de información y la interacción entre la comunidad o comunidades remotas.

I.10 Conceptos básicos de la administración de redes

Administración: es el cumplimiento de los objetivos deseados mediante el establecimiento de un medio ambiente favorable a la ejecución por personas que operan en grupos organizados, (Koontz y O'Donnell). Es la combinación más efectiva posible del hombre, materiales, maquinas, métodos y dinero para obtener la realización de los fines de una empresa. (Milliam J. Mclarney)

En sus inicios la administración de redes se concebía como un programa que se cargaba en una estación de alto rendimiento, la cual desplegaba una serie de gráficas útiles para monitorear el funcionamiento de la máquina y en caso de alguna falla emitía una señal de alarma.

El crecimiento de las redes generó la necesidad de un plan completo de control de la red más que un simple programa de computadora, estos programas se siguen utilizando, pero solo como una herramienta de la administración de redes. Sería muy difícil dar una definición precisa de lo que es la administración de redes porque es un proceso que abarca muchas otras actividades; sin embargo, podemos decir que el administrar una red es tomar las medidas necesarias para maximizar la eficiencia y productividad de la misma.

Para el administrador de una Red de Área Local, el término administración se refiere a la habilidad de configurar puertos en los servidores para controlar el acceso a las bases de datos distribuidas, o para dar acceso a los dispositivos compartidos por los usuarios de la red (por ejemplo: impresoras o dispositivos de almacenamiento). En este ambiente el funcionamiento de los servidores es crítico para el trabajo de la red, por lo tanto, deben ser administrados de forma correcta.

Por otro lado, para el administrador de una Red de Área Amplia, el término administración significa hacerse cargo de revisar el funcionamiento de las líneas de comunicación para asegurar la integridad de los datos. En este caso la administración de la red incluye la habilidad de tomar las medidas para restaurar equipos que se encuentren fallando o en su defecto, buscar métodos para evitar las zonas de fallas antes que los problemas degraden el funcionamiento de la red. Y de esta forma podemos localizar diferentes ambientes, donde la administración de la red implicará la ejecución de tareas diferentes.

I.10.1 El administrador de redes

Un administrador de redes será una persona que tenga los conocimientos suficientes para responder a las preguntas de los usuarios y emergencias que puedan producirse. Los servicios del administrador de redes también se pueden contratar con una empresa exterior o puede ser un consultor temporal que informaría a los empleados de la empresa sobre el funcionamiento de la red.

I.10.2 Funciones del administrador

Entre estas funciones está el control de usuarios, garantizar la seguridad, instalación y puesta de las aplicaciones y la realización de copias de seguridad del sistema. El administrador tiene además la responsabilidad de asegurar el funcionamiento eficiente de la red frente a otros usuarios.

I.10.2.1 Proceso para la administración de redes

El responsable del sistema habrá de preparar la forma en que cada usuario tendrá que trabajar con el sistema. También deberá preparar la instalación y el trabajo con el servidor de las aplicaciones “software”. Algunas de ellas podrán ser usadas por todos los usuarios; sin embargo, otras solo podrán ser utilizadas por ciertos usuarios.

I.10.2.2 Documentación del flujo operativo de la red

El supervisor de la red debe tener un registro que incluya toda actividad realizada en el sistema. Gracias a la documentación el administrador de la red podrá localizar rápidamente los recursos de la red y de esta forma el tipo de equipo usado. La documentación puede contener información sobre usuarios del sistema, el “hardware” instalado y el “software” que ejecuta el sistema.

Los registros de usuario son importantes al definir la seguridad del sistema y los registros del “software” son útiles al planificar la estructura de directorios del servidor.

I.10.2.3 Control de los usuarios, los grupos y sus derechos

Control de los usuarios: El administrador de la red estará encargado de dar de alta a cada usuario. Esta tarea consiste en asignar a cada usuario nuevo una palabra de entrada, un texto de entrada y un directorio de usuario especial, entonces se le asigna a cada usuario sus derechos de acceso, según sus necesidades de ingresar a los distintos programas.

Creación de grupos de trabajo: Un grupo es un conjunto de usuarios que tienen los mismos derechos en directorios específicos. Se podrían crear grupos cada vez que un conjunto de usuarios va a compartir los mismos datos o programas, o tienen los mismos requisitos de seguridad. Planificar los grupos por adelantado ayudará a determinar cómo ha de organizarse el sistema, ya que ayudará a determinar quien ha de usar cada aplicación y directorio. Preparar los grupos según el trabajo que han de realizar sus componentes o el nivel del cargo que ocupan ayudará a determinar la seguridad de los accesos que harán al sistema.

Asignación de los derechos: El acceso a los directorios y archivos por parte de los usuarios está limitado por los distintos derechos de acceso que por seguridad establece el administrador del sistema. La seguridad es importante para evitar que los usuarios puedan destruir o dañar importantes archivos de datos, además de permitir que los usuarios tengan la adecuada privacidad y seguridad con sus propios archivos.

I.10.3 Puntos importantes para el administrador de redes

Estrategias ante emergencias: El administrador del sistema ha de elaborar estrategias para el caso de que el servidor de archivos en la red u otros sistemas no pudieran funcionar por alguna razón. El fuego, los problemas eléctricos, las caídas de los equipos, los sabotajes y otras razones pueden hacer que una red deje de funcionar, y con ellas la empresa u organización que depende de ella. El responsable del sistema ha de desarrollar planes para mantener el sistema funcionando, asegurándose la realización de copias de seguridad adecuadas de los datos y que el método para volver a poner la red completamente en funcionamiento esté a punto.

Herramientas de administración de red: Cuando más grande es una red, más difícil resulta de administrar. Hay un amplio rango de utilidades “software” y de dispositivos de análisis disponibles para ayudar al administrador a mejorar las prestaciones de la red, y aislar los problemas. Algunas herramientas para redes sólo son accesibles a un grupo de técnicos, que llegan al lugar donde instalan sus dispositivos de análisis y localizan la fuente de los problemas.

Las herramientas de administración de redes se pueden clasificar de la siguiente forma:

Analizadores de rendimiento de redes: El rendimiento de una red se puede monitorizar y analizar para localizar problemas o cuellos de botellas con la herramienta de análisis adecuada.

Monitorizadores de redes: Las redes también se pueden monitorizar para comprobar su rendimiento, el cual se puede mejorar con pequeños cambios en la configuración.

Herramientas “software” de administración de redes: Estas herramientas pueden ofrecer menús de ayuda adecuados para guiar a los usuarios en ciertas tareas, o pueden asistir al responsable en el diseño de los menús del sistema que hagan operativo el entorno en la red.

Herramientas para la administración de las estaciones de trabajo remotas: Hay distintos productos accesibles que permiten al responsable conectarse con la estación de trabajo del usuario desde su propia estación, y trabajar con el sistema como si estuviera sentado en la estación de trabajo del usuario.

I.10.4 Administración de la configuración de la red

Incluye tanto el control de la configuración actual como el de posibles cambios a futuro. Las tareas de este nivel consisten en la recopilación detallada de toda la información referente a los elementos que conforman la red, tanto de “software” como de “hardware”. Se debe conocer su ubicación, características, números de serie y versiones.

I.10.5 Administración de fallas

Se refiere al proceso de detección, aislamiento, manejo y la eventual solución de las fallas. Este servicio es crítico por el costo que implica tener el sistema fuera de operación. El paso principal de la administración de fallas es detectar errores en la red. Esto puede ser realizado por una variedad de métodos. Por ejemplo: se puede establecer una alarma que se activa al detectar cierto comportamiento en el funcionamiento de la red, en seguida es necesario revisar el lugar donde se generó la alarma para ver si existe o no un problema, la solución de los problemas dependerá de la política establecida por la compañía dueña de la red.

I.10.6 Administración de rendimiento

El rendimiento del sistema envuelve a las tareas que deben ser ejecutadas para evaluar el grado de utilización del equipo de la red, con el objetivo de detectar sobrecargas o cargas muy bajas de trabajo que afecten el buen funcionamiento del sistema. Con la administración del rendimiento se logra eliminar un desbalanceo en las cargas de trabajo entre servidores, grupos de trabajo o sectores de la red. Con un buen análisis el rendimiento de la red puede incrementarse el rendimiento del sistema.

I.10.7 Administración de seguridad

Se encarga de asegurar que sólo personal autorizado haga uso de la red. Las tareas o funciones asociadas son: la identificación de posibles puntos de acceso no autorizado, cifrado de los datos, la administración de las claves para cifrar datos, administración de las claves de acceso y la verificación de la seguridad de las mismas. Se incluyen tareas encaminadas a la prevención de ataques de virus, procesos que garanticen la continuidad de operación y la planeación de sistemas encaminados a recuperar la información en caso de que se presente algún desastre.

I.10.7.1 Organización de la seguridad

Una de las funciones más importantes del administrador es ofrecer seguridad sobre los datos almacenados en el servidor de archivos. No sólo se debe dificultar que un entrometido entre en el servidor, sino que también a aquellos que trabajan con el sistema les debe ser difícil listar los archivos. Otra razón para planificar una correcta seguridad es la amenaza de los virus informáticos.

I.10.7.2 Seguridad de los datos

Comienza con el procedimiento de conexión, a los usuarios se les asigna un nombre de conexión y una palabra clave (“password”) para poder acceder al sistema. Una vez que se ha dado acceso al sistema a un usuario, este necesita un lugar donde trabajar. Se puede crear un directorio especial para cada persona que accede al sistema. Un usuario puede tener acceso sólo a su directorio personal, siendo capaz de ejecutar los programas almacenados en otros directorios.

I.10.7.3 Seguridad del “hardware”

Para que la seguridad de la red sea efectiva, no basta con las medidas relativas al “software”, sino también han de tomarse medidas físicas. El propio servidor de archivos debe de estar fijo en un sitio adecuado y es recomendable tener los sistemas bajo llave para evitar que sean encendidos por personas no autorizadas.

Los usuarios deben desconectarse antes de dejar un equipo solo. Se puede obtener un cierto grado de seguridad a nivel de estaciones de trabajo si se utilizan estaciones sin unidades de disco. Las estaciones sin discos son ideales para la carga de datos y las labores de edición cuando los operadores han de limitarse a trabajar con los archivos del servidor. También es conveniente situar las estaciones de trabajo sin unidades de disco en los puntos con mucho movimiento, o en los que no es posible disponer de personal responsable que controle la actividad de las estaciones de trabajo.

La transmisión de los datos por los cables de la red también puede ser aprovechada por espías. Se pueden interceptar los cables en un punto desconocido por el responsable del sistema. Entonces pueden ser monitorizadas y descifradas las señales que el sistema de cables radia al exterior.

En el primer caso se pueden detectar las intromisiones gracias a un “software” especial que es capaz de señalar las anomalías que se producen en la señal del cable que pueden indicar una interceptación. En el segundo caso, la monitorización de las señales se pueden prevenir usando cables con fibra óptica o codificando la información.

I.10.7.4 Seguridad en conexiones remotas

Una conexión remota es un estación de trabajo alejada, y las posibilidades de intromisión son grandes. Para evitar que un intruso pueda introducirse desde un punto alejado, se puede utilizar un sistema con respuesta, en este sistema un usuario autorizado ha de llamar al sistema principal y colgar.

Para evitar la monitorización de las señales cuando hay conexiones remotas, se pueden utilizar técnicas de codificación de la información. Con este método, los datos quedan codificados antes de la transmisión, cuando se reciben, un algoritmo de decodificación devuelve el archivo a su formato legible. El algoritmo de decodificación sólo estará al alcance del personal autorizado de la información.

* * *

Resumiendo el presente capítulo, una red de computadoras es un conjunto de computadoras, equipos de comunicaciones y otros dispositivos que se pueden comunicar entre sí, a través de un medio en particular.

Las redes son generalmente descritas de acuerdo a su propietario y por las áreas geográficas que cubren, cada una con sus características, tecnologías, velocidades y nichos propios.

Las redes de computadoras están formadas por una amplia variedad de componentes organizados según diversas topologías. Las topologías básicas en las redes locales son las topologías en estrella, en bus, en malla, en árbol y en anillo. Sin embargo, actualmente las topologías más utilizadas son las denominadas híbridas, las cuáles son una mezcla de las anteriores con las que se refuerzan, principalmente, los aspectos de fiabilidad de la red, administración de averías y capacidad de expansión debido a que la organización topológica permite reducir costos, fomentar la fiabilidad y rendimiento y reducir el retardo.

Otro aspecto importante es el medio de transmisión el cual constituye el elemento físico a través del cual se transporta la información. Sus parámetros más significativos a considerar son el ancho de banda, la longitud, la fiabilidad, seguridad, facilidad de instalación y costo.

La arquitectura de red es el conjunto de capas, protocolos y servicios que forman parte de una red de telecomunicaciones. Hay dos arquitecturas que han sido determinantes y básicas en el desarrollo de los estándares de comunicación: el conjunto de protocolos TCP/IP y el modelo OSI.

El modelo OSI, se trata de un modelo teórico de referencia: únicamente explica lo que debe hacer cada componente de la red sin entrar en los detalles de implementación.

Los protocolos Internet se han convertido en una de las familias de protocolos más ampliamente utilizada en el mundo. Están diseñados para facilitar la interconexión de redes de computadoras. Aunque se conocen con el nombre genérico de TCP/IP, los protocolos Internet constan de muchos protocolos diseñados para dar soporte a las operaciones de comunicación entre redes.

Por otro lado, sería muy difícil dar una definición precisa de lo que es la administración de redes porque es un proceso que abarca muchas otras actividades; sin embargo, podemos decir que el administrar una red es tomar las medidas necesarias para maximizar la eficiencia y productividad de la misma.

Una vez, expuestos los conceptos básicos de redes, en el siguiente capítulo se definen con más detalles los conceptos de la conmutación de paquetes, que es la forma de transmisión utilizada cuando hablamos de redes y conmutación de circuitos en su aplicación a la telefonía o redes de voz.

CAPÍTULO 2:

TECNOLOGÍAS DE REDES

II.1 Introducción

Desde la invención del teléfono, la conmutación de circuitos ha sido la tecnología dominante en las comunicaciones de voz., y la conmutación de paquetes es la forma de arquitectura para comunicaciones de datos digitales de larga distancia. X.25 es un estándar para las comunicaciones WAN, que define como se establecen y mantienen las conexiones entre los dispositivos de usuario y los dispositivos de red. Es el protocolo más utilizado y se usa en la conmutación de paquetes.

Frame Relay es una tecnología para Redes de Área Amplia (WAN) que comenzó fundamentalmente como medida para superar la lentitud de X.25, hasta hace relativamente poco tiempo, X.25 se ha venido utilizando como medio de comunicación para datos a través de redes telefónicas con infraestructuras analógicas, en las que la norma ha sido la baja calidad de los medios de transmisión, con una alta tasa de errores. Frame Relay, por el contrario, maximiza la eficacia, aprovechándose para ello de las modernas infraestructuras, de mayor calidad y con muy bajos índices de error, y además permite mayores flujos de información.

Posteriormente aparece la Red Digital de Servicios Integrados que es una red de comunicaciones, digital, de banda estrecha, que evolucionó a partir de la red telefónica y permite conectividad digital de usuario a usuario, proporcionando servicios telefónicos y no telefónicos entre los mismos, a lo largo de este capítulo se explican con mas detalle los conceptos aquí mencionados.

II.2 Conmutación de circuitos

La conmutación de circuitos se usa en redes telefónicas públicas. La técnica de conmutación de circuitos se desarrolló para tráfico de voz aunque también puede administrar tráfico de datos, si bien su uso en este último tipo de aplicaciones resulta en ocasiones ineficiente.

En la conmutación de circuitos se establece un canal de comunicaciones dedicado entre dos estaciones. Se reservan recursos de transmisión y de conmutación de la red para su uso exclusivo en el circuito durante la conexión, una vez establecida parece como si los dispositivos estuviesen directamente conectados, (Stallings, 2002).

II.2.1 Redes conmutadas

Para la transmisión de datos a larga distancia, más allá de un entorno local, la comunicación se realiza generalmente mediante la transmisión de datos desde el origen hasta el destino a través de una red de nodos de conmutación intermedios. El propósito de los nodos de conmutación es proporcionar un servicio de conmutación que posibilite el intercambio de datos entre nodos hasta que alcancen su destino. Los dispositivos finales que desean comunicarse se denominan *estaciones*. Éstas pueden ser computadoras, terminales, teléfonos u otros dispositivos de comunicación.

Los dispositivos de conmutación cuyo objetivo es proporcionar la comunicación se les denomina *nodos*. Los nodos se conectan entre sí mediante enlaces formando una topología dada. Cada estación se conecta a un nodo, llamándose *red de comunicaciones* al conjunto de todos los nodos.

En las redes de comunicación conmutadas los datos que entran a la red procedentes de una estación se encaminan hacia el destino mediante su conmutación de nodo en nodo. Diversas consideraciones se pueden realizar acerca de las redes de comunicación conmutadas:

1. Algunos nodos sólo se conectan con otros nodos, siendo su única tarea la conmutación interna (en la red) de los datos. Otros nodos tienen también conectadas una o más estaciones, de modo que además de sus funciones de conmutación estos nodos aceptan datos desde y hacia las estaciones conectadas a ellos.
2. Los enlaces entre nodos están normalmente multiplexados, utilizándose Multiplexación por División de Frecuencias (FDM) o por División en el Tiempo (TDM).
3. Generalmente, no existe un enlace directo entre cada posible pareja de nodos, siempre resulta deseable tener más de un camino posible a través de la red para cada par de estaciones. Esto mejora la fiabilidad o seguridad de la red.

II.2.2 Redes de conmutación de circuitos

Las comunicaciones mediante la conmutación de circuitos implica la existencia de un camino o canal de comunicaciones dedicado entre dos estaciones, que es una secuencia de enlaces conectados entre nodos de la red. En cada uno de los enlaces físicos se dedica un canal lógico para cada conexión establecida. La comunicación vía la conmutación de circuitos implica tres fases:

1. **Establecimiento del circuito:** Antes de transmitir alguna señal, se establece un circuito extremo a extremo (estación a estación). La estación origen envía una solicitud a los nodos de conmutación intermedios, pidiendo una conexión con la estación destino. Se realiza un "test" con objeto de determinar si la estación destino está ocupada o se encuentra lista para aceptar la conexión.
2. **Transferencia de datos:** Tras el establecimiento del circuito se puede transmitir la información desde el origen hasta el destino a través de la red. Los datos pueden ser analógicos o digitales dependiendo de la naturaleza de la red. Normalmente la conexión es "full-duplex".
3. **Desconexión del circuito:** Tras la fase de transferencia de datos, la conexión finaliza por orden de una de las dos estaciones involucradas. Las señales se deben propagar a los nodos de conmutación intermedios para que éstos liberen los recursos dedicados a la conexión que se cierra.

El canal de conexión se establece antes de que comience la transmisión de datos, por lo que la capacidad del canal se debe reservar entre cada par de nodos en la ruta y cada nodo debe ser capaz de conmutar internamente para administrar la conexión solicitada. Los conmutadores deben contar con la inteligencia necesaria para realizar esta reserva y establecer una ruta a través de la red.

La capacidad del canal se dedica permanentemente a la conexión mientras está se mantiene, incluso si no se transfieren datos. La información se transmite a una velocidad fija sin otro retardo que el de propagación a través de los enlaces de transmisión, siendo despreciable el retardo introducido por cada nodo de la ruta.

La conmutación de circuitos fue desarrollada para el tráfico de voz, el mejor ejemplo conocido de una red de conmutación de circuitos es el de la red telefónica pública, [Figura 2.1] la cual es en la actualidad un conjunto de redes nacionales interconectadas para ofrecer un servicio internacional. Otra aplicación de la conmutación de circuitos son las centralitas privadas (PBX) que se usan para conectar teléfonos dentro de un edificio u oficina.

Una red pública de telecomunicaciones se puede describir a través de los cuatro componentes que forman su arquitectura:

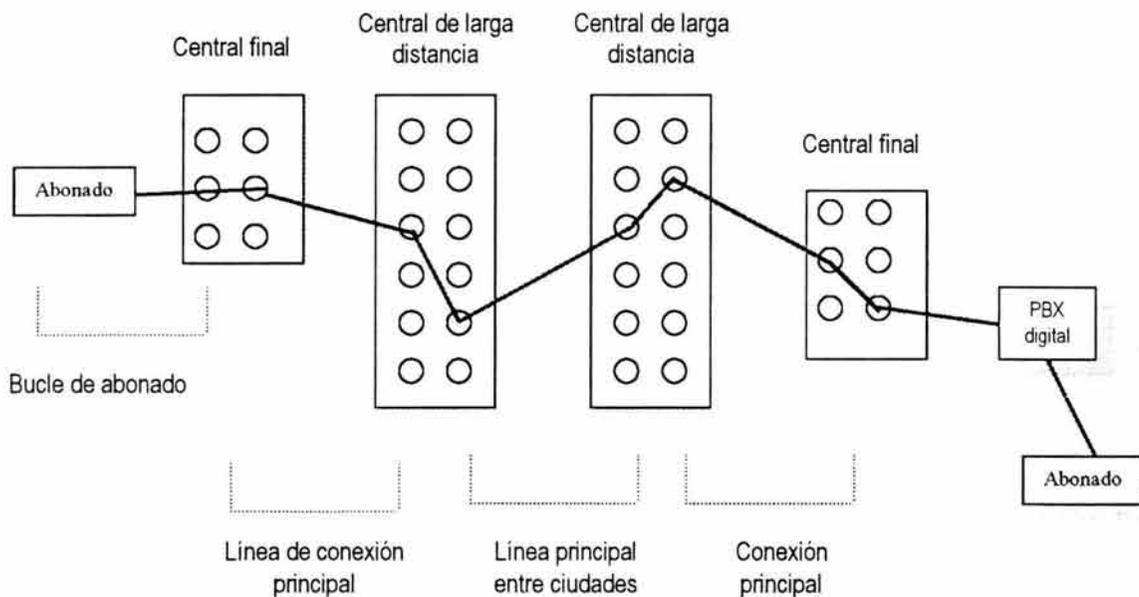


Figura 2.1 Conexión sobre una red pública de conmutación de circuitos.

- **Abonados:** Son los dispositivos que se conectan a la red. La mayoría de los dispositivos de abonado en redes de telecomunicaciones públicas continúan siendo en la actualidad los teléfonos.

- **Bucle local:** Es el enlace entre el abonado y la red, también denominado *bucle de abonado* o *línea de abonado*. En casi todas las conexiones de bucle local se hace uso de cable de par trenzado. La longitud del bucle local está normalmente comprendida en el rango que va desde unos pocos kilómetros hasta varias decenas de ellos.
- **Centrales:** Son los centros de conmutación de la red. Aquellos centros de conmutación a los que se conectan directamente los abonados se denominan centrales finales. Generalmente, una central final da servicio a varios miles de abonados.
- **Líneas principales:** Son los enlaces entre centrales. Las líneas principales transportan varios circuitos de voz haciendo uso de FDM o de TDM síncrona. Al conjunto de estas líneas se le denomina *sistema de transporte*.

Los abonados se conectan directamente a una central final, que conmuta el tráfico entre abonados y entre un abonado y otras centrales de larga distancia. Las otras centrales son responsables de encaminar y conmutar el tráfico entre centrales finales.

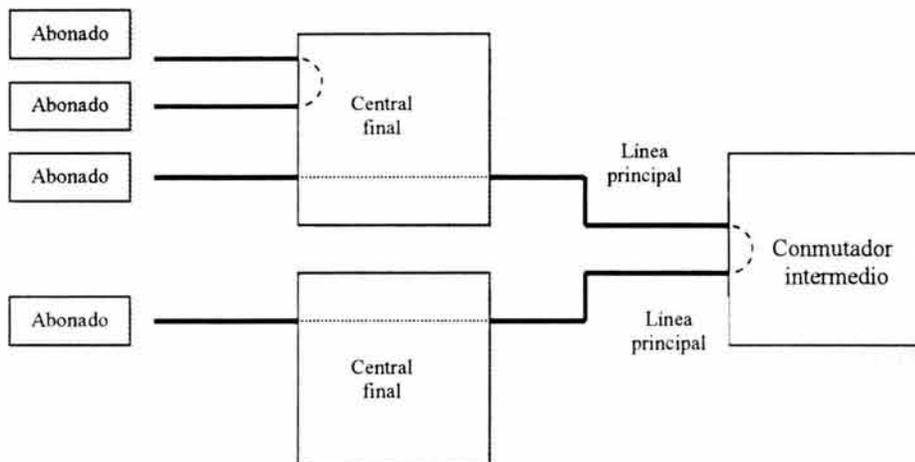


Figura 2.2 Establecimiento de un circuito.

Uno de los aspectos clave del tráfico de voz es que no debe haber prácticamente retardo en la transmisión ni variaciones en el mismo.

Para comunicar entre sí dos abonados que están conectados a la misma central se establece un circuito directo en la central final. Si los abonados están conectados a dos centrales finales diferentes, el circuito establecido entre ellos consistirá en una concatenación de circuitos a través de una o más centrales intermedias, [Figura 2.2].

La velocidad de transmisión de la señal se debe mantener constante, ya que, tanto la emisión como la recepción se realizan a la misma velocidad. Estos requisitos son necesarios para permitir una conversación humana normal.

Una de sus ventajas principales es la transparencia: una vez que se ha establecido el circuito, éste parece una conexión directa entre las dos estaciones conectadas.

II.2.3 Conceptos de conmutación de circuitos

Una red diseñada en torno a un único nodo de conmutación de circuitos consiste en un conjunto de estaciones conectadas a una unidad central de conmutación. El conmutador central establecerá un canal dedicado entre cualesquiera dos dispositivos que deseen comunicarse.

Los elementos de un nodo de conmutación de circuitos son los siguientes, [Figura 2.3]:

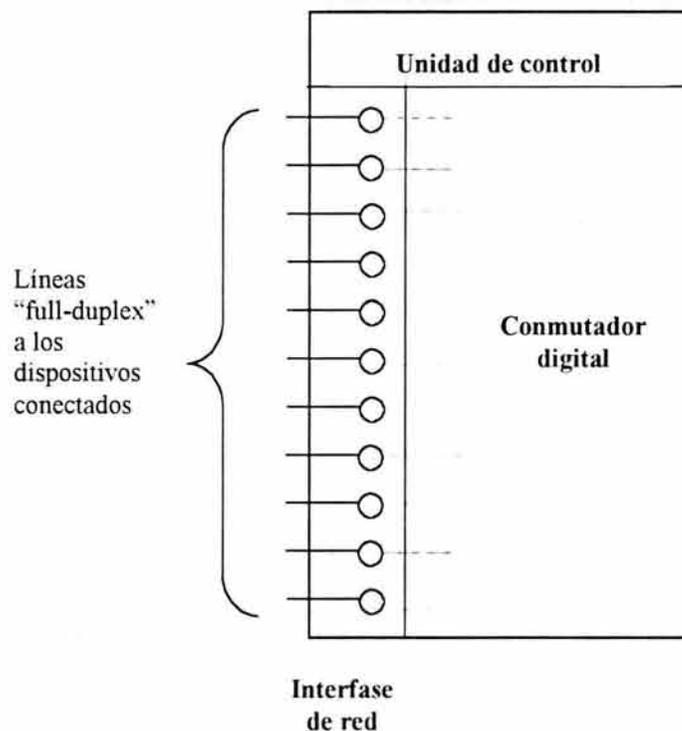


Figura 2.3 Elementos de un nodo de conmutación de circuitos.

Conmutador digital: Es la parte central de todo sistema moderno, cuya función es proporcionar una ruta transparente entre cualesquiera dos dispositivos conectados. El camino es transparente en el sentido de que parece como si existiese una conexión directa entre los dispositivos. Generalmente, la conexión debe permitir transmisión "full-duplex".

Elemento de interfase de red: Incluye las funciones y el “hardware” necesarios para conectar dispositivos digitales, tales como dispositivos de procesamiento de datos y teléfonos digitales, a la red. Los teléfonos analógicos también se pueden conectar si la interfase de red contiene la lógica necesaria para convertir la señal digital. Las líneas principales a otros conmutadores digitales transportan señales TDM y facilitan los canales para la construcción de redes de varios nodos.

Unidad de control: Realiza tres tareas generales. En primer lugar establece conexiones, lo cual se realiza generalmente bajo demanda (es decir, ante la solicitud de un dispositivo conectado a la red). Para establecer la conexión, la unidad de control debe administrar y confirmar la petición, determinar si la estación de destino está libre y construir una ruta a través del conmutador. En segundo lugar, la unidad de control debe mantener la conexión. Dado que el conmutador digital utiliza una aproximación por división de tiempo, esta segunda tarea puede precisar un control continuo de los elementos de conmutación. No obstante, los “bits” de la comunicación se transfieren de forma transparente (desde el punto de vista de los dispositivos del nodo). Por último, la unidad de control debe liberar la conexión, bien en respuesta a una solicitud generada por una de las partes o por razones propias.

Una característica importante de un dispositivo de conmutación de circuitos es si es bloqueante o no bloqueante.

- Una red bloqueante es aquella en la que es posible el bloqueo. El bloqueo ocurre cuando la red no puede conectar dos estaciones debido a que todos los posibles caminos entre ellas están siendo ya utilizados.
- Una red no bloqueante se caracteriza porque permite que todas las estaciones se conectan simultáneamente (por parejas) y garantiza el servicio a todas las solicitudes de conexión posibles siempre que el destino esté libre.

II.2.3.1 Conmutación por división en el espacio

La conmutación por división en el espacio se desarrolló originalmente para entornos analógicos, desplazándose posteriormente al contexto digital. Los principios fundamentales de un conmutador son los mismos si se usa para transportar señales analógicas como para el transporte de señales digitales. Un conmutador por división en el espacio es aquel en el que las rutas de señal que se establecen son físicamente independientes entre sí (divididas en el espacio). Cada conexión necesita el establecimiento de un camino físico a través del conmutador que se dedique únicamente a la transferencia de señales entre los dos extremos. El bloque básico de un conmutador consiste en una matriz de conexiones metálicas (o puntos de cruce) o puertas semiconductoras que una unidad de control puede habilitar o deshabilitar.

En la [Figura 2.4] se muestra una matriz con 10 líneas de entrada/salida “full-duplex”; cada estación se conecta a la matriz a través de una línea de entrada y otra de salida.

La conexión entre cualesquiera dos líneas es posible habilitando el punto de cruce correspondiente. Una matriz de una sola etapa es no bloqueante; es decir, siempre hay un camino disponible para conectar una entrada con una salida.

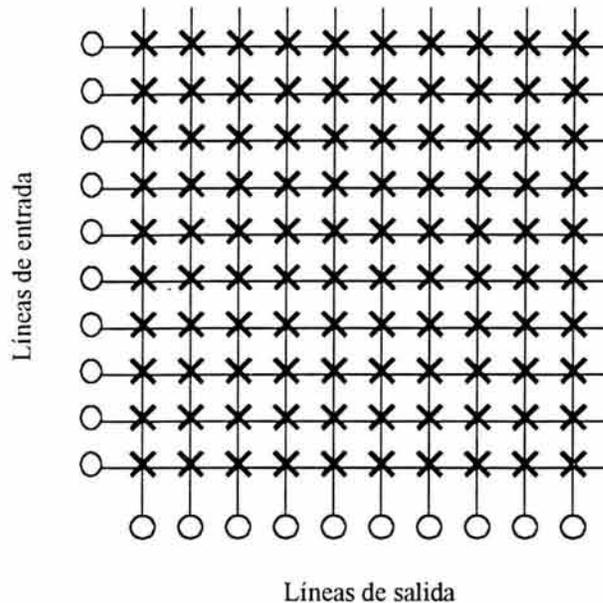


Figura 2.4 Conmutador por división en el espacio de una etapa.

Los conmutadores matriciales presentan varias limitaciones:

- El número de conexiones crece con el cuadrado del número de estaciones conectadas, lo cual resulta costoso para conmutadores grandes.
- La pérdida de un cruce impide la conexión entre los dos dispositivos cuyas líneas interseccionan en ese punto de cruce.
- Las conexiones se utilizan de forma ineficiente; incluso cuando todos los dispositivos conectados se encuentran activos, sólo está ocupada una pequeña fracción de los puntos de cruce.

Para superar estas limitaciones se emplean conmutadores multietapa. Esta solución presenta dos ventajas sobre una matriz de una sola etapa.

- El número de conexiones se reduce, aumentando la utilización de las líneas de cruce.
- Existe más de una ruta a través de la red para conectar dos extremos, incrementándose así la seguridad de la red.

Una red multietapa, [Figura 2.5] necesita un esquema de control más complejo. Para establecer un camino en una red de una etapa sólo se necesita habilitar una única puerta. En una red multietapa se debe determinar una ruta libre a través de las etapas habilitando las puertas correspondientes. Un conmutador por división en el espacio multietapa puede ser bloqueante, pero puede convertirse en no bloqueante aumentando el número o el tamaño de los conmutadores intermedios, si bien ello incrementará el costo.

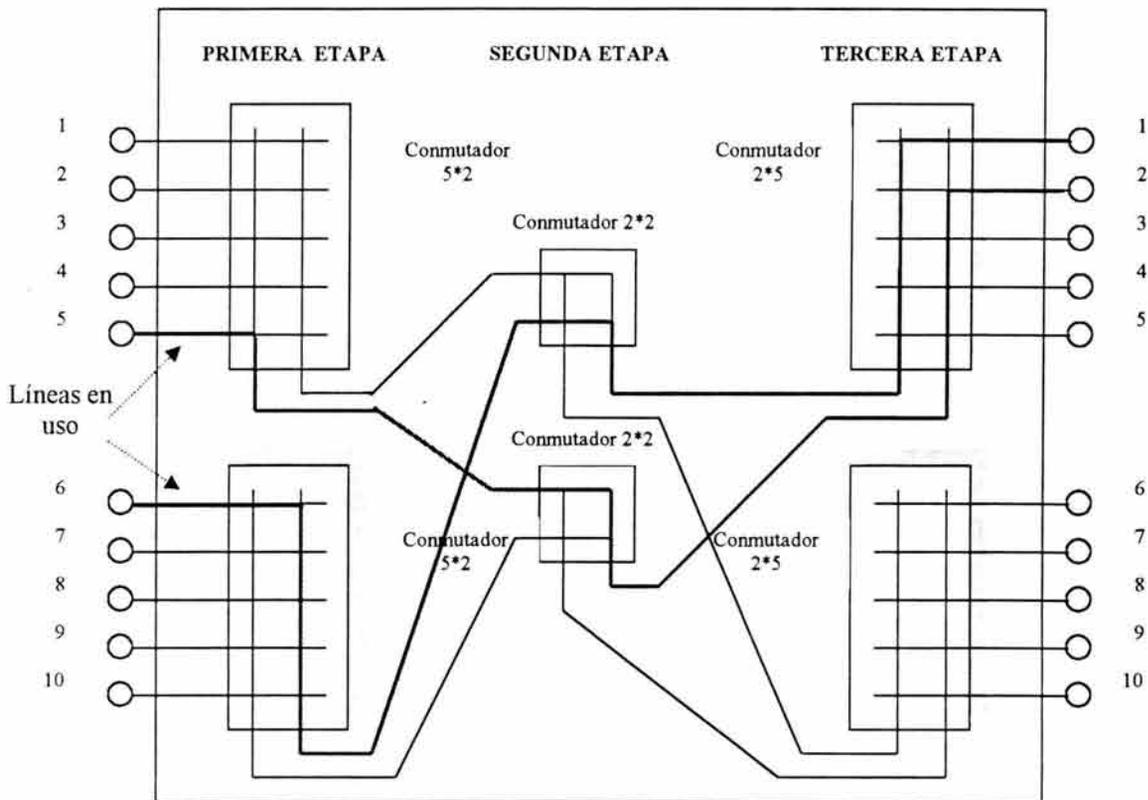


Figura 2.5 Conmutador por división en el espacio de tres etapas.

II.2.3.2 Conmutación por división en el tiempo

La conmutación por división en el tiempo involucra la fragmentación de una cadena de bits de menor velocidad en segmentos que compartirán una secuencia de velocidad superior con otras cadenas de bits. Los fragmentos individuales, o ranuras, se administran por parte de la lógica de control con el fin de encaminar los datos desde la entrada hacia la salida. Existen distintas variantes, una de las más sencillas pero a la vez la más popular:

Conmutación mediante bus TDM, [Figura 2.6]: Todas las técnicas de conmutación digital, se fundamentan en la utilización de la Multiplexación por División en el Tiempo síncrona (TDM). La técnica TDM síncrona permite que varias cadenas de bits de baja velocidad compartan una línea de alta velocidad. Las entradas se muestran por turnos.

Las muestras en serie se organizan en ranuras (canales) para formar una trama recurrente de ranuras, siendo el número de ranuras por trama igual al número de entradas. Una ranura puede ser un bit, un octeto o un bloque de longitud mayor. Una cuestión importante es que con TDM síncrona se conocen el origen y el destino para cada ranura.

Cada dispositivo se conecta al conmutador a través de una línea “full-duplex”.

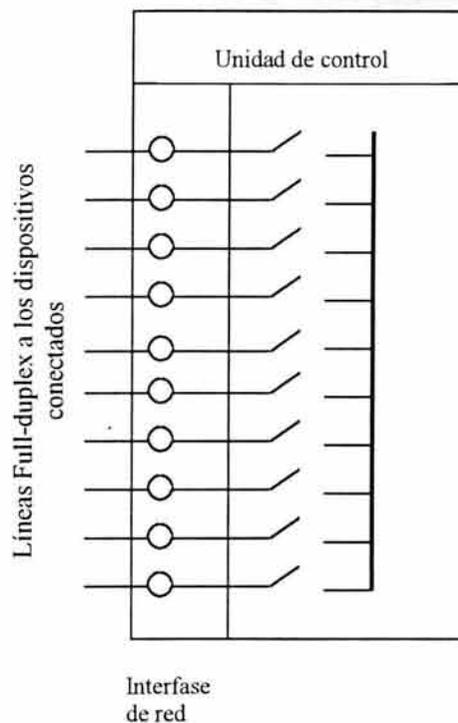


Figura 2.6 Conmutador mediante bus TDM.

Estas líneas se conectan a un bus digital de alta velocidad a través de unas puertas controlables. A cada línea de entrada se le asigna una ranura temporal. La puerta de una línea se encuentra habilitada durante el período de la ranura asociada, permitiendo así que una ráfaga pequeña de datos se dirija hacia el bus.

Durante esa misma ranura se encuentra habilitada también una de las puertas correspondiente a una de las líneas de salida. De este modo, durante esa ranura temporal, los datos se conmutan desde la línea de entrada hasta la línea de salida habilitadas. A través de las sucesivas ranuras se habilitan diferentes parejas de líneas de entrada/salida, permitiendo así numerosas conexiones sobre el bus compartido. Los dispositivos conectados al bus siguen la operación “full-duplex” transmitiendo durante una ranura asignada y recibiendo durante otra. El otro extremo de la conexión es una pareja de entrada/salida para la que estas ranuras temporales tienen justo el significado contrario al anterior.

El conmutador mediante bus TDM es no bloqueante. La asignación de las líneas de entrada puede ser fija, mientras que las de salida varían para permitir distintas conexiones. Cuando comienza una ranura temporal, la línea de entrada designada (habilitada) puede insertar una ráfaga de datos en la línea, sobre la cual se propagará. Durante este tiempo, la línea de salida designada (habilitada) copia los datos, si es que los hay. Por tanto, la duración de la ranura debe ser igual al tiempo de transmisión de la entrada más el retardo de propagación desde la entrada hasta la salida sobre el bus. Para mantener uniforme la duración de las sucesivas ranuras, se define su longitud como el tiempo de transmisión más el retardo de propagación de extremo a extremo en el bus.

Para no perder información de las líneas de entrada, la razón de datos en el bus debe ser suficientemente elevada para que las ranuras completen el ciclo con suficiente rapidez. No hay una asignación fija de líneas de entrada a ranuras temporales, sino que ésta se lleva a cabo bajo demanda. La velocidad de datos del bus establece cuántas conexiones se pueden establecer en un momento dado.

II.2.4 Encaminamiento en redes de conmutación de circuitos

Existen dos requisitos fundamentales para la arquitectura de red que tiene efecto sobre la estrategia de encaminamiento:

1. **Eficiencia:** Es deseable minimizar la cantidad de equipos (conmutadores y enlaces) en la red teniendo en cuenta que debe ser capaz de aceptar toda la carga esperada. Las necesidades de carga se expresan usualmente en términos de tráfico en horas pico. Esto es la carga promedio esperada durante los periodos de más actividad a lo largo del día. Desde el punto de vista de costos, sería deseable administrar esta carga con el menor equipamiento posible.

2. **Flexibilidad:** Es otro requisito y aunque la red se puede dimensionar teniendo en cuenta el tráfico en horas pico, es posible que la carga supere temporalmente este nivel. Puede darse también el caso de que, ocasionalmente, los conmutadores y las líneas fallen y se encuentren momentáneamente inaccesibles. Sería deseable por tanto que la red proporcionase un nivel razonable de servicio incluso bajo tales circunstancias.

El punto clave de diseño que determina la naturaleza del compromiso entre eficiencia y flexibilidad es la estrategia de encaminamiento:

Aproximación estática: Los conmutadores de una red se organizaban en una estructura de árbol o jerarquía, se establecía una ruta a través del árbol comenzando en el abonado llamante hasta el primer nodo común, y después hasta el abonado llamado. Para proporcionar cierta flexibilidad a la red, se incluían en el árbol enlaces de alta capacidad adicionales para conectar entre sí centrales con altos volúmenes de tráfico. La incorporación de enlaces de alta capacidad proporciona redundancia y una capacidad extra, pero persisten las limitaciones en términos de eficiencia y de flexibilidad.

Aproximación dinámica: Para hacer frente a la creciente demanda de las redes de telecomunicaciones públicas, los proveedores han pasado de una aproximación jerárquica estática a la adopción de una aproximación dinámica. En una aproximación de encaminamiento dinámica las decisiones de encaminamiento están influenciadas en cada instante de tiempo por las condiciones de tráfico actuales. Generalmente, los nodos de conmutación de circuitos mantienen toda relación de igual a igual entre sí. Todos los nodos están capacitados para realizar las mismas funciones. Esta arquitectura de encaminamiento es más compleja y a la vez, más flexible. Más compleja porque la arquitectura no proporciona una ruta natural o conjunto de rutas basándose en la estructura jerárquica. Pero al mismo tiempo es más flexible debido a que hay más rutas alternativas.

Encaminamiento alternativo: Las posibles rutas entre dos centrales finales se encuentran predefinidas. Es responsabilidad del conmutador origen seleccionar el camino adecuado para cada llamada. Cada conmutador dispone de un conjunto de rutas prefijas en orden de preferencia para cada destino. Si existe una conexión directa entre dos conmutadores, ésta suele ser la elección preferida. Si no está disponible esta línea se prueba con la segunda alternativa, y así sucesivamente. Las secuencias de encaminamiento (conjunto de rutas intentadas) reflejan un análisis basado en patrones de tráfico conocidos y se diseñan para optimizar la utilización de recursos de la red. Sólo se define una secuencia de encaminamiento para cada pareja origen-destino, el esquema se conoce como esquema de encaminamiento alternativo fijo.

Encaminamiento alternativo dinámico: En este caso se utiliza un conjunto diferente de rutas preplanificadas en instantes distintos de tiempo con objeto de aprovechar las distintas condiciones de tráfico en las diferentes zonas horarias y en los distintos periodos en un día. Por tanto, la decisión de encaminamiento se basa tanto en el estado del tráfico actual (una ruta se descartará si está ocupada) como en patrones de tráfico conocidos (que determinan la secuencia de rutas a considerar).

II.2.5 Señalización de control

En las redes de conmutación de circuitos, las señales de control constituyen el medio mediante el que se administra la red y por el que se establecen, mantienen y finalizan las llamadas. Tanto la administración de las llamadas como la administración de la red necesitan que se intercambie información entre el abonado y los conmutadores, entre los conmutadores entre sí y entre los conmutadores y el centro de administración de red.

II.2.5.1 Funciones de señalización

Las señales de control afectan varios aspectos relativos al funcionamiento de la red, incluyendo tanto los servicios de la red visibles por el abonado como los procedimientos internos. A medida que la red se hace más compleja, crece necesariamente el número de funciones que se realizan a través de la señalización de control. Entre las funciones más importantes de encuentran las siguientes:

1. Comunicación audible con el abonado, que incluye el tono de marcar, el tono de llamada, la señal de ocupado, etcétera.
2. Transmisión del número marcado a las centrales de conmutación, que tratarán de establecer una conexión.
3. Transmisión de información entre los conmutadores indicando que una llamada dada no se puede establecer.
4. Transmisión de información entre conmutadores indicando que una llamada ha finalizado y que la ruta puede desconectarse.
5. Generación de la señal que hace que el teléfono suene.
6. Transmisión de información con fines de tarificación.

7. Transmisión de información indicando el estado de los equipos y líneas principales de la red. Esta información se puede emplear con fines de encaminamiento y mantenimiento.
8. Transmisión de información, utilizada para el diagnóstico y aislamiento de fallos en el sistema.
9. Control de equipos especiales tales como equipos para canales vía satélite.

Ejemplo del empleo de la señalización de control (secuencia de conexión telefónica típica desde una línea a otra en la misma central):

1. Ambos teléfonos deben estar libres (colgados) antes de la llamada. Ésta empieza cuando uno de los abonados toma el auricular (descuelga), lo cual se indica automáticamente al conmutador de la central final a la que está conectado.
2. El conmutador responde con un tono audible de marcar, señalizando al abonado que puede marcar el número deseado.
3. El abonado llamante marca el número, lo cual se comunica al conmutador como la dirección del abonado destino.
4. Si el abonado llamado no está ocupado, el conmutador lo alerta acerca de la llamada entrante enviando una señal de llamada que provoca que el teléfono suene.
5. El conmutador proporciona realimentación al abonado llamante.
 - a) Si el abonado destino no está ocupado, el conmutador devuelve un tono audible de llamada al abonado origen mientras que simultáneamente se envía la señal de llamada al abonado llamado.
 - b) Si el destino está ocupado, el conmutador envía una señal audible de ocupado al llamante.
 - c) Si la llamada no puede establecerse a través del conmutador, éste envía un mensaje audible de "reintento" al abonado llamante.
6. El destino acepta la llamada levantando el auricular (descolgando) lo que se comunica automáticamente al conmutador.
7. El conmutador corta la señal y el tono de llamada estableciendo una conexión entre los dos abonados.
8. La conexión se libera cuando una de las dos partes cuelga.

Cuando el abonado llamado está conectado a un conmutador diferente al que está conectado el abonado origen, son necesarias las siguientes funciones de señalización en los enlaces que unen dos conmutadores.

1. El conmutador origen ocupa un enlace libre entre ambos conmutadores, envía una indicación de descolgar a través del enlace y solicita un registro al otro conmutador para comunicar la dirección destino.
2. El conmutador final envía una señal de descolgar seguida por una de colgar, conocida como "parpadeo" o "guiño". Esto indica que el registro está preparado.
3. El conmutador origen envía los dígitos de la dirección al conmutador final.

II.2.5.2 Localización de la señalización

Es necesario considerar la señalización de control en dos contextos: La señalización entre el abonado y la red y la señalización dentro de la red. La señalización funciona de forma diferente en estos dos contextos.

La señalización entre un teléfono, o cualquier otro dispositivo de abonado, y la oficina de conmutación a la que se encuentra conectado se determina, en gran medida, por las características del dispositivo a intercambios entre computadoras. Esta señalización interna no se ocupa sólo de la administración de llamadas del abonado, sino también de la administración de la propia red. Así, para la señalización interna se necesita un conjunto de órdenes, respuestas y parámetros más complejos.

Dado que se utilizan dos técnicas de señalización diferentes, la central de conmutación a la que esta conectado el abonado debe proporcionar una correspondencia entre la técnica de señalización relativamente poco compleja usada por el abonado y la técnica de mayor complejidad utilizada internamente en la red.

II.2.5.3 Señalización por canal común

La señalización de control tradicional en redes de conmutación de circuitos se ha realizado a través de la propia línea principal o intracanal.

Señalización intracanal, [Figura 2.7]: En esta técnica se usa el mismo canal para transportar tanto las señales de control como la llamada. Esta señalización comienza en el abonado origen y sigue la misma ruta que la llamada. Tiene la ventaja de que los recursos para transmisión de voz son compartidos por la señalización de control.

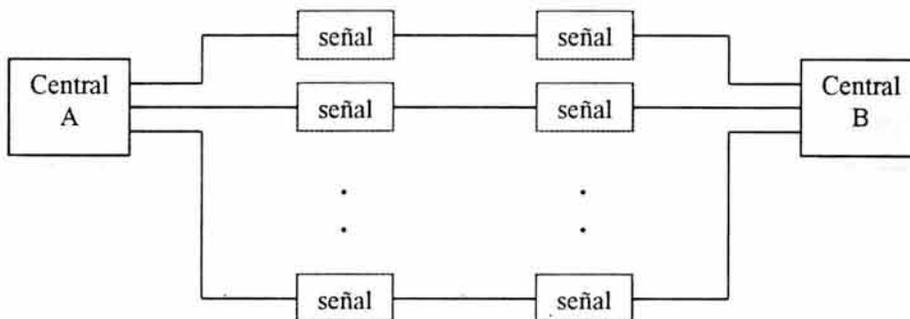


Figura 2.7 Señalización intracanal.

Las señales de control de un conmutador dado se generan en un procesador de control y posteriormente se conmutan sobre el canal de salida correspondiente. En el receptor, las señales de control se deben conmutar desde el canal de voz al procesador de control.

Existen dos formas de señalización intracanal:

1. *Señalización intrabanda:* Utiliza el mismo camino físico que la llamada a la que sirve, usa también la misma banda de frecuencias que la señales de voz que se transmiten. Esta técnica de señalización presenta varias ventajas: Dado que las señales de control tienen las mismas propiedades electromagnéticas que las señales de voz, pueden llegar a los mismos lugares. No existe limitación alguna para el uso de la señalización intrabanda en cualquier punto de la red.

Es posible establecer una llamada sobre un canal de voz con errores ya que las señales de control usadas en el establecimiento de la ruta tendrían que seguir el mismo camino.

2. *Señalización fuera de banda:* Aprovecha que las señales de voz no utilizan completamente los 4 KHz de ancho de banda reservado para ellas, dentro de los 4 KHz se hace uso de una banda de señalización estrecha e independiente para el envío de las señales de control. La principal ventaja radica en que las señales de control se pueden enviar tanto si hay como si no señales de voz en la línea permitiéndose así la supervisión y el control continuo de la llamada.

Las desventajas que presenta la señalización intracanal son las siguientes: la velocidad de transferencia de información se encuentra bastante limitada, el retardo existente desde que un abonado introduce una dirección (marcar el número) hasta que la conexión se establece, ambos problemas se pueden evitar mediante la señalización por canal común.

Señalización por canal común, [Figura 2.8]: Las señales de control se transmiten por rutas completamente independientes de los canales de voz. Una ruta independiente para las señales de control puede transportar las señales de varios canales de abonado, siendo en consecuencia un canal de control común para todos estos canales de abonado.

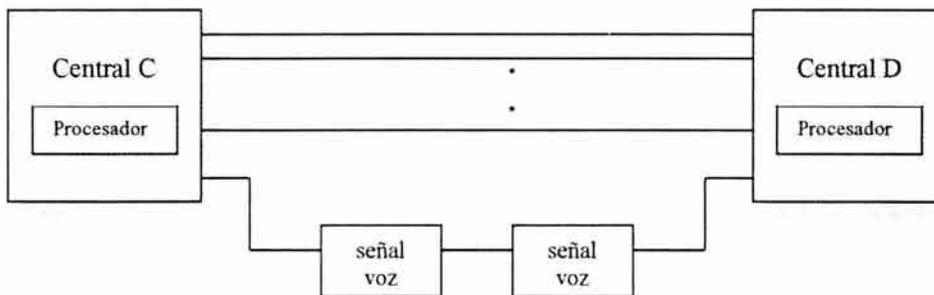


Figura 2.8 Señalización por canal común.

Las señales de control se transfieren directamente desde un procesador al siguiente, sin ser asociadas a un canal de voz, este procedimiento es el más sencillo y el menos susceptible a interferencias entre la señal del abonado y las de control.

Las señales de control son mensajes que se transfieren entre los conmutadores y entre el conmutador y el centro de administración de red.

Existen dos modos de funcionamiento en la señalización por canal común:

1. El modo asociado, [Figura 2.9]: El canal común sigue los pasos, a lo largo de toda la línea, a los grupos de enlace entre conmutadores a los que sirve entre los dos extremos. Las señales de control viajan en canales diferentes a los de las señales de abonado y dentro de un mismo conmutador las señales de control se encaminan directamente hacia un procesador de señales de control.

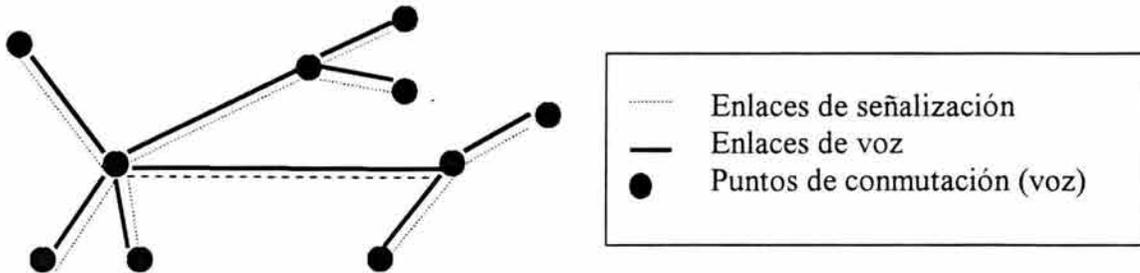


Figura 2.9 Modo de señalización asociado por canal común.

2. Modo no asociado, [Figura 2.10]: Es un modo más complejo, aunque más potente; se hace crecer la red a través de la adición de nodos llamados puntos de transferencia de la señal, no existe una asignación o correspondencia entre los canales de control y los grupos de enlace. En este modo existen dos redes separadas con enlaces entre ellas de modo que la parte de control de la red puede realizar sus funciones a través de los nodos de conmutación que están dando servicio a las llamadas de abonado.

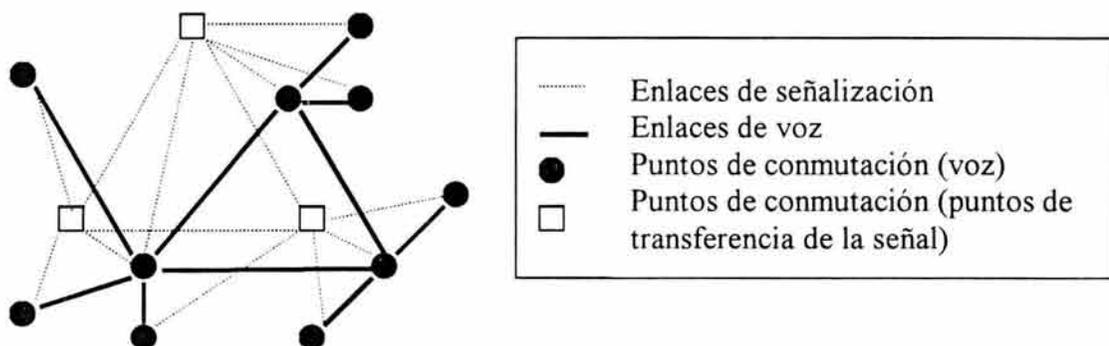


Figura 2.10 Modo de señalización no asociado por canal común.

La administración de la red resulta más fácil en el modo no asociado ya que los canales de control se pueden asignar a tareas de una manera más flexible, además se pueden establecer uno o más puntos centrales de control. Toda la información de control se puede encaminar a un centro de control de red en el que se procesan las solicitudes y se envían las señales de control a los conmutadores que administran el tráfico de los abonados. De esta forma, las solicitudes se pueden procesar teniendo en cuenta una visión más global del estado de la red.

II.2.5.4 Sistema de Señalización Número 7

El esquema más ampliamente usado es el Sistema de Señalización Número 7 (SS7), se ideó con ánimo de ser una norma abierta de señalización por canal común que se pudiera utilizar en diversas redes de conmutación de circuitos digitales. SS7 es el mecanismo que proporciona el control interno y la inteligencia esenciales a una Red Digital de Servicios Integrados (RDSI).

El objetivo de SS7 es proporcionar un sistema de señalización por canal común de propósito general estandarizado internacionalmente con las siguientes características principales:

- Optimizado para su utilización en redes digitales de telecomunicaciones con nodos digitales controlados por programas y que hace uso de canales digitales a 64 Kbps.
- Diseñado para satisfacer las necesidades, tanto actuales como futuras, de transferencia de información para el control de llamadas, control remoto, administración y mantenimiento.
- Diseñado con objetivo de construir un medio seguro para la transferencia de información en el orden correcto sin pérdidas ni duplicaciones.
- Apropiado para su uso en canales analógicos a velocidades inferiores a 64 Kbps.
- Adecuado para enlaces terrestres y satélite punto a punto.

En SS7 los mensajes de control se encaminan a través de la red para llevar a cabo la administración de las llamadas (establecimiento, mantenimiento, terminación) y las funciones relativas a la administración de la red. Estos mensajes son bloques o paquetes pequeños que se pueden encaminar a través de la red, la señalización de control se basa en la tecnología de conmutación de paquetes. De hecho, la red de conmutación de circuitos se recubre por una de conmutación de paquetes para llevar a cabo el control y funcionamiento de la primera.

Elementos de la red de señalización:

SS7 define tres unidades funcionales: puntos de señalización, puntos de transferencia de señal y enlaces de señalización.

- Punto de señalización (SP): Es un nodo de la red de señalización con capacidad de administración de mensajes de control SS7. Los nodos de conmutación de circuitos de la red podrían ser, por ejemplo, los extremos origen o destino de una comunicación o un centro de control de red.
- Punto de transferencia de la señal (STP): Es un punto de señalización capaz de encaminar mensajes de control; es decir, un mensaje recibido sobre un enlace de señalización se transfiere a otro enlace. Un STP podría consistir en un nodo de encaminamiento puro, pudiendo realizar las funciones de un punto final (origen destino) de comunicaciones.

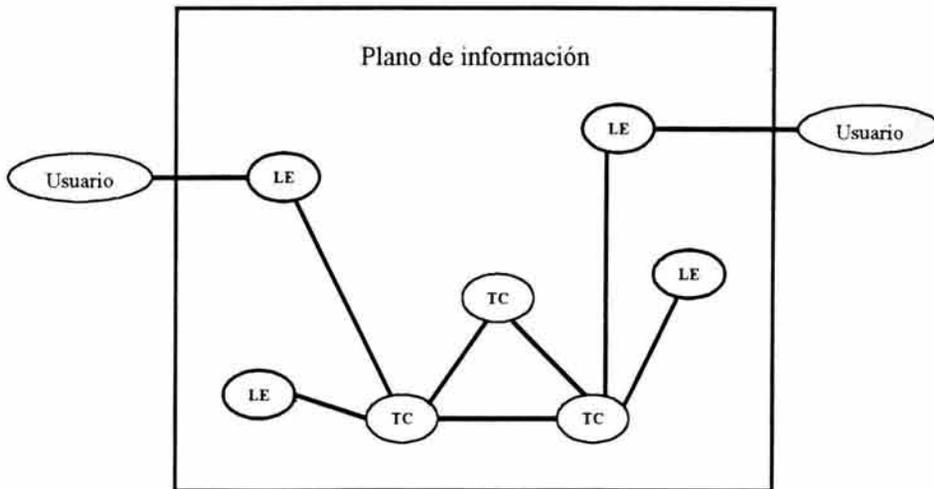


Figura 2.11(b) Puntos de señalización y de transferencia de información en SS7.

Estructuras de la red de señalización

Las redes complejas disponen generalmente tanto de puntos de señalización (SP) como de puntos de transferencia de señal (STP). Una red de señalización que incluye nodos SP y nodos STP puede considerarse que tiene una estructura jerárquica en la que los SP constituyen el nivel inferior y los STP representan el nivel superior. Estos últimos pueden dividirse a su vez en varios niveles STP.

Los parámetros que pueden influir en las decisiones relativas al diseño de la red y al número de niveles a considerar son:

- **Capacidad de los STP:** Incluye el número de enlaces de señalización que puede administrar un STP, el tiempo de transferencia de los mensajes de señalización y la capacidad de mensajes.
- **Prestaciones de la red:** Comprende el número de SP y los retardos de señalización.
- **Eficacia y seguridad:** Mide la capacidad de la red para proveer servicios ante la ocurrencia de fallos en los STP.

Cuando se consideran las restricciones de la red desde el punto de vista de las prestaciones, parece más adecuada la consideración de un solo nivel STP. Sin embargo, la consideración de los parámetros de eficacia y seguridad puede requerir un diseño con más de un nivel. La ITU-T sugiere las siguientes pautas:

- En una red de señalización jerárquica con un único nivel de STP:
 - Cada SP que no sea simultáneamente un STP se conecta con al menos dos STP.
 - El entramado de STP debe ser tan completo como sea posible, entendiendo por entramado completo aquel en el que existe un enlace directo entre cualesquiera dos STP.

- En una red de señalización jerárquica con dos niveles de STP:
 - Cada SP que no sea al mismo tiempo un STP se conecta con al menos dos STP del nivel inferior.
 - Cada STP del nivel inferior se conecta con al menos dos STP del nivel inferior.
 - Los STP del nivel superior forman un entramado completo.

El diseño jerárquico en dos niveles de STP es generalmente tal que el nivel inferior se dedica a la administración del tráfico correspondiente a una región geográfica particular de la red, mientras que el nivel superior administra el tráfico entre regiones.

II.3 Conmutación de paquetes

En 1970 se ideó una nueva forma de arquitectura para comunicaciones de datos digitales de larga distancia: la conmutación de paquetes. Una red de conmutación de paquetes es un conjunto distribuido de nodos de conmutación de paquetes, los cuales, conocen siempre el estado de la red completa. Dado que los nodos están distribuidos, existe un tiempo de retardo entre la producción de un cambio en el estado de una parte de la red y la constatación de dicho cambio por parte de todos los nodos. En la conmutación de paquetes, una estación realiza la transmisión de los datos en base a pequeños bloques llamados paquetes, cada uno de los cuales contiene una parte de los datos de usuario además de información de control necesaria para el adecuado funcionamiento de la red, (Stallings, 2000).

II.3.1 Principios de conmutación de paquetes

Los datos se transmiten en paquetes cortos, siendo 1.000 octetos un límite superior típico de la longitud de los mismos. Si un emisor tiene que enviar un mensaje de mayor longitud, éste se segmenta en una serie de paquetes, [Figura 2.12]. Cada paquete contiene una parte (o todas en el caso de que se trate de un mensaje corto) de los datos de usuario más cierta información de control. Esta información comprende, como mínimo, la información que necesita la red para encaminar el paquete a través de ella y alcanzar el destino deseado. En cada nodo de la ruta, el paquete se recibe, se almacena temporalmente y se envía al siguiente nodo.

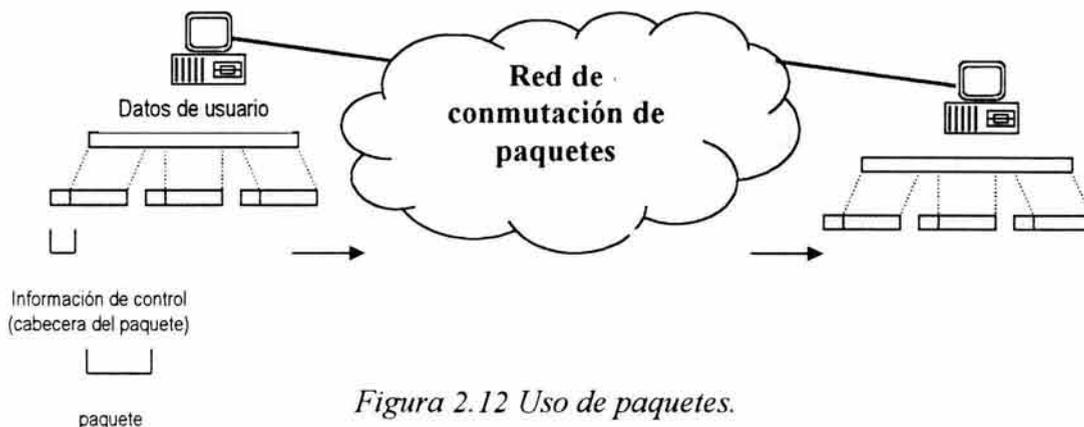


Figura 2.12 Uso de paquetes.

Un único enlace entre dos nodos se puede compartir dinámicamente en el tiempo por varios paquetes. Los paquetes forman una cola y se transmiten sobre el enlace tan rápidamente como es posible. Se puede realizar una conversión en la velocidad de los datos, dos estaciones de diferentes velocidades pueden intercambiar paquetes ya que cada una se conecta a su nodo con su propia velocidad.

Cuando aumenta el tráfico en una red de conmutación de paquetes la aceptación de solicitudes de conexión continua pero aumenta el retardo en la transmisión. Se puede hacer uso de prioridades, de modo que si un nodo tiene varios paquetes en cola para su transmisión, éste puede transmitir primero aquellos con mayor prioridad. Estos paquetes experimentarán así un retardo menor que los de prioridad inferior.

II.3.1.1 Técnicas de conmutación

Si una estación tiene que enviar un mensaje de longitud superior a la del tamaño de paquete permitido a través de una red de conmutación de paquetes, ésta fragmenta el mensaje y los envía, de uno en uno, hacia la red, a través de las siguientes técnicas:

1. Técnica de circuito virtual: Se establece una ruta previa al envío de los paquetes. Primero se envía un paquete especial de control, llamado Petición de Llamada (“Call Request”), solicitando una conexión lógica a la estación destino si esta estación acepta la conexión, envía un paquete Llamada Aceptada (“Call Accept”). Las estaciones origen y destino pueden ya intercambiar datos sobre la ruta establecida. Dado que el camino es fijo mientras dura la conexión lógica y se le llama circuito virtual, además de los datos, cada paquete contiene un identificador de circuito virtual en lugar de una dirección de destino, cada nodo de la ruta preestablecida sabe hacia dónde dirigir los paquetes.

Eventualmente, una de las estaciones finaliza la conexión con un paquete Petición de Liberación (“Clear Request”). Una estación puede disponer en un instante de tiempo dado de más de un circuito virtual hacia otra estación así como de circuitos virtuales a más de una estación.

La principal característica de esta técnica es que la ruta entre las estaciones se establece antes de la transferencia de los datos. Esto no significa que sea una ruta dedicada, con circuitos virtuales el nodo no necesita tomar decisiones de encaminamiento para cada paquete por lo tanto, los paquetes viajan por la red más rápidamente.

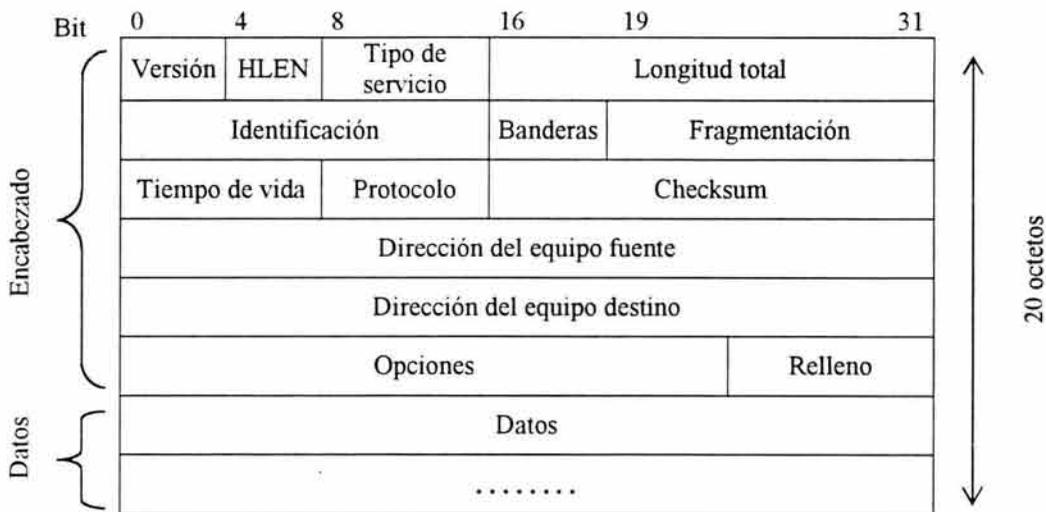
Si dos estaciones desean intercambiar datos durante un periodo de tiempo largo, existen ciertas ventajas al utilizar la técnica de circuitos virtuales. La red puede ofrecer servicios sobre el circuito virtual, incluyendo orden secuencial y control de errores. El orden secuencial hace referencia al hecho de que, dado que los paquetes siguen la misma ruta, éstos se reciben en el mismo orden en que fueron enviados. El control de errores es un servicio que asegura que los paquetes no solo se reciben en orden, sino que además son correctos. Con la utilización de circuitos virtuales, si un nodo falla se perderán todos los circuitos virtuales que atraviesan ese nodo.

2. Técnica de datagrama: Cada paquete se trata de forma independiente, es posible que los paquetes se reciban en el destino en orden distinto al que se enviaron, siendo tarea de esta estación su reordenación.

Una ventaja del empleo de la técnica de datagrama es que no existe la fase de establecimiento de llamada. Si una estación desea enviar solo uno o pocos paquetes, el envío datagrama resultará más rápido.

Otra ventaja es que, dado que es más rudimentario, resulta más flexible. Una tercera ventaja es que el envío datagrama es inherentemente más seguro. En el envío datagrama, si un nodo falla los paquetes siguientes pueden encontrar una ruta alternativa que no atraviese dicho nodo.

Datagrama (“datagram”), [Figura 2.13]: Es un grupo de datos que de manera independiente llevan información suficiente para ser encaminada desde la computadora de origen a una de destino sin que esto dependa de que antes se haya producido tráfico entre ambos y la red que transporta la información.



HLEN = Header length (número de palabras de 32 bits).

Figura 2.13. Formato de un datagrama.

II.3.1.2 Funcionamiento externo e interno

La conexión lógica se denomina usualmente circuito virtual, mientras que el servicio orientado a conexión se conoce como servicio de circuito virtual externo.

Estas decisiones de diseño interno y externo no necesitan ser coincidentes:

- **Circuito virtual externo, circuito virtual interno:** Cuando el usuario solicita un circuito virtual se crea una ruta dedicada a través de la red, de forma que todos los paquetes sigan ese mismo camino.

- **Circuito virtual externo, datagrama interno:** La red administra cada paquete de forma separada de modo que los distintos paquetes correspondientes a un mismo circuito virtual externo pueden seguir rutas diferentes.

No obstante, si es necesario, la red almacena temporalmente los paquetes en el nodo destino con objeto de enviarlos en el orden adecuado hacia la estación destino.

- **Datagrama externo, datagrama interno:** Cada paquete se trata de forma independiente tanto desde el punto de vista del usuario como desde el de la red.
- **Datagrama externo, circuito virtual interno:** El usuario externo no ve conexión alguna, limitándose a enviar paquetes a lo largo del tiempo. En cambio, la red establece una conexión lógica entre estaciones para el envío de paquetes, pudiéndose mantener esta conexión durante un largo periodo de tiempo con objeto de satisfacer futuras necesidades.

Elegir circuitos virtuales o datagramas, tanto interna como externamente, dependerá de los objetivos específicos en el diseño de la red de comunicaciones y de los factores de costo prioritarios.

II.3.2 Encaminamiento

Uno de los aspectos más complejos y cruciales del diseño de redes de conmutación de paquetes es el encaminamiento.

II.3.2.1 Ruteador (“router”)

Es un dispositivo que conecta dos redes locales y es el responsable de controlar el tráfico entre ellas y de clasificarlo, [Figura 2.14]. En sistemas complejos suele ser un filtro de seguridad para prevenir daños en la red local. Es posible conectar varias redes locales de forma que los ordenadores o nodos de cada una de ellas tenga acceso a todos los demás. Estos dispositivos operan en el tercer nivel de red (Capa de Red) del Modelo OSI y enlazan los tres primeros niveles de este modelo.

Los “routers” redirigen paquetes de acuerdo al método entregado por los niveles más altos. Actualmente, son capaces de manejar un protocolo o varios protocolos a la vez. Son también llamados sistemas intermediarios. Originalmente, fueron usados para interconectar múltiples redes corriendo el mismo protocolo de alto nivel (por ejemplo; TCP/IP) con múltiples caminos de transmisión origen/destino, (Martínez, 1997).

Aplicación
 Presentación
 Sesión
 Transporte
Red ←
 Enlace de
 Datos
 Física

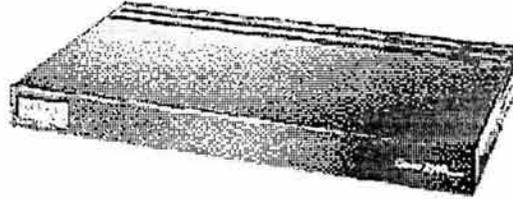


Fig. 2.14 Ruteador marca Cisco serie 2500.

Los ruteadores pueden ser de dos tipos:

1. **Ruteador estáticos:** Estos ruteadores no determinan rutas. En lugar de eso, se debe de configurar la tabla de enrutamiento, especificando las rutas potenciales para los paquetes.
2. **Ruteador dinámicos:** Estos ruteadores tienen la capacidad de determinar rutas (y encontrar la ruta más óptima) basados en la información de los paquetes y en la información obtenida de los otros ruteadores.

II.3.2.2 Características

La función primordial de una red de conmutación de paquetes es aceptar paquetes procedentes de una estación emisora y enviarlos hacia una estación destino. Para ello se debe determinar una ruta o camino a través de la red, siendo posible la existencia de más de uno. Así pues, se debe realizar una función de encaminamiento. Los requisitos de esta función comprenden:

- Exactitud
- Simplicidad
- Estabilidad
- Optimización
- Robustez
- Eficiencia
- Imparcialidad

Las primeras características en la lista se explican por sí mismas. La robustez está relacionada con la habilidad de la red para enviar paquetes de alguna forma ante la aparición de fallos localizados y sobrecargas.

Algunos criterios de funcionamiento pueden dar prioridad al intercambio de paquetes entre estaciones vecinas frente al intercambio realizado entre estaciones distantes, lo cual puede maximizar la eficiencia promedio pero será injusto para aquella estación que necesite comunicarse principalmente con estaciones lejanas.

Una técnica de encaminamiento implica cierto costo de procesamiento en cada nodo y, en ocasiones, también un costo en la transmisión, impidiéndose en ambos casos el funcionamiento eficiente de la red. Este costo debe ser inferior a los beneficios obtenidos tal como la mejora de la robustez o la imparcialidad.

Criterios de funcionamiento: La elección de una ruta se fundamenta generalmente en algún criterio de funcionamiento:

- Criterio de menor número de saltos: Consiste en elegir el camino que atraviesa el menor número de nodos en la red. Éste es un criterio que se puede medir fácilmente y que debería minimizar el consumo de los recursos de la red.
- Criterio de encaminamiento de mínimo costo: En este caso se asocia un costo en cada enlace y se elige aquella ruta a través de la red que implique el costo mínimo.

Instante y lugar de decisión: Las decisiones de encaminamiento se realizan de acuerdo con algún criterio de funcionamiento. Dos cuestiones importantes de esta decisión son el instante temporal y el lugar en que se toma la decisión:

El instante de decisión viene determinado por el hecho de que la decisión de encaminamiento se hace en base a un paquete o a un circuito virtual. Cuando la operación interna de la red es mediante datagramas, la decisión de encaminamiento se toma de forma individual para cada paquete.

En el caso de circuitos virtuales internos, la decisión sólo se realiza en el momento en que se establece un circuito virtual dado, de modo que, en el caso más sencillo, todos los paquetes siguientes que usan ese circuito virtual siguen la misma ruta. El término lugar de decisión hace referencia al nodo o nodos en la red responsables de la decisión de encaminamiento.

Encaminamiento distribuido: Es el más común en el que cada nodo de la red tiene la responsabilidad de seleccionar un enlace de salida sobre el que lleva a cabo el envío de los paquetes a medida que éstos se reciben.

Encaminamiento centralizado: La decisión se toma por parte de algún nodo designado al respecto como puede ser un centro de control de red. El peligro de esta última aproximación es que el fallo del centro de control puede bloquear el funcionamiento de la red.

Encaminamiento del origen: Es la estación origen y no los nodos de la red quien realmente toma la decisión de encaminamiento, comunicándosela a la red. Esto permite al usuario fijar una ruta a través de la red de acuerdo a criterios locales al mismo.

El instante y el lugar de decisión son variables de diseño independientes.

Fuente de información de la red y tiempo de actualización: En el encaminamiento distribuido, en el que la decisión de encaminamiento se toma en cada uno de los nodos, éstos hacen uso de información local como es el costo asociado y los distintos enlaces de salida; también pueden utilizar información de los nodos adyacentes (directamente conectados), tal como la congestión experimentada en cada nodo. Existen algoritmos que permiten al nodo obtener información de todos los nodos de una potencial ruta de interés. En el caso de encaminamiento centralizado, el nodo central hace uso generalmente de información procedente de todos los nodos.

Un concepto relacionado es el tiempo de actualización de la información, el cual es función de la fuente de información y de la estrategia de encaminamiento. Si no se usa información no existe actualización. Si sólo se utiliza información local, la actualización es esencialmente continua ya que un nodo individual conoce siempre sus condiciones locales actuales.

Para el resto de categorías de fuentes de información (nodos adyacentes, todos los nodos), el tiempo de actualización depende de la estrategia de encaminamiento. Para una estrategia de encaminamiento estático la información no se actualiza nunca, mientras que para una técnica adaptable la actualización se lleva a cabo periódicamente a fin de posibilitar la adaptación de la decisión de encaminamiento a las condiciones cambiantes de la red.

Como cabe esperar, cuanto mayor sea la información disponible y más frecuentemente se actualice, más probable será que las decisiones de encaminamiento tomadas por la red sean buenas. Teniendo presente que la transmisión de esta información consumirá recursos de red.

II.3.2.3 Estrategias de encaminamiento

Existen numerosas estrategias para abordar las necesidades de encaminamiento en redes de conmutación de paquetes. Las estrategias principales son: estática, inundaciones, aleatoria y adaptable.

Encaminamiento estático: Se configura una única y permanente ruta para cada par de nodos origen-destino en la red. Las rutas son fijas, o al menos mientras lo sea la topología de la red. Así, los costos de enlace usados para el diseño de las rutas no pueden estar basados en variables dinámicas tales como el tráfico, aunque sí podrían estarlo en tráfico esperado o en capacidad.

En el encaminamiento estático no existe diferencia entre uso de datagramas y circuitos virtuales, ya que todos los paquetes procedentes de un origen dado y con un destino concreto siguen la misma ruta. La ventaja del encaminamiento estático es su simplicidad, además de su buen funcionamiento. Su desventaja radica en la falta de flexibilidad, ya que no reacciona ante fallos ni congestión en la red.

Inundaciones: Un nodo origen envía un paquete a todos sus nodos vecinos, los cuales, a su vez, lo envían sobre todos los enlaces de salida excepto por el que llegó. Dado que eventualmente el nodo destino recibirá varias copias del paquete, éste debe contener un identificador único (por ejemplo, nodo origen o número de circuito virtual y número de secuencia) para que el nodo destino pueda quedarse con una sola copia y descartar el resto.

A menos que se haga algo para cesar las continuas retransmisiones de paquetes, el número de éstos en circulación para un mismo paquete origen crece sin límite. Una forma de prevenir estas retransmisiones consiste en que cada nodo recuerde la identidad de los paquetes que ha retransmitido con anterioridad, de manera que se rechazan copias duplicadas. La técnica más sencilla consiste en incluir un campo de cuenta de saltos en cada paquete. Este contador puede ponerse inicialmente a un valor máximo como es por ejemplo el diámetro de la red (longitud de la ruta más larga de menor número de saltos a través de la red). Cada vez que un nodo transmite un paquete decrementa la cuenta en uno, de modo que cuando el contador alcanza el valor cero se elimina el paquete de la red.

La técnica de inundaciones presenta tres propiedades importantes:

1. Se prueban todos los posibles caminos entre los nodos origen y destino. De este modo, independientemente de lo que pueda sucederle a un nodo o a un enlace, se garantiza la recepción del paquete siempre que exista al menos una ruta entre el origen y el destino.
2. Dado que se prueban todos los caminos, al menos una copia del paquete a recibir en el destino habrá usado una ruta de menor número de saltos.
3. Se visitan todos los nodos que están directa o indirectamente conectados al nodo origen.

La principal desventaja de la técnica de inundaciones es la gran cantidad de tráfico que genera, directamente proporcional a la conectividad de la red.

Encaminamiento aleatorio: En esta técnica, un nodo selecciona un único camino de salida para retransmitir un paquete entrante. El enlace de salida se elige de forma aleatoria, excluyendo el enlace por el que llegó el paquete. Si todos los enlaces son igualmente probables de ser elegidos, una implementación sencilla consistiría en seleccionarlos de forma alternada. Una mejora a esta técnica consiste en asignar una probabilidad a cada uno de los enlaces de salida y llevar a cabo la selección de acuerdo con estas probabilidades.

Encaminamiento adaptable: Las decisiones de encaminamiento cambian en la medida que lo hacen las condiciones de la red. Las principales condiciones que influyen en las decisiones de encaminamiento son:

- Fallos: Cuando un nodo o una línea principal fallan, no pueden volver a ser usados como parte de una ruta.

- Congestión: Cuando una parte de la red sufre una congestión importante, es deseable encaminar a los paquetes de forma que se rodease la zona congestionada en lugar de realizar el encaminamiento a través de ella.

Para hacer posible el encaminamiento adaptable es necesario que los nodos intercambien información acerca del estado de la red.

II.3.3 X.25

Uno de los protocolos estándares más ampliamente usado es X.25, aprobado originalmente en 1976 y sucesivamente modificado desde entonces. El estándar especifica una interfase entre una estación y una red de conmutación de paquetes.

En el estándar se hace referencia a la máquina de usuario como Equipo Terminal de Datos (DTE), y al nodo de conmutación de paquetes al que está conectado el DTE como Equipo Terminal del Circuito de Datos (DCE), (Stalings, 2000).

El estándar especifica tres capas de protocolos, estas tres capas corresponden a las tres capas inferiores del Modelo OSI:

- Capa física: El protocolo de capa física, llamado X.21, especifica la interfase física, eléctrica y de procedimientos entre el "host" y la red.
- Capa de enlace: Se encarga de la transferencia fiable de datos a través del enlace físico mediante la transmisión de datos como una secuencia de tramas. La capa de enlace estándar es el Protocolo Equilibrado de Acceso al Enlace (LAPB).
- Capa de red: Se ocupa de la asignación de direcciones, el control de flujo, la confirmación de entrega, las interrupciones y otras consideraciones relacionadas.

Básicamente, este protocolo permite al usuario establecer circuitos virtuales y después enviar paquetes de hasta 128 bytes a través de ellos. Estos paquetes se entregan en forma confiable y en orden, (Tanenbaum, 1997).

La mayor parte de las redes X.25 trabajan a velocidades de hasta 64 Kbps, lo cual las hace obsoletas para mucho propósitos.

Los datos de usuario se pasan hacia abajo al nivel 3 de X.25, que les añade una cabecera consistente en información de control dando lugar a un paquete. Alternativamente, los datos de usuario se pueden segmentar en varios paquetes. La información de control incluida en el paquete tiene varios objetivos, entre los que se encuentran los siguientes:

1. Identificación de un circuito virtual dado mediante un número al que se asociarán los datos.
2. Definición de números de secuencia para su uso en el control de flujo y errores sobre los circuitos virtuales.

El paquete X.25 completo se pasa después a la entidad LAPB, que añade información de control al principio y al final del paquete, dando lugar a una trama LAPB, [Figura 2.15].

De nuevo, esta información de control en la trama es necesaria para el funcionamiento del protocolo LAPB.

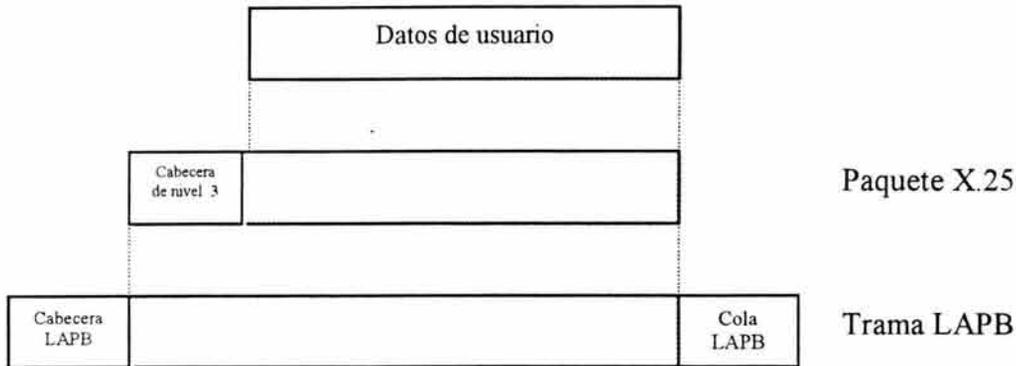


Figura 2.15 Datos de usuario e información de control del protocolo X.25.

II.3.3.1 Servicio de circuito virtual

El servicio de circuito virtual de X.25 ofrece dos tipos de circuitos virtuales:

1. Circuito virtual conmutado: Se crea cuando una computadora envía un paquete a la red y pide que se haga una llamada a una computadora remota. Una vez establecida la conexión los paquetes se pueden enviar por ella y siempre llegarán en orden. X.25 proporciona control de flujo para asegurar que un emisor rápido no pueda abrumar a un receptor lento u ocupado.

2. Circuito virtual permanente: Se usa de la misma forma que uno conmutado pero se establece previamente por un acuerdo entre el cliente y la portadora. La transferencia de los datos se produce con las llamadas virtuales, pero en este caso no se necesita realizar ni el establecimiento ni el cierre de la llamada.

II.3.3.2 Multiplexación

Quizás el servicio más importante ofrecido por X.25 sea la multiplexación. Un DTE puede establecer hasta 4.095 circuitos virtuales simultáneamente con otros DTE sobre un mismo enlace físico DTE-DCE. El DTE puede asignar internamente estos circuitos como mejor le parezca. Cada uno de los circuitos virtuales corresponde, por ejemplo, a una aplicación, a un proceso o a un terminal. La línea DTE-DCE permite multiplexación “full-duplex”, es decir, un paquete asociado a un circuito virtual dado se puede transmitir en ambos sentidos en cualquier instante de tiempo.

II.3.3.3 Control de flujo y de errores

Se hace uso de un protocolo en el que cada paquete incluye un número de secuencia correspondiente al paquete enviado P(S), y un número de secuencia relativo al paquete recibido P(R). Aunque por defecto se utilizan números de secuencia de 3 bits, un DTE puede solicitar, de forma opcional a través del mecanismo de facilidades de usuario, el empleo de números de secuencia de 7 ó de 15bits. El campo P(S) se asigna por parte del DTE a los paquetes salientes de acuerdo con el circuito virtual al que se asocian; es decir, el campo P(S) de cada nuevo paquete de salida sobre un circuito virtual es uno más que el del anterior paquete de ese circuito. El campo P(R) contiene el número del siguiente paquete esperado por el otro extremo de un circuito virtual dado, siendo usado para la confirmación en la técnica de incorporación de confirmaciones (“piggybacking”). Si uno de los extremos no dispone de datos que enviar, puede llevar a cabo la confirmación de los paquetes recibidos mediante los paquetes de control Preparado para Recibir (RR, “Receive Ready”) y No preparado para Recibir (RNR, “Receive Not Ready”). El esquema de control de errores consiste en la técnica ARQ adelante-atrás-N (“go-back-N”). Las confirmaciones negativas se llevan a cabo en forma de paquetes de control Rechazo (REJ, “Reject”), de modo que si un nodo recibe un paquete de este tipo transmitirá el paquete especificado y todos los siguientes.

II.3.3.4 Secuencias de paquetes

X.25 posibilita la identificación de secuencia de paquetes de datos, lo que se conoce como secuencia completa de paquetes. Esta característica presenta varios usos. Uno importante es su empleo en la interconexión de redes para permitir el envío de bloques de datos de tamaño mayor al permitido por la red sin que pierdan su integridad.

II.3.3.5 Reinicio y reenganche

X.25 proporciona dos facilidades para la recuperación de errores. La facilidad de reinicio se usa para reiniciar un circuito virtual, lo que significa que los números de secuencia se hagan igual a cero en ambos extremos y que se pierdan los paquetes de datos o de interrupción en tránsito. Es función de un protocolo de nivel superior la recuperación de los paquetes perdidos. Un reinicio puede estar provocado por diversas condiciones de error tales como la pérdida de paquetes, errores en el número de secuencia, congestión o pérdida de un circuito virtual interno a la red. En este último caso, ambos DCE deben reestablecer el circuito virtual interno para atender al circuito virtual externo aún existente entre los dos DTE. Tanto un DTE como un DCE puede originar un reinicio a través del uso de un paquete Petición de Reinicio (“Reset Request”) o una Indicación de Reinicio (“Reset Confirmation”). Independientemente de quien origine el reinicio, es responsabilidad del DCE involucrado informar al otro extremo. Una situación de error más seria requiere un reenganche. El envío de un paquete de Petición de Reenganche (“Restart Request”) es equivalente a la emisión de un paquete de Petición de Liberación sobre todas las llamadas virtuales y uno de Petición de Reinicio sobre todos los circuitos virtuales. Como antes, tanto el DCE como el DTE pueden iniciar la acción. Un ejemplo de una condición de reenganche consiste en la pérdida temporal del acceso a la red.

II.4 Evolución de los conceptos de redes de datos (de X.25 a Frame Relay)

X.25, la tecnología de conmutación de paquetes más usada, fue introducida a principios de los años 70 en un ambiente caracterizado por líneas analógicas dentro de la red y en la periferia de equipos de usuario (CPE) sin inteligencia. La red permitía altas tasas de error, y los CPE podían realizar solo funciones muy básicas. En tal entorno, los nodos de red tenían la responsabilidad total de asegurar que la información del usuario se entregara fielmente a su destino. Esto requería una gran cantidad de procesamiento en el nivel de red del Modelo OSI, incluyendo funciones tales como control de error y retransmisión.

Retransmisión de Tramas (Frame Relay) es una tecnología nacida de la necesidad de incrementar el ancho de banda, la aparición de impredecibles modelos de tráfico, y de un crecimiento de usuarios que demandan un servicio eficaz. Es un protocolo emergente del protocolo de paquetes X.25. Ambos protocolos, Frame Relay y X.25, están basados en los Sistemas de Interconexión Abiertos (OSI).

De lo contrario a lo que se especulaba, el objetivo de Frame Relay no es reemplazar a X.25, sino dirigirse a las necesidades de ciertas aplicaciones para las cuales X.25 no es efectivo. El principal objetivo de Frame Relay es la interconexión de redes LAN.

II.4.1 Fundamentos

La aproximación tradicional de conmutación de paquetes hace uso de X.25, no sólo determina la interfase usuario-red sino que también afecta al diseño interno de la red. Algunas de las características básicas de X.25 son:

- Los paquetes de control de llamada, usados para el establecimiento y liberación de circuitos virtuales, se transmiten por el mismo canal y circuito virtual que los paquetes de datos, empleándose en consecuencia, una señalización en banda.
- La multiplexación de circuitos virtuales tiene lugar en la capa tres.
- Tanto la capa 2 como la 3 incluyen mecanismos de control de flujo y de errores.

Esta aproximación es muy costosa, ya que en cada salto a través de la red el protocolo de control de enlace intercambia tramas de datos y de confirmación. Además, cada nodo intermedio debe mantener tablas de estado para cada circuito virtual con objeto de abordar aspectos de administración de llamadas y de control de flujo/errores del protocolo X.25.

Este costo queda justificado en caso de que la probabilidad de error en los enlaces de la red sea significativa, por lo que esta técnica puede no ser la más apropiada para los servicios de comunicación digitales modernos dado que las redes actuales hacen uso de tecnologías de transmisión fiables sobre enlaces de transmisión de alta calidad, fibra óptica en muchos de los casos.

Adicionalmente a este hecho, con la utilización de fibra óptica y transmisión digital se pueden conseguir velocidades de transmisión de datos elevadas. En este contexto el costo de X.25 no sólo es innecesario sino que además degrada la utilización efectiva de las altas velocidades de transmisión disponibles.

II.4.2 Concepto de Frame Relay

Frame Relay es un protocolo de transmisión de paquetes de datos en ráfagas de alta velocidad a través de una red digital, fragmentados en unidades de transmisión llamadas "frame". Un paquete es de tamaño fijo y un "frame" es variable en tamaño y puede ser tan largo como mil bytes o más.

Frame Relay requiere una conexión exclusiva durante el periodo de transmisión, esto no es válido para transmisiones de video y audio ya que requieren un flujo constante de transmisiones. Frame Relay es una tecnología de paquete-rápido ya que el chequeo de errores no ocurre en ningún nodo de la transmisión. Los extremos son los responsables del chequeo de errores. Sin embargo, los errores en redes digitales son menos frecuentes en comparación con las redes analógicas.

Una conexión Frame Relay es conocida como una conexión virtual. Una conexión virtual permanente es exclusiva al par origen-destino y puede transmitir por encima de 1.544 Mbps, dependiendo de las capacidades del par origen-destino. Una conexión virtual de intercambio es también posible usando la red pública y puede proporcionar elevados anchos de banda.

II.4.3 Diferencias entre X.25 y Frame Relay

La retransmisión de tramas se ha diseñado para eliminar gran parte del costo que supone X.25 para el sistema final de usuario para la red de conmutación de paquetes. Las principales diferencias entre la técnica de retransmisión de tramas y un servicio convencional de conmutación de paquetes X.25 son:

- La señalización de control de llamadas se transmiten a través de una conexión lógica distinta de la de los datos de usuario. De este modo, los nodos intermedios no necesitan mantener tablas de estado ni procesar mensajes relacionados con el control de llamadas individuales.
- La multiplexación y conmutación de conexiones lógicas tienen lugar en la capa dos en lugar de en la capa tres, eliminándose así una capa completa de procesamiento.
- No existe control de flujo ni de errores a nivel de líneas individuales. Si se lleva a cabo este control, será extremo a extremo y responsabilidad de capas superiores. En retransmisión de tramas sólo se envía una trama de datos de usuario desde el origen hasta el destino, devolviéndose al primero una trama de confirmación generada por una capa superior. En este caso no existe intercambio de tramas de datos y confirmación en cada uno de los enlaces del camino entre el origen y el destino.

El protocolo X.25 usa los niveles uno, dos y tres del Modelo OSI, mientras que el protocolo Frame Relay, usa sólo los dos primeros como se muestra en la siguiente tabla:

	Aplicación	
	Presentación	
	Sesión	
	Transporte	
	Red	
X.25	Enlace	Frame Relay
	Físico	Frame Relay

Tabla 1: Niveles utilizados por Frame Relay y X.25.

Nivel 1: El nivel físico, define la conexión actual entre el terminal y el primer nodo de la red. Este nivel especifica los estándares con la transmisión y recepción de datos mecánica y eléctricamente.

Nivel 2: El nivel de conexión, contiene el protocolo que define el "troceado" de los datos para la transmisión, y establece la ruta que los datos deben seguir a través de la red. Esto significa que los datos son colocados en un "frame" (secuencia específica de bits), que es la unidad fundamental del intercambio de datos. Ambos protocolos, X.25 y Frame Relay, usan estos dos niveles.

Nivel 3: El nivel de red, la unidad fundamental del intercambio de datos es el paquete. El nivel 3, prepara los "frames" de datos del nivel 2 en paquetes y rutas de datos a través de la red por medio de Circuitos Virtuales Permanentes (PVC). El nivel 3 también realiza detección y corrección de errores con peticiones de retransmisión de los "frames" y paquetes dañados. Este es el punto en el que X.25 y Frame Relay divergen. X.25 usa el nivel 3 en su totalidad, mientras que Frame Relay usa esencialmente sólo los niveles 1 y 2.

La razón para esto es que Frame Relay está basado en la premisa de que las redes digitales son mucho menos propensas a errores que las que analógicas que había en el pasado. Esta premisa es debida exactamente al cambio a digital y a la fibra óptica.

Gran parte de las funciones de X.25 se eliminan en Frame Relay. La función de direccionamiento se desplaza desde la capa 3 en X.25 a la capa 2 en Frame Relay, [Tabla 2]. Todas las demás funciones del nivel 3 de X.25 no están incorporadas en el protocolo de Frame Relay.

X.25	Capa	Frame Relay
Establecimiento de circuito Control de circuito Control de flujo de circuito Direccionamiento.	Red	
Control de enlace Creación de tramas Control de errores Control de flujo de enlaces Fiabilidad	Enlace	Direccionamiento Creación de tramas Control de errores Gestión de interfases
Conexión Física	Físico	Conexión Física

Tabla 2: Funciones suministradas por cada uno de los niveles OSI para X.25 y Frame Relay.

En comparación con X.25, la principal desventaja teórica en retransmisión de tramas es que se pierde la posibilidad de llevar a cabo un control de flujo y de errores en cada enlace (aunque la retransmisión de tramas no ofrece control de flujo de errores extremo a extremo, éste se puede implementar fácilmente en una capa superior). En X.25 existen varios circuitos virtuales a través de un mismo enlace físico, permitiendo una transmisión fiable a nivel de enlace desde el origen hacia la red de conmutación de paquetes, y desde ésta hacia el destino. El protocolo de control de enlace proporciona además fiabilidad en cada enlace de la red. Con el uso de la técnica de retransmisión de tramas desaparece dicho control a nivel de enlace, aunque este hecho no supone un gran inconveniente gracias al incremento en la fiabilidad en la transmisión y en los servicios de conmutación.

La ventaja de la retransmisión de tramas es la potencia del proceso de comunicaciones, reduciéndose la funcionalidad del protocolo necesaria en la interfase usuario-red así como el procesamiento interno de red.

En consecuencia, cabe esperar un menor retardo y un mayor rendimiento. Así algunos estudios indican que la mejora en el rendimiento mediante el uso de la técnica de retransmisión de tramas frente a X.25 puede ser un orden de magnitud o más. La recomendación I.233 de ITU-T especifica que la retransmisión de tramas consigue velocidades de acceso de hasta 2 Mbps, (Ocioso.net).

II.5 Evolución de la telefonía digital a RDSI

Desde que A. Graham Bell descubriera el teléfono, las redes analógicas han dominado el panorama de las comunicaciones durante más de un siglo y han resultado adecuadas para la transmisión de voz a través de las redes telefónicas o de imágenes en movimiento mediante la difusión de las señales de TV. Sin embargo, este tipo de redes resultaron inapropiadas para transmitir datos cuando aparecieron los primeros ordenadores digitales, ya que la naturaleza de estas señales no coincidía con la de las redes de comunicaciones existentes. Este requerimiento empujó al desarrollo de los módems (laboratorios Bell, 1958) para realizar la transformación analógico-digital y poder utilizar las redes telefónicas existentes para conectar equipos digitales. Pero la tecnología digital hoy en día ya no sólo se utiliza para transmitir datos informáticos, sino que también ha sido adoptada para la transmisión de voz e incluso de video gracias a las posibilidades que ofrece y a la mayor calidad obtenida.

A causa de las ventajas que ofrecen las tecnologías digitales frente a sus equivalentes analógicas, las tres últimas décadas han estado marcadas por la progresiva digitalización de las redes de comunicaciones que, sucesivamente, han ido sustituyendo tramos enteros de la red analógica: primero fueron las troncales, luego los conmutadores, y finalmente, han sido los bucles de abonado hasta llegar a ser finalmente redes totalmente digitales, [Figura 2.16].

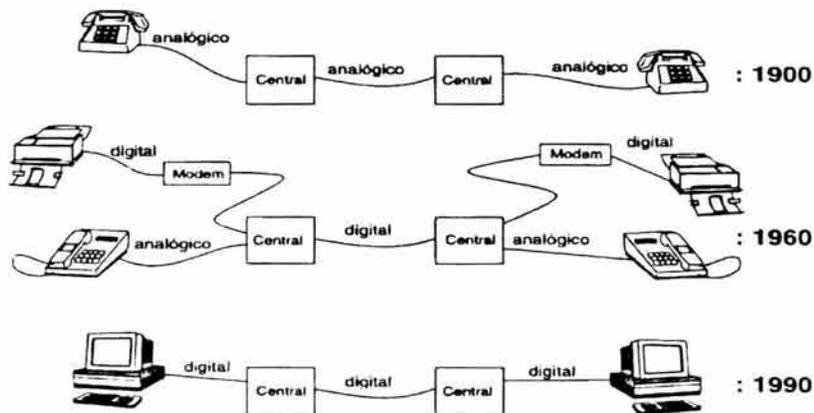


Figura 2.16 Las redes telefónicas han ido evolucionando hacia la digitalización.

II.5.1 Redes analógicas

Las redes analógicas puras, a pesar de su uso extensivo durante casi un siglo, presentan dos graves inconvenientes intrínsecos a su misma naturaleza. Por un lado, el ruido que inevitablemente se introduce y que resulta prácticamente imposible de eliminar y, por otro, las dificultades para el almacenamiento, la reproducción fidedigna y análisis de las señales transmitidas. La combinación de ambos problemas limita la detección de errores, imprescindibles para la transmisión de datos.

Otro inconveniente es el de la multiplexión que resulta excesivamente compleja cuando se han de conmutar por separado varios canales. En una red telefónica analógica los canales de comunicación llegan a las centrales donde las señales son moduladas y transmitidas utilizando técnicas de Multiplexión por División de Frecuencia (FDM). Los canales de comunicación pasan por varios centros de conmutación, donde necesariamente la señal ha de ser demultiplexada y demodulada antes de ser reenviada hacia su destino a través de la arteria adecuada, donde es nuevamente modulada y multiplexada.

II.5.2 La digitalización

Desde que se realizaron los primeros ensayos, las tecnologías digitales resultaron más fáciles de manipular y almacenar; no obstante, el costo de los primeros equipos limitó su instalación a gran escala, quedando reducido su uso a unos pocos sectores. El concepto de telefonía digital ya fue desarrollado en los años treinta y cuarenta, y las primeras implementaciones datan de los años cincuenta. Desde entonces, la evolución hacia la digitalización ha utilizado dos fundamentos tecnológicos:

- La conmutación digital.
- La transmisión digital.

AT&T fue la primera operadora que introdujo, en 1962, la transmisión digital y Western Electric la primera que introdujo la conmutación digital en 1976. Cuando la transmisión y la conmutación son digitales, los conmutadores basados en Multiplexión por División de Tiempo (TDM) pueden extraer señales individuales sin necesidad de decodificarlas, ni tampoco son necesarios los multiplexores pues el mismo conmutador realiza esta función.

La utilidad de los nodos digitales, que integran en una sola operación conmutación y transmisión, dio lugar a las denominadas Redes Digitales Integradas (IDN) de extremo a extremo. Si a estas redes les añadimos unos estándares universales de acceso, empezaremos a estar muy cerca de lo que se conoce como Red Digital de Servicios Integrados, por sus siglas en Inglés (ISDN).

II.5.3 RDSI

En 1984 la UIT-T (cuando se denominaba CCITT) definía la Red Digital de Servicios Integrados (RDSI) como una red evolucionada de la red de telefonía integrada digital, que proporciona una conectividad digital extremo a extremo para dar soporte a una amplia gama de servicios, a los cuales los usuarios tienen acceso a través de un conjunto limitado de interfases estándar multipropósito. El término sajón original es ISDN (“Integrated Service Digital Network”), acuñado en 1972 por Japón y homologado en 1984 por el CCITT.

El concepto extremo a extremo significa que RDSI es una tecnología diseñada para digitalizar hasta el último metro, es decir, llevar la red digital hasta el abonado, fábrica u oficina.

Sus principales ventajas sobre la red de telefónica convencional son una mayor calidad de voz, mayores velocidades, menor tasa de error, mayor rapidez en el establecimiento de llamadas y mayor flexibilidad.

Los objetivos de la RDSI son, fundamentalmente, proporcionar una capacidad de interoperatividad en red que permita a los usuarios acceder fácilmente, integrar, compartir información de todo tipo: datos, audio, texto, imagen y vídeo, con independencia de las fronteras geográficas, organizativas y tecnológicas.

Los estudios del CCITT hicieron patente la absoluta necesidad de que los servicios primarios de RDSI, evolucionaran a partir de las actuales redes telefónicas, entre otras razones para el aprovechamiento de las inversiones en los actuales cables de cobre. Sin embargo, es de esperar la evolución en instalaciones de mayor calidad para transferencias digitales, que a largo plazo son sin duda más rentables, como por ejemplo, fibra óptica.

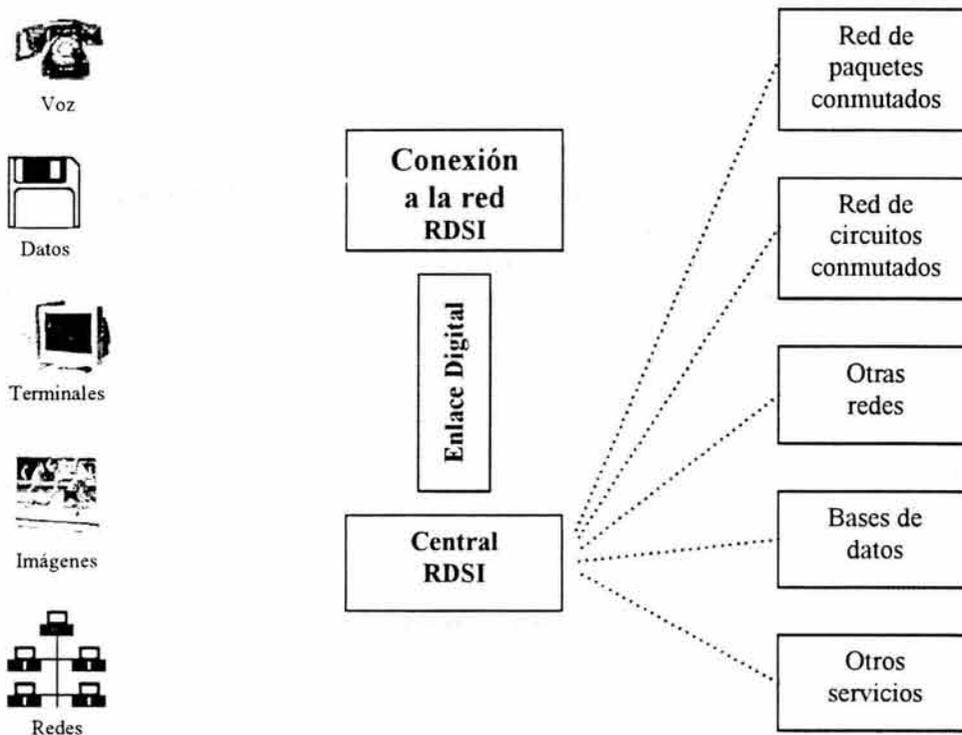


Figura 2.17 Visión global de la RDSI.

La figura anterior [Figura 2.17] es una visión global de la RDSI desde el punto de vista del usuario o cliente. El usuario tiene acceso a la RDSI mediante una interfase local a un “enlace digital” con una cierta razón de bits. Hay disponibles enlaces de varios tamaños para satisfacer las diferentes necesidades, (Palet, 1994).

II.6 Problemas de dos tecnologías separadas: voz y datos

Tradicionalmente, las redes de voz están separadas de las de datos y, si bien, hace ya muchos años que se habla de la integración de unas y otras, la realidad es que se ha avanzado poco en este aspecto; la razón puede que sea que, económicamente aún no resulta del todo rentable, por lo que los administradores de redes siguen pensando en dos redes separadas como solución a las comunicaciones, a pesar de las desventajas técnicas y de administración que tal hecho les pueda suponer, (Huidobro, 2002).

Sin embargo, actualmente, hay nuevos factores que juegan a favor de la integración y que pueden servir de catalizador: la imagen, la telefonía asistida por computadora y, en general, todo lo que es multimedia, entendiendo por tal la combinación de sonido, textos, imágenes y vídeo en la que el usuario tiene cierto grado de interactividad y puede intervenir en el desarrollo de la acción. En el futuro las redes se han de construir para ser capaces de soportar tráfico multimedia, con lo que la integración verá facilitado su camino.

La integración de voz y datos en una red corporativa ofrece una serie de ventajas para el administrador de la red, como es el disponer de una infraestructura común de acceso y transporte y un sistema único de administración. Para ello se confía en una red digital y medios de conmutación capaces de tratar cualquier tipo de información, basados en tecnologías tales como puede ser TDM, RDSI, Frame Relay o ATM.

Cuando se habla de integración de voz y datos en la misma red se pueden dar tres situaciones distintas:

- a) Transporte de datos, junto con voz, sobre redes específicas de voz, como son las redes telefónicas públicas, sean fijas o móviles.
- b) Transporte de voz, junto con datos, sobre redes específicamente diseñadas para datos, como puede ser Internet.
- c) Transporte de voz y datos sobre redes específicas para ambos tipos de tráfico, como es la RDSI.

Cuando se trata de integrar hay que tener en cuenta las diferentes características del tráfico de voz y de datos; por una parte, la voz necesita de un retardo constante en la red, mientras que los datos pueden fluir a distinto ritmo, encargándose el receptor de reordenarlos; por otra parte, la voz admite cierta distorsión en la señal ya que el ser humano es capaz de entender un mensaje aunque presente algunas alteraciones, mientras que una transmisión de datos requiere una alta calidad ya que si no, se producen errores en la misma que pueden ser fatales.

II.6.1 Problemas en la transmisión de voz

Los problemas mas importantes derivados de la transmisión de datos en redes de comunicaciones son los derivados de la transmisión de voz. El problema en este caso no es la conversión de una señal analógica en digital, pues existen numerosos mecanismos para muestrear la señal y codificarla en modo digital.

El problema radica en su recepción y emisión para al receptor. Esta recepción y mas concretamente su emisión hacia el exterior ha de ser en tiempo real, si nosotros hablamos por teléfono esperamos que nuestro interlocutor reciba nuestra voz inmediatamente y sin espera.

El receptor no tiene que esperar a que el emisor acabe para recibir toda una señal de la conversación, sino que a medida que el emisor habla, la voz se codifica y envía, y el receptor a medida que recibe esa información la decodifica y la emite hacia el exterior para que sea escuchada, (Ruiz, 2000).

En este sentido surgen dos problemas básicos:

- El retardo.
- Los errores de transmisión.

El retardo: Todo paquete emitido en una red, llega con un aumento en el tiempo al receptor, también es cierto que no todos los paquetes tienen el mismo retardo, y por tanto se produce una espera ante la recepción de un paquete y otro, a veces es inapreciable otras veces no. Esta variación del retardo entre paquetes se llama "jitter".

Los errores de transmisión. En cualquier transmisión se pueden producir errores, existen códigos de error que nos permiten arreglar los errores cometidos. Pero muchas veces estos códigos de error se penalizan con tiempo de espera en solucionar el error, así como tiempo de espera al interlocutor. También las pérdidas de paquetes producen retardos en las emisiones.

II.6.2 Problemas en la transmisión de datos

Los problemas más significativos que ocurren durante la transmisión de datos son los siguientes:

Atenuación: Es el debilitamiento de la señal con la distancia, debido a la resistencia eléctrica que presentan tanto el canal como los demás elementos que intervienen en la transmisión, el debilitamiento se manifiesta en un descenso de la amplitud de la señal transmitida. La atenuación no afecta por igual a todas las frecuencias, cuando la frecuencia de la señal es mayor, más posibilidades tiene de producirse la atenuación.

Distorsión de retardo: Es la deformación de la señal producida normalmente porque el canal se comporta de forma distinta según la frecuencia de la señal transmitida.

Debido a que en medios guiados, la velocidad de propagación de una señal varía con la frecuencia, hay frecuencias que llegan antes que otras dentro de la misma señal y por lo tanto las diferentes componentes en frecuencia de la señal llegan en instantes diferentes al receptor. Para atenuar este problema se usan técnicas de ecualización.

Ruido: Es toda aquella señal no deseada que se inserta entre el emisor y el receptor de una señal dada. Hay diferentes tipos de ruido:

- **Ruido Térmico:** Es inevitable y es debido a las altas o bajas temperaturas a las que está sometida la línea de transmisión, de modo que aunque sea pequeño siempre va a existir.
- **Ruido Impulsivo:** Es el ruido ocasionado por agentes ajenos a la línea de transmisión. Por ejemplo, un fenómeno meteorológico, el rayo. Es de corta duración y de gran amplitud.
- **Diafonía:** Aparece a partir del hecho físico de que al circular una corriente eléctrica por un conductor se genera un campo magnético en torno al mismo y si cerca de este conductor se encuentra un segundo conductor que también está transmitiendo, el campo magnético generado por el primero se superpone con el segundo. La forma de evitar este tipo de ruido es apantallando los cables o entrelazando unos cables con otros.
- **Intermodulación:** Este ruido está relacionado con el comportamiento no lineal del medio de transmisión y consiste en la aparición de frecuencias que son suma o diferencias de la señal que se transmite.

Capacidad del canal: Se llama capacidad del canal a la velocidad a la que se pueden transmitir los datos en un canal de comunicación. La velocidad de los datos esta expresada en bits por segundo (bps).

Ancho de banda: Es el margen de frecuencias de transmisión de la señal y que está limitado por el transmisor y por la naturaleza del medio de transmisión. La tasa de errores es la razón a la que ocurren errores, (El planetamx, 2001).

II.7 Video y sus problemas en redes integradas

El tratamiento de la información multimedia requiere de importantes cantidades de memoria y de potencia de procesamiento. Podemos ver los requerimientos aproximados, [Tabla 3], (Torres, 1994):

Tipo de información	Requerimientos de memoria
Texto	2 KB por página
Imagen baja resolución	64 KB
Imagen detallada	7,5 MB
Voz	6 a 44 KB/seg
Audio calidad	176 KB/seg

Tabla 3: Requerimientos de multimedia.

El tratamiento del vídeo por computadora es el que exige las prestaciones más elevadas. Existen tres factores comunes a los que prestar atención a la hora de configurar el equipamiento o accesorios:

1. Tamaño de la ventana visible en pantalla: Puede variar entre 1/16 de pantalla VGA (160 x 120 pixeles) hasta 640 x 480 para una resolución normal de pantalla entera VGA.
2. Velocidad de cuadros o "frame rate": Es el número de cuadros por segundo (cps) presentados en pantalla. 10 a 15 cps sirve para presentaciones aceptables; 24 cps es el utilizado en las películas; hasta 30 cps que equivale a la utilizada en televisión.
3. Capacidad de presentación de colores: Indica la habilidad de presentar profundidad de color y su resolución. Profundidad de color es el número de colores diferentes disponibles que puede variar entre una paleta VGA de 16 colores (a 4 bits), hasta color real de 16,7 millones de matices (a 24 bits). La resolución de color se refiere al grano obtenible en color. La mayor calidad se obtiene asignando a cada píxel su color, en lugar de asignar un mismo color a un grupo de éstos.

La calidad final de las imágenes que obtengamos dependerá de la combinación de estas tres cualidades. Estas prestaciones se obtienen según el tipo de microprocesador, tarjeta gráfica y disco duro que se utilice en conjunto. Otro aspecto importante es la compresión de secuencias de vídeo. Si se tiene en cuenta que tan solo un minuto de vídeo sin comprimir puede ocupar hasta 50 MB.

La tecnología de compresión/descompresión desarrollada por Intel, "Indeo-video", permite reducir archivos de 50 MB a alrededor de 9 MB. Otra característica interesante en los paquetes y programas de tratamiento de vídeo es que sean "escalables", de modo que a medida que avanzan las tecnologías de arquitectura de sistemas pueda seguirse utilizando.

IBM tiene en sus planes emplearlo en sus sistemas operativos, de modo que se podrá intercambiar archivos de vídeo libremente entre las plataformas basadas en Windows, OS/2 y Macintosh.

La captura y posterior compresión de vídeo puede realizarse en un solo paso, evitando el almacenamiento masivo (para su posterior procesado) del vídeo sin comprimir. La tecnología del Intel Smart Video Recorder hace estas funciones en un solo paso en tiempo real, entregando al disco duro el vídeo digitalizado y comprimido a 30 cps.

Las secuencias así grabadas pueden ser luego distribuidas tanto por diskettes, redes locales o por RDSI. Existe una relación en la que si se quiere mayor velocidad de cuadros, habrá que reducir el tamaño de la ventana, contrariamente si se lo que se pretende es un mayor detalle a toda pantalla, habrá que reducir la velocidad, (Intel).

La evolución de los estándares y de la tecnología, como por ejemplo la compresión de vídeo, la calidad de servicio en las redes, los protocolos para el envío de señales, etcétera. Ha hecho que el envío de vídeo por redes sea hoy una realidad en cualquiera de sus formas habituales:

- Transmisión de vídeo en tiempo real.
- Transmisión en modo programado.
- Transmisión en modo vídeo bajo demanda .

En cada uno de estos casos, el equipamiento de captura, transmisión y visionado del vídeo será diferente, según el ancho de banda disponible, la calidad requerida, el retardo admisible y el tipo de terminal de vídeo, (Audiovisual Systems).

II.8 Problemas de las limitantes de ancho de banda

El ancho de banda es la capacidad de una línea para transmitir información, es un factor que limita la capacidad de transmisión dentro de una red, otros factores son la potencia eficaz de la señal transmitida y la cantidad de ruido que afecta el canal. El ruido es inherente a la naturaleza del propio canal y nunca puede eliminarse por completo, (Caravantes, 1997).

Relación entre la velocidad de transmisión y el ancho de banda: El medio de transmisión de las señales limita mucho las componentes de frecuencia a las que puede ir la señal, por lo que el medio sólo permite la transmisión de cierto ancho de banda. Al duplicar el ancho de banda, se duplica la velocidad de transmisión a la que puede ir la señal. Al considerar que el ancho de banda de una señal está concentrado sobre una frecuencia central, al aumentar ésta, aumenta la velocidad potencial al transmitir la señal. Pero al aumentar el ancho de banda, aumenta el costo de transmisión de la señal aunque disminuye la distorsión y la posibilidad de ocurrencia de errores. El ancho de banda está limitado por el transmisor y por la naturaleza del medio de transmisión, por ejemplo (Cárdenas, 2000):

Par trenzado: Velocidad del orden de 10-100 Mbps, el ancho de banda depende del grosor y de la distancia:

- Categoría 3 hasta 16 MHz,
- Categoría 4 hasta 20 MHz,
- Categoría 5 hasta 100 MHz.

Cable coaxial: Los cables coaxiales tienen anchos de banda de alrededor de 10 MHz, hasta varios cientos de MHz.

Los hay de 2 impedancias:

- 75 ohmios: banda ancha, utilizado en TV, distintos canales, 300 MHz,
- 50 ohmios: banda base, utilizado en Ethernet, un canal,
- 10Base5: coaxial grueso, 500 metros, 10 Mbps,
- 10Base2: coaxial fino, 185 metros, 10 Mbps, conector BNC.

Fibra óptica: Alcanza un ancho de banda de 30,000 GHz.

- Multimodo con salto de índice.: Se consigue un ancho de banda de 100 MHz,
- Multimodo con índice gradual: Es la fibra más utilizada y proporciona un ancho de banda de 1 GHz,
- Monomodo: Ancho de banda de 50 GHz.

Radio: De 2 a 40 GHz.

Microondas y Satélites: De 300 GHz a 200,000 GHz

- Banda C (4 - 6 GHz),
- Banda Ku (12-14 GHz),
- Banda Ka (20/30 GHz).

* * *

Dentro de los aspectos más importantes del presente capítulo destacamos que el propósito de la conmutación es proporcionar un servicio que posibilite el intercambio de datos entre nodos hasta que alcancen su destino. La técnica de conmutación de circuitos se desarrolló para tráfico de voz, el mejor ejemplo conocido de una red de conmutación de circuitos es el de la red telefónica pública, aunque también puede administrar tráfico de datos, si bien su uso en este último tipo de aplicaciones resulta en ocasiones ineficiente.

En la conmutación de circuitos se establece un canal de comunicaciones dedicado entre dos estaciones. Se reservan recursos de transmisión y de conmutación de la red para su uso exclusivo en el circuito durante la conexión, una vez establecida parece como si los dispositivos estuviesen directamente conectados.

En la conmutación de paquetes, una estación realiza la transmisión de los datos en base a pequeños bloques llamados paquetes, cada uno de los cuales contiene una parte de los datos de usuario además de información de control necesaria para el adecuado funcionamiento de la red.

En cuanto a tecnologías de redes, X.25 es el estándar de interfase de red más ampliamente utilizado que existe. No obstante, hay tecnologías más recientes que proporcionan mayor caudal efectivo y menor retardo, como es el caso de Frame Relay que es una tecnología nacida de la necesidad de incrementar el ancho de banda, la aparición de impredecibles modelos de tráfico, y de un crecimiento de usuarios que demandan un servicio eficaz.

Por otro lado, RDSI es una tecnología diseñada para digitalizar hasta el último metro, es decir, llevar la red digital hasta el abonado, fábrica u oficina. Los objetivos de la RDSI son, fundamentalmente, proporcionar una capacidad de interoperatividad en red que permita a los usuarios acceder fácilmente, integrar, compartir información de todo tipo: datos, audio, texto, imagen y vídeo, con independencia de las fronteras geográficas, organizativas y tecnológicas.

Una vez que se ha analizado detalladamente la conmutación de circuitos y paquetes con su aplicación en las redes de voz y datos respectivamente, en el siguiente capítulo se presentan los conceptos de redes de alta velocidad como parte fundamental de su evolución, en donde la unificación de ambas redes (voz y datos) es un punto esencial en la administración de la red.

CAPÍTULO 3:

CONCEPTOS DE REDES DE ALTA VELOCIDAD

III.1 Introducción

Dada la creciente demanda de los usuarios por tener mayor conexión entre sí mediante distintas aplicaciones (por ejemplo, teléfono, correo electrónico, imágenes, video, etcétera) fue necesario desarrollar tecnologías de mejor desempeño. Es por eso que se han desarrollado nuevas tecnologías, para permitirnos poder comunicarnos con todo el mundo, sea del lugar que sea, sin importar las distancias ni el tipo de información.

Estas tecnologías han borrado las barreras de la comunicación, permitiéndonos así una comunicación más rápida y con mayor seguridad. Mucha gente en la industria de las comunicaciones se alegra por la rapidez con que está mejorando la tecnología de las computadoras, pero debemos decir que en la carrera entre las computadoras y la comunicación ha ganado la comunicación, por los avances realizados en los últimos tiempos.

III.2 Sincronización en redes

El receptor debe saber la velocidad a la que se están recibiendo los datos de tal manera que pueda muestrear la línea a intervalos constantes de tiempo para así determinar cada uno de los bits recibidos, (Stalings,2000).

Para transmisión de datos existen las siguientes técnicas de sincronización: asíncrona, síncrona e isócrona.

III.2.1 Transmisión asíncrona

Cada carácter se trata independientemente, los datos viajan por el canal sin una velocidad fija, es decir, el tiempo que transcurre desde la transmisión de un dato, hasta la transmisión del próximo dato es variable.

El primer bit de cada carácter es un bit de inicio que alerta al receptor sobre la llegada del carácter y el último es un bit de parada, [Figura 3.1]. El receptor muestrea cada bit del carácter y busca el comienzo del siguiente. Esta técnica puede no funcionar correctamente para bloques de datos excesivamente largos debido a que el reloj del receptor podría desincronizarse del reloj del emisor. No obstante, la transmisión de datos en bloques grandes es más eficaz que la transmisión carácter a carácter.

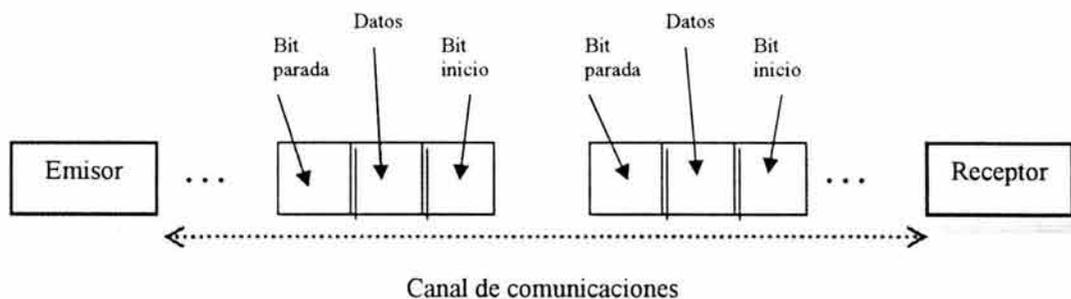


Figura 3.1 Transmisión asíncrona.

III.2.2 Transmisión síncrona

En este caso los datos son transmitidos a una velocidad fija de bits, por una línea que se mantiene viva aún cuando no se esté enviando información. Se utiliza para el envío de bloques grandes, cada bloque de datos forma una trama, que incluirá entre otros campos los delimitadores de principio y fin (bits de sincronización), [Figura 3.2]. Se utilizan canales separados de reloj que administran la recepción y transmisión de los datos.

Las señales de reloj determinan la velocidad a la cual se transmite o recibe, hay intervalos de tiempo pre-definidos para mantener la sincronía, el ancho de banda se comparte de una manera determinada y las aplicaciones son sensibles al retardo.

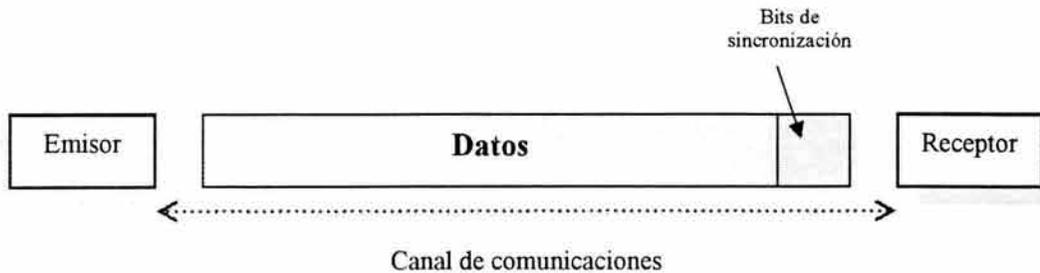


Figura 3.2 Transmisión síncrona.

III.2.3 Transmisión isócrona

Se envían porciones de la información para ser transmitida en forma periódica (“slots” de tiempo) donde cada sesión tiene asignado su “slot” independientemente de que envíe información, [Figura 3.3]. El tiempo de acceso tiene una duración fija, el ancho de banda es específico y está enfocado a aplicaciones que requieren un estricto control de acceso y entrega de datos sensibles a tiempo, como transmisiones por voz o por video.

Las redes que son capaces de llevar a cabo un servicio isócrono preasignan una cantidad específica de ancho de banda sobre intervalos regulares para garantizar que la transmisión no se interrumpa. El servicio isócrono no debe experimentar variaciones de retardo en la señal de salida.

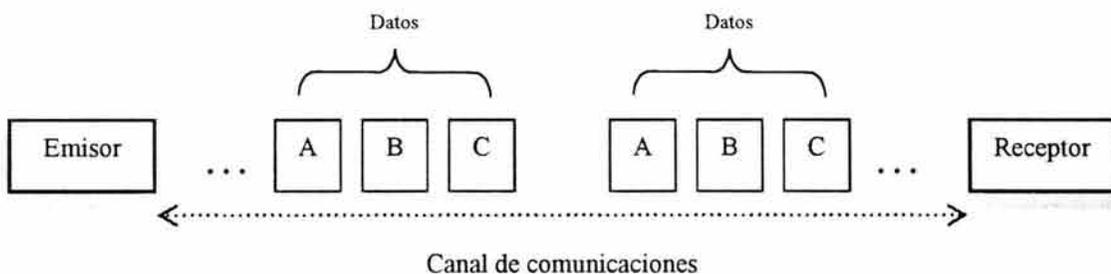


Figura 3.3 Transmisión isócrona.

III.3 Jerarquía Digital Plesiócrona (PDH)

Las señales de datos que tienen el mismo rango de transmisión pero que son provenientes de diferentes fuentes, siempre tienen un desplazamiento mayor o menor del valor nominal de la tasa de transferencia. Por otra parte, cada una de las señales es también sincrónica con las otras, es por ello que se ha llamado a este tipo de señales plesiócronas.

En la Jerarquía Digital Plesiócrona (PDH), la idea básica es la de hacer una serie de multiplexaciones de señales provenientes de fuentes distintas, para así formar una señal común con una tasa de transferencia superior, haciendo determinada cantidad de multiplexaciones se van logrando las diferentes jerarquías propias de PDH.

Actualmente existen en el mundo dos PDH definidas por el CCITT que son: la Europea basada en la velocidad primaria de 2.048 Kbps, y la Americana (utilizada en E.U.A y Japón) basada en la velocidad primaria de 1.544 Kbps, ambas obtenidas por la multiplexación sincrónica de trenes básicos de 64 Kbps (30 y 24 canales respectivamente).

Cada una de estas jerarquías exige en cuanto a sincronización una correcta temporización en ambos extremos para demultiplexar adecuadamente las señales, (Sandoval, 2000).

A estas velocidades, por ejemplo en el caso de las Europeas, se llega haciendo una serie de multiplexaciones, las cuales se realizan tomando cuatro líneas de la jerarquía inmediata inferior, y multiplexando las mismas en tiempo se llega a la siguiente jerarquía.

La siguiente figura, [Figura 3.4 y Tabla 1] muestra como se realizan las sucesivas multiplexaciones hasta llegar a la jerarquía más alta que se encuentra estandarizada:

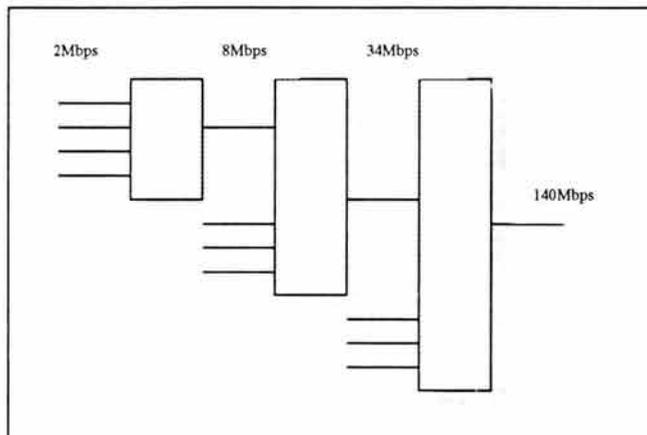


Figura 3.4 Serie de Multiplexaciones.

Zonas	Nivel Jerárquico	Velocidad binaria en Mbps	Capacidad de Canales	Denominación
Europa	1	2.048	30	E1
	2	8.448	120	E2
	3	34.368	480	E3
	4	139.264	1,920	E4
	5	564.992	7,680	*
Norte América	1	1.544	24	T1
	2	6.312	96	T2
	3	44.736	672	T3
	4	274.176	4,032	*

* Estos niveles no están estandarizados

Tabla 1: Jerarquía Digital Plesiócrona.

El factor multiplicador es mayor para las distintas tasas de transferencia, [Figura 3.5], esto se debe a que para cada nivel de jerarquía son insertados algunos bits adicionales, destinados a la generación de la trama y también para llevar información adicional dentro de la misma.

Método de multiplexación: La multiplexación en la jerarquía PDH, se realiza utilizando el método de entrelazado bit a bit, esto quiere decir que la señal de entrada de un multiplexor aparecerá solamente cada 4 bits de la señal de salida del mismo.

En la multiplexación habrá que diferenciar dos casos:

1. Las señales originales son síncronas, por ejemplo: tienen exactamente el mismo reloj.
2. Las señales originales no son síncronas, por ejemplo sus relojes provienen de distintos lugares.

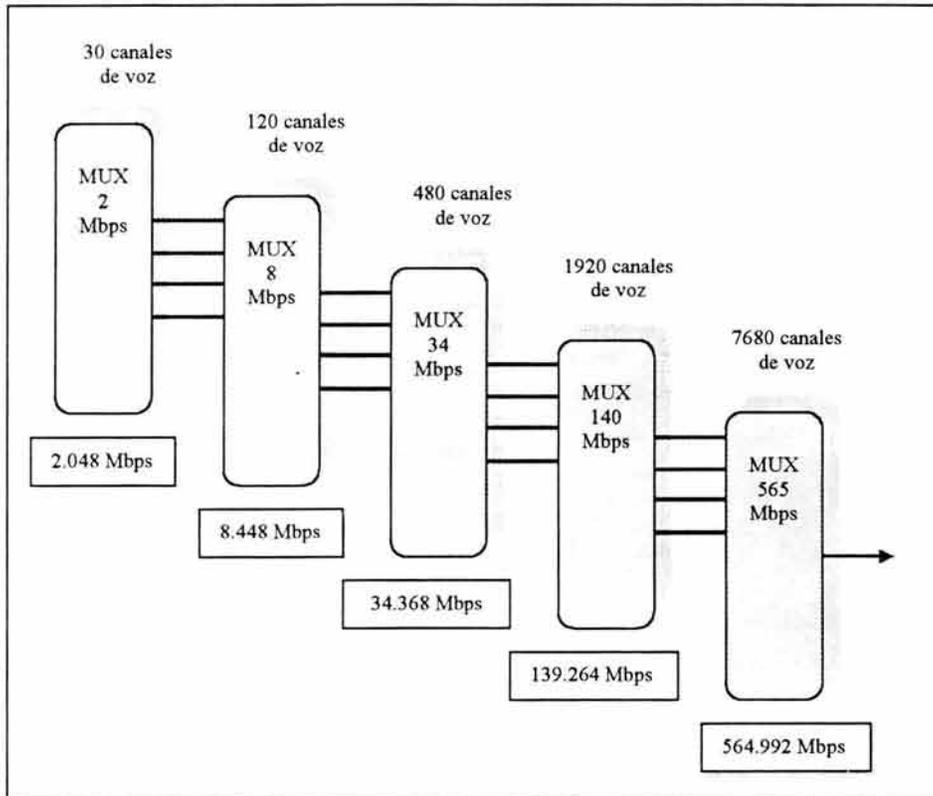


Figura 3.5 Jerarquía Digital Plesiócrona Recomendación Europea.

La PDH es una tecnología plesiócrona, por ello no es posible insertar o extraer ningún canal o tributaria sin demultiplexar completamente la señal de entrada hasta el nivel requerido.

Obviamente, y conjuntamente con el problema de la limitación en las posibilidades de administración y mantenimiento, esta es la mayor desventaja para esta tecnología, especialmente para operadores cuando proyectan sus redes.

Por esta razón nuevas tecnologías de transmisión tales como SDH se han desarrollado permitiendo configuraciones de red más flexible y menos costosas.

III.4 Jerarquía Digital Síncrona (SDH)

La existencia de diversas jerarquías digitales (la Europea y la Americana), hacen que cuando el tráfico sobrepasa las fronteras nacionales, haya necesidad de efectuar conversiones generalmente costosas para llevar la señal a otro país. Esto y las desventajas de la PDH forzaron a crear una jerarquía digital que proporcionara un estándar mundial unificado que a su vez ayude a que la administración de la red sea mas efectiva y económica. Además satisface las demandas de nuevos servicios y más capacidad de transmisión, por parte de los usuarios, (Sandoval, 2000).

Entre 1988 y 1992 se produce la primera regulación de la Jerarquía Digital Síncrona (JDS), o más conocida por sus siglas en la lengua Inglesa “Synchronous Digital Hierarchy” (SDH) en Europa; SDH es un estándar definido por el sector de estandarización de telecomunicaciones de la Unión Internacional de Telecomunicaciones (ITU-T). El principal objetivo en la definición de SDH era la adopción de una verdadera norma mundial que posibilitara una compatibilidad máxima entre diferentes suministradores y operadores. Este estándar especifica velocidades de transmisión, formato de las señales, estructura de multiplexación, codificación de línea, parámetros ópticos, etcétera, así como normas de funcionamiento de los equipos y de administración de red. Por otro lado, dotará a las redes de una mayor flexibilidad, mejor aprovechamiento del ancho de banda potencial de la fibra óptica, y más capacidad de monitorización de la calidad y administración centralizada, (IDG Communications, 2002).

SDH es un estándar para redes de telecomunicaciones de “alta velocidad y alta capacidad”. La constante básica de tiempo es de 8,000 tramas por segundo, trabaja con una estructura básica la cual tiene una duración de 125 μ s, y corresponde a una matriz de 9 filas y 270 columnas, cuyos elementos son octetos (8 bits) de 64 Kbps cada uno; por lo tanto la trama tendrá: $2430 \text{ Octetos} * 64 \text{ Kbps} = 155.520 \text{ Kbps}$. [Figura 3.6].

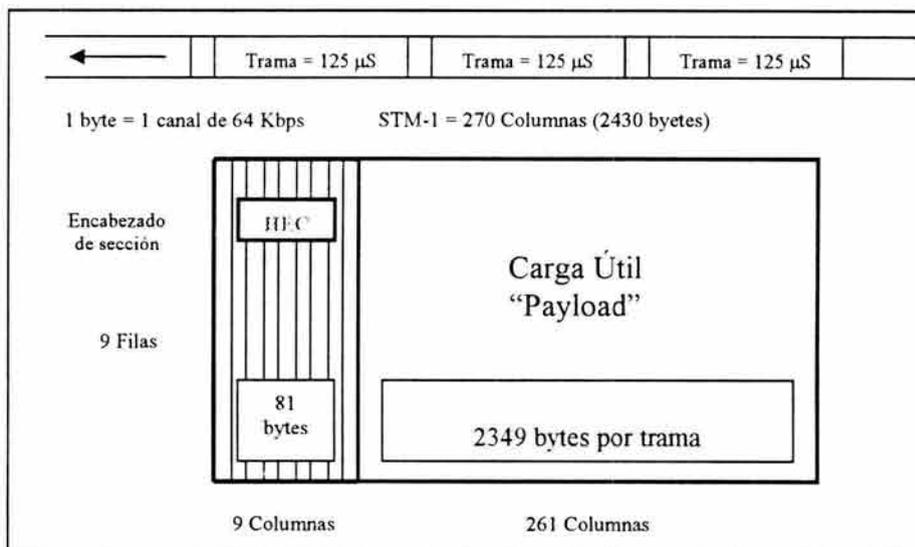


Figura 3.6 Estructura de la trama SDH.

La parte derecha de la trama es para información transmitida (261*9 bytes) mientras que la parte izquierda se usa para otros tipos de información: encabezado de sección y puntero. Esta trama básica recibe el nombre de Módulo de Transporte Síncrono de Nivel 1 (STM-1), consiste en la capacidad correspondiente a un Contenedor Virtual (información del usuario).

SDH es un estándar de transmisión síncrona sobre 155 Mbps, diseñado para operar con ATM, tiene muchas ventajas sobre tecnologías de transmisión existentes, como flexibilidad en la administración de transmisión, reconfiguración y control y conmutación a velocidades de 622 Mbps y superiores.

Originalmente este estándar fue diseñado para el transporte de las distintas señales definidas en la jerarquía PDH en una trama STM-1. Posteriormente ha sido desarrollado para transportar otros tipos de tráfico, como ATM o IP, a tasas de transferencia que son múltiplos enteros de 155 Mbps.

La flexibilidad en el transporte de señales digitales de todo tipo permite de esta forma la provisión de toda clase de servicios sobre una única red SDH: telefonía, provisión de redes alquiladas, creación de redes MAN y WAN, videoconferencia, distribución de televisión por cable, etcétera. En ella se pretendieron cubrir las carencias presentadas por PDH.

En SDH se parte de una señal de 155 Mbps denominada Módulo de Transporte Síncrono de Primer Nivel o STM-1, [Tabla 2] definida tanto para interfase óptica como de cobre, SDH define interfases de tráfico que son independientes de los distintos vendedores de equipos, (Comunicaciones World, 2003).

Tasa Mbps	Nomenclatura	Capacidad
51.84	STM-0	
155.52	STM-1	63 E1's o 1 E4
622.08	STM-4	252 E1's o 4 E4's
2488.32	STM-16	1,008 E1's o 16 E4's

Tabla 2: Velocidad de Transmisión en línea SDH.

III.5 Modo de Transmisión Asíncrono (ATM)

La tecnología subyacente que hace posible la RDSI-BA se llama ATM, su nombre se debe a que no sigue la referencia de un reloj maestro que impone la sincronización de los datos a la hora de transmitir. El modo de transferencia asíncrono (ATM) es el modo de transporte en una red RDSI-BA, (Recomendación ITU-T I.121).

ATM es una técnica de conmutación rápida de paquetes porque consigue una conmutación de paquetes con la funcionalidad mínima en la red y con independencia del servicio que esté facilitando al usuario. Para conseguir una conmutación de paquetes con funcionalidad mínima se basa en tener que segmentar toda la información que transmite a un tamaño estándar de celda pequeño para facilitar las operaciones de conmutación.

El uso de conmutación de celdas es un rompimiento drástico con la tradición centenaria de conmutación de circuitos que establecía una trayectoria de cobre entre los usuarios, dentro del sistema de teléfonos. Pero se tomó la conmutación de celdas porque es altamente flexible y permite el manejo sencillo de tráfico a velocidad constante (audio, video) como variable (datos).

Permiten unas velocidades de transmisión en torno a los Gbps y la conmutación digital de las celdas es más fácil que el empleo de las tradicionales técnicas de multiplexación (en especial con el uso de fibra óptica). Además si se busca poder implementar transmisión por difusión (por cualquier medio) no se puede implementar conmutación de circuitos.

III.5.1 Funcionamiento de ATM

ATM transmite utilizando celdas de tamaño constante para simplificar las operaciones de conmutación y reducir la variabilidad del retardo de transmisión. De este modo la información de los usuarios se segmenta en paquetes de longitud constante de 53 octetos de los cuales 5 son de encabezado y 48 de carga útil "payload", [Figura 3.7].

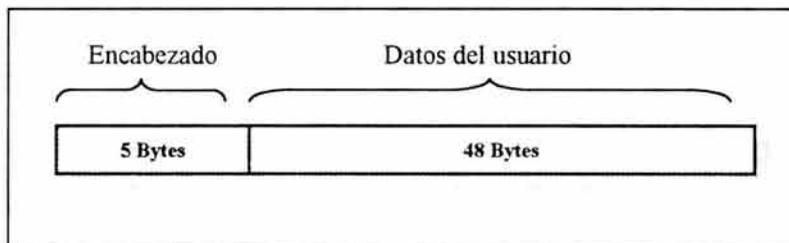


Figura 3.7 Celda ATM.

Todas las celdas que pertenecen a un mismo flujo de información (por ejemplo; todas las celdas obtenidas tras segmentar un fichero) se marcan con un mismo identificador y se transportan en secuencia por la red a través de un circuito virtual. Esto quiere decir que todas estas celdas van a recorrer los mismos enlaces por orden, según se envían se reciben manteniendo la secuencia entre las mismas.

ATM es un modo de transporte orientado a conexión, para hacer una llamada primero se debe enviar un mensaje para establecer la conexión. Después todas las celdas subsecuentes siguen la misma trayectoria hacia el destino. La transmisión (multiplexación) de celdas sobre un enlace físico es asíncrona.

ATM no realiza control de errores, ni control de flujo, si se desean estas opciones deben ser implementadas en los extremos dependientes del servicio. Básicamente, ATM garantiza que las celdas van a llegar en el mismo orden que son transmitidas pero no que van a llegar.

Las celdas se conmutan por “hardware” a partir del identificador de circuito virtual. Lo que quiere decir que las celdas eligen los enlaces por los que deben pasar cada vez que cambian de nodo por el identificador de circuito virtual, éste les da la información necesaria para comprobar dentro del nodo en cuestión el camino que deben seguir.

En ATM los canales se identifican por su etiqueta, ancho de banda variable asignado bajo demanda, [Figura 3.8]. Esto quiere decir que no hay una asignación previa de ancho de banda por usuario por lo que dependiendo de lo sobrecargada que vaya la red, un usuario va a poder hacer mayor o menor uso de ella, si los demás usuarios no la están utilizando va a poder utilizar todo el ancho de banda para el sólo, pueden haber momentos en que un canal no este asignado a ningún usuario (vacío).

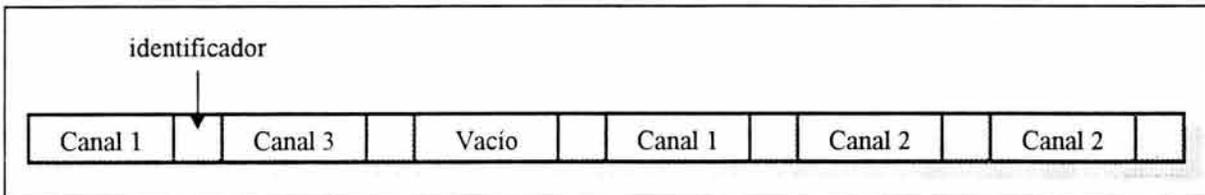


Figura 3.8 Canales ATM.

ATM es igualmente adecuada para entornos de LAN y WAN, para aplicaciones de voz, datos, imagen y video, para redes públicas y privadas. ATM puede manejar tráfico isócrono, combina los beneficios de la conmutación de paquetes y la conmutación de circuitos, reservando ancho de banda bajo demanda de una manera eficaz y de costo efectivo, a la vez que garantiza ancho de banda y calidad de servicio para aquellas aplicaciones sensibles a retardos, (Unitronics Comunicaciones, 1998).

III.6 Aparición de RDSI-BA

Con el desarrollo de las nuevas redes de comunicaciones se puede ver como las compañías telefónicas enfrentan un problema bastante fundamental: las redes múltiples. Esto se debe a que hay que mantener el antiguo servicio telefónico ordinario, la red antigua de circuitos conmutados, los nuevos servicios de datos, en consecuencia, mantener todas estas redes individuales es complicado.

Como solución a esto, se busca una nueva red única para todos los servicios, el sistema telefónico y las redes especializadas con una red integrada con todos los tipos de transferencia de información. Esta red debe tener una velocidad de transmisión elevada (comparada con las existentes) y debe permitir una gran variedad de servicios nuevos.

Este nuevo servicio se llama Red Digital de Servicios Integrados de Banda Ancha (RDSI-BA) o mejor conocida como (B-ISDN) por sus siglas en Inglés: “Broadband Integrated Services Digital Network”, esto supone una gran comodidad al usuario, le permite tener video bajo demanda (ver una película y poder pararla, repetir, interactuar con ella, etcétera), transporte de alta definición para datos científicos e industriales, correo electrónico multimedia (permitiendo imágenes con movimiento total y música con calidad de disco compacto).

III.6.1 Concepto de RDSI-BA

La RDSI-BA se define como un servicio que requiere canales de transmisión capaces de soportar velocidades mayores que la velocidad primaria, (CCITT Rec I.121, 1998).

Se definió ATM como la tecnología de conmutación que utilizaría RDSI-BA y 155 Mbps la velocidad que debía soportar. A pesar de las diferencias entre RDSI-BA y RDSI-BE, ambas mantienen muchos puntos en común, ya que la RDSI-BA es la evolución hacia la alta velocidad de la RDSI-BE (conocida ahora como RDSI de banda estrecha). Alguno de estos puntos en común son:

- El modelo de referencia para la configuración es similar, ya que RDSI-BA asumió con algunas modificaciones el de RDSI-BE.
- Ambas son de naturaleza conmutada y con conexión, utilizando un protocolo de señalización similar.

III.6.2 Modelo ATM

El hecho de utilizar ATM en la RDSI-BA marca la diferencia en los protocolos de RDSI-BA y RDSI-BE. En efecto, aunque RDSI-BA debe admitir aplicaciones en modo de circuito, éstas se realizarán sobre un mecanismo de transporte basado en paquetes, por lo tanto, podemos decir que RDSI será una red de conmutación de paquetes ya que contiene servicios de banda ancha. El modelo ATM se define en tres dimensiones, [Figura 3.9] (Trujillo, 1997):

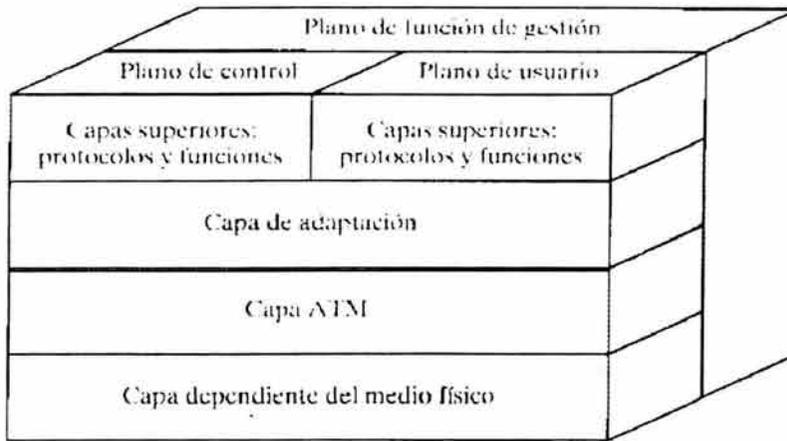


Figura 3.9 Modelo de referencia de protocolos
(Rec. ITU-T 1.321, 1991).

La RDSI de Banda Ancha con ATM tiene su propio modelo de referencia, diferente del modelo OSI y también del modelo TCP/IP, este modelo consiste en:

La capa dependiente del medio físico: Tiene que ver con voltajes, temporización de bits y varias consideraciones más. ATM dice que las celdas ATM se pueden enviar por si solas por un cable, fibra o bien se pueden empaquetar como carga útil de otros sistemas portadores. De este modo ATM está diseñado para ser independiente del medio de transmisión.

La capa ATM: Tiene que ver con las celdas y su transporte, define la organización de las celdas y dice lo que significan los campos del encabezado. Además también participa en el establecimiento y la liberación de circuitos virtuales y aquí es en donde se localiza el control de la congestión.

La capa de adaptación de ATM ("ATM Adaptation Layer", AAL): Se ha definido para permitir a los usuarios enviar paquetes mayores de una celda, ya que la mayor parte de las aplicaciones no requieren trabajar directamente con celdas. Entonces esta capa se encarga de segmentar los paquetes en celdas, transmitirlos de manera individual y reensamblarlo todo en el otro extremo.

Se distinguen tres planos separados:

Plano de usuario (U): Se encarga del transporte de los datos, el control de flujo, la corrección de errores y otras funciones del usuario.

Plano de control (C): Se encarga del establecimiento, mantenimiento y terminación de las conexiones.

Plano de gestión (M): Se encarga de la coordinación entre planos y de las funciones de operaciones, administración y mantenimiento.

Las capas física y AAL se dividen a su vez en dos subcapas o subniveles, [Figura 3.10] una que hace el trabajo y otra de convergencia con la capa superior.

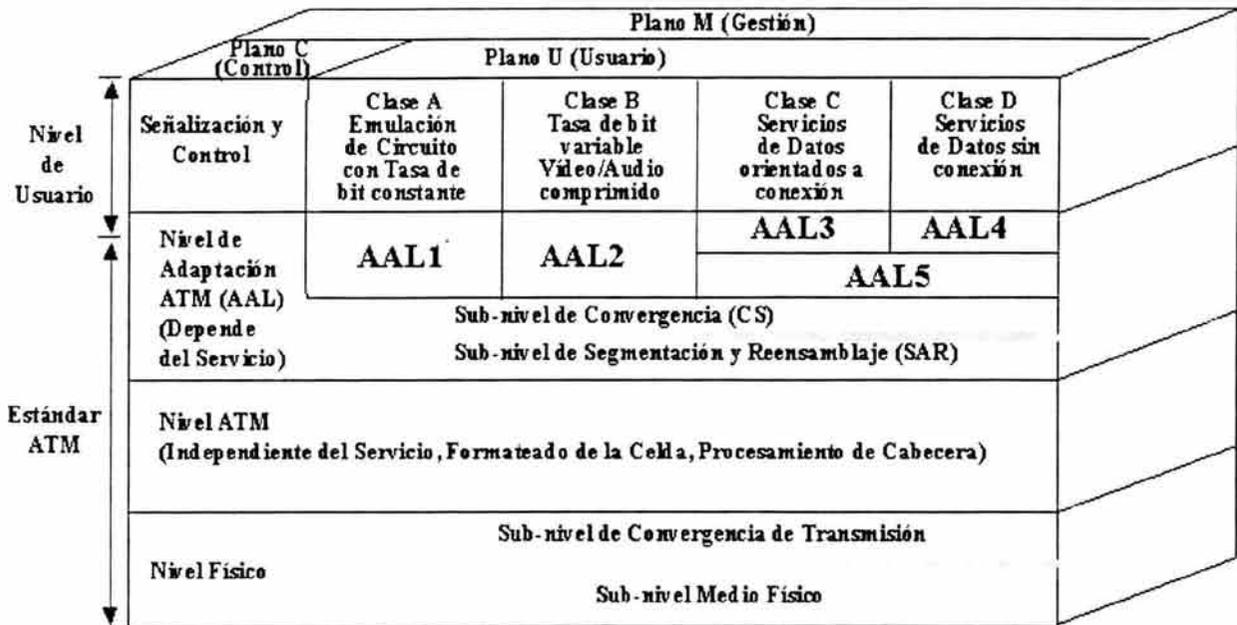


Figura 3.10 Funciones de las subcapas.

III.7 Red Óptica Síncrona (SONET)

En el año de 1985 la empresa Bell Core le hace una propuesta al ANSI de estandarizar las velocidades mayores a 140 Mbps, que hasta el momento eran propietarias de cada empresa. En 1986, la Bell Core, y la AT&T proponen al CCITT, posibles velocidades de transmisión para que las mismas sean estandarizadas, cada una de estas empresas propone diferentes velocidades de transmisión posible.

Dicho estándar por sus siglas en inglés; "Synchronous Optical Network" (Red Óptica Síncrona) es considerada como una red de alta velocidad especialmente para las comunicaciones de datos, voces e imágenes por fibra óptica, para ser utilizado en Norteamérica, su contraparte en Europa es SDH, seleccionando las opciones adecuadas, un subconjunto de SDH es compatible con el subconjunto de SONET, por consiguiente es posible la interoperatividad de tráfico y nodos SDH y SONET. No obstante, no es posible la interoperatividad de alarmas y la supervisión de calidad entre ambos sistemas, (IDG Communications, 2002).

SONET provee un método de estandarización para construir un equipo de telecomunicaciones que penetre en la gran capacidad de llevar información de la fibra óptica, mientras mantenga compatibilidad con las grandes instalaciones de cobre.

La velocidad está en el rango de 51.8 Mbps a 2.44 Gbps, además de proveer una guía para crear interfaces ópticas estándares, incluyen un esquema "multiplexing" que hace posible extraer fácilmente canales de baja velocidad en canales de alta velocidad ("fiber-based bit stream"). En adición de proveer transmisión a alta velocidad, la transmisión SONET incluye señales de encabezado que provee una mejoría en la administración de las redes y en la eficiencia de suministrar y mantener los servicios, (Díaz, 2000).

SONET, usa un esquema de transmisión síncrono, con un trama cada 125 μ s (microsegundos). Cada trama es organizada como una serie de bytes. El tamaño de la trama depende de la velocidad de transmisión. La transmisión básica de SONET es una Señal de Transporte Síncrono-1 (STS-1), [Figura 3.11] que consiste en tramas que tienen 810 bytes organizados en 9 filas a través de 90 columnas. A 8,000 tramas por segundo, esto da una velocidad de transmisión de 51.840 Mbps.

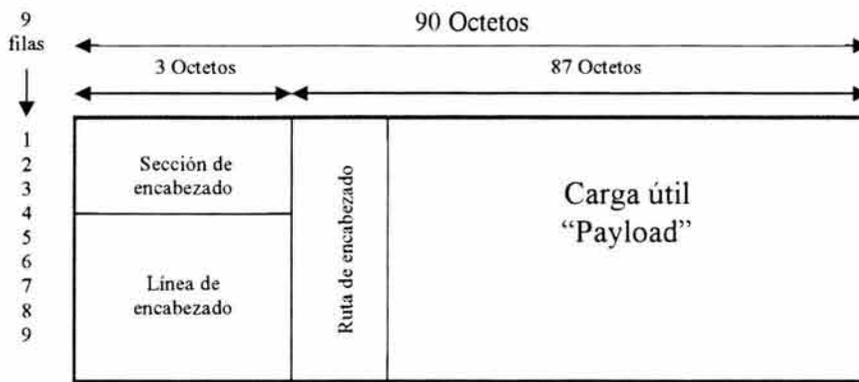


Figura 3.11 Estructura de una trama SONET STS-1.

En SONET, se parte de una señal de 51.84 Mbps denominada Señal de Transporte Síncrono de primer nivel o STS-1 en la interfase de cobre, o bien contenedor óptico de primer nivel OC-1 en la interfase óptica, [Tabla 3].

Nomenclatura			Capacidad
Tasa Mbps	Nivel Óptico	Nivel Eléctrico	SONET
51.84	OC-1	STS-1	28 DS1's o 1 DS3
155.52	OC-2	STS-3	336 DS1's o 3 DS3's
662.08	OC-12	STS-12	28 DS1's o 12 DS3's
2,488.32	OC-48	STS-48	1,344 DS1's o 48 DS3's

STS = Señal de Transporte Síncrono
OC = Portadora Óptica

Tabla 3: Velocidad de transmisión en línea SONET.

SONET se basa en una arquitectura de anillo, es un sistema con Multiplexación por División en el Tiempo (TDM). Hay distintos tipos de canales estandarizados para distintas velocidades, cada una con un tamaño de trama diferente. SONET se despliega típicamente encima de la fibra óptica en un anillo doble de la siguiente forma, [Figura 3.12]:

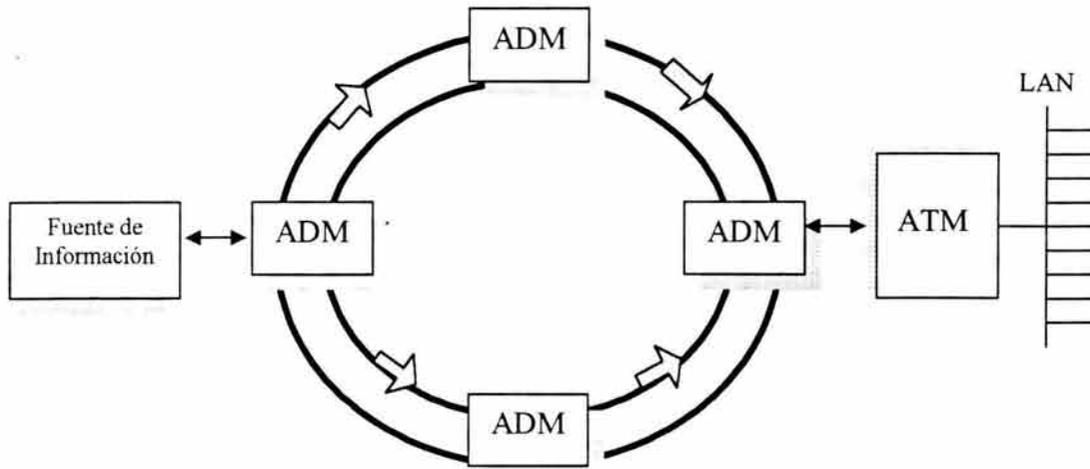


Figura 3.12 Arquitectura de SONET.

El multiplexor de agregar/liberar (ADM add/drop multiplexer) sustituye a los dispositivos punto a punto convencionales en las conexiones cruzadas DS1. El ADM es un multiplexor síncrono que sirve para agregar y liberar señales DS1 en el anillo SONET. El ADM también sirve para regenerar anillos en caso de que falle uno de ellos, (Villanueva, 2000).

III.8 Fast Ethernet

El crecimiento de las Redes de Área Local ha sido conducido a través de la introducción de la tecnología Ethernet, al igual que las computadoras personales disponibles en el mercado. Como resultado de lo anterior, muchas aplicaciones pueden correr ahora en una red LAN. Pero algunas pueden provocar que las redes se vuelvan más lentas, cuando se trata de redes que utilizan 10 Mbps, como en Ethernet.

La velocidad de las redes y su disponibilidad son requerimientos críticos. Con más aplicaciones que requieren mayores velocidades en una Red de Área Local para tener un modo de operación aceptable.

La demanda de velocidades de transmisión mayores para permitir el crecimiento de las redes ha sido llevada a cabo por la nueva especificación de Fast Ethernet. Esta nueva norma de Redes de Área Local ha elevado los límites de velocidad de Ethernet desde 10 Mbps a 100 Mbps, (Montenegro, 2000).

III.8.1 Tipos de Fast Ethernet

Los inventores de “Fast Ethernet” han buscado el incremento de la tasa de transmisión de 10 Mbps en múltiplos de 10. Esto ha hecho que se hayan creado dos estándares diferentes: 100Base-T y 100VGAnyLAN, (Communications World, 1997).

III.8.1.1 100Base-T

En 1993, un grupo de compañías se juntó para formar la alianza de Fast Ethernet, este grupo desarrolló la especificación 802.3, la cual fue aprobada en 1995. Los objetivos de esta alianza son:

- Mantener el protocolo de Acceso Múltiple por Detección de Portadora con Detección de Colisión (CSMA/CD) como protocolo de transmisión, este protocolo funciona de la siguiente manera: un nodo que desea transmitir espera a que el canal esté aislado, una vez que se encuentra en este estado empieza la transmisión. Si otro nodo empezara también a transmitir en este instante se produciría colisión, por lo tanto se detiene la transmisión y se retransmite tras un retraso aleatorio.
- Soportar los esquemas existentes de cableado, por ejemplo 10Base-T.
- Asegurar que la tecnología de Fast Ethernet no requerirá cambios en los protocolos de las capas superiores, ni en el “software” que corre en las estaciones de trabajo.

El objetivo principal de la alianza es el de asegurar que se pueda pasar de Ethernet tradicional a Fast Ethernet, manteniendo el protocolo tradicional de transmisión Ethernet.

La topología usada es la estrella, la transmisión está limitada a un cable de 250 metros, antes de que un dispositivo tal como un puente o ruteador se necesite para regenerar una señal. El estándar 100Base-T consiste en las siguientes especificaciones:

Capa física(3): Tres tipos de condiciones de operaciones: par trenzado no apantallado, par trenzado apantallado y fibra óptica.

Interfase Independiente del Medio (MII): Ésta es una nueva subcapa localizada sobre la capa física. Define un interfase estándar entre la capa MAC (debajo), y cualquiera de las tres capas físicas.

Control de Acceso al Medio (MAC): Está localizado debajo de la capa MII, y está basado en el protocolo CSMA/CD previamente usado en el estándar Ethernet de 10 Mbps.

III.8.1.2 100VG-AnyLan

La segunda tecnología competidora fue puesta en práctica por compañías incluyendo IBM y Hewlett Packard. Es conocida como 100VG-AnyLan (IEEE 802.12). La tecnología detrás de “Any Lan” es nueva, en lugar de usar CSMA/CD, usa un Protocolo de Acceso de Prioridad de Demanda (DPAM): un dispositivo de usuario envía un tono de control al centro de la red cuando desea enviar un paquete, y el centro sondea todos los dispositivos conectados y luego concede el acceso basado en la prioridad, proporciona dos niveles de prioridad para obtener el acceso a la LAN: *prioridad normal*, para las transferencias típicas, y *alta prioridad*, para las transferencias críticas. Este se ejecuta en cuatro pares de cables de cobre, distribuyendo los datos equitativamente en cada par.

100VG-AnyLan utiliza topología de árbol, soporta cable UTP, STP ó fibra óptica, permite una longitud de cable de 4,000 metros sin la necesidad de dispositivos que refuercen la señal. 100VG-AnyLan soporta paquetes de Ethernet y Token Ring, lo que la hace muy flexible. Sin embargo, su método de transmisión de estos paquetes difiere mucho de los métodos tradicionales. 100VG-AnyLan es un mejor protocolo para Redes de Área Local que transmite gran cantidad de datos sensibles al tiempo, tales como video y otros ficheros multimedia.

Puede argumentarse que 100VG-AnyLan no es actualmente Ethernet por completo, debido al uso de un protocolo de transmisión diferente. Los puristas de las redes reclaman que como CSMA/CD es la base completa de Ethernet, 100VG no está calificada para llamarse a sí misma Ethernet.

	100 Base-T	100 VG-AnyLAN
Complejidad	Baja	Medio-Alta
Sencillez de migración	Buena	Pobre
Transmisión	100 Mbps	100 Mbps
Diámetro máximo	450m-fibra 205m-UTP	2500m-fibra 600m-UTP,STP

Tabla 4: 100 Base-T(802.3) y 100 VG-AnyLAN (802.12).

III.9 Gigabit Ethernet

El crecimiento permanente de las redes necesita encontrar una tecnología más rápida para acomodar los anchos de banda necesarios para soportar aplicaciones que utilizan audio y video. Gigabit Ethernet es una extensión del estándar 802.3 de 10 Mbps y 100 Mbps del IEEE, fue creado por la alianza Gigabit-Ethernet (11 compañías) en 1996, corre a 1,000 Mbps, es decir 1 Gbps. Ésta puede ser utilizada para actualizar las redes dorsales (“backbones”) Ethernet existentes.

Mantiene compatibilidad con el estándar Fast Ethernet IEEE 802.3. Además fue diseñado para soportar las aplicaciones existentes, es decir, los sistemas operativos, los protocolos de comunicación como TCP/IP, etcétera. Por lo que ésta tecnología es muy similar a las antecesoras de 10 y 100 Mbps. Gigabit Ethernet fue optimizado para la capa 3, por lo que tiene más funcionalidad que las tecnologías previas, (Gómez, 2002).

III.9.1 Características de Gigabit Ethernet

- Protocolo CSMA/CD.
- Fácil migración desde Ethernet.
- 1,000 Mbps de velocidad.
- Compatible con los nodos Ethernet.
- Soporta operaciones “half duplex” y “full duplex”.
- Cableado: UTP categoría 5, STP y fibra óptica.
- Topología estrella similar a 10Base T.

La razón por la que se elige Ethernet sobre las demás tecnologías se debe a las siguientes ventajas: menor costo, escalabilidad, interoperabilidad, facilidad de uso, capacidades de monitoreos, confiabilidad y promisorio futuro.

III.9.2 Especificaciones técnicas

Las especificaciones técnicas necesarias para Gigabit Ethernet se pueden subdividir en las siguientes categorías:

Opciones de cableado: Los productos para Gigabit Ethernet fueron diseñados para operar con fibra óptica, pero más tarde fue descubierto que el cable de cobre podía ser diseñado de tal manera que operara a 1,000 Mbps. Los diferentes tipos de esquemas de transmisión disponibles para los módulos de Gigabit Ethernet son:

1000 Base SX: Es un esquema de transmisión de fibra óptica de corta longitud de onda que puede usarse con fibra óptica multimodo con un núcleo central de 50 o 62.5 micrones de diámetro; y la distancia máxima es de 220 a 500 metros.

1000 Base LX: Es similar al anterior pero con mayor longitud de onda y a su vez puede soportar mayor distancia. Usa fibra óptica multimodo de 50 o 62.5 micrones de diámetro de núcleo central. También puede usarse fibra óptica monomodo, ésta soporta distancias de 440 metros a 5 Km.

1000 Base T: Es un esquema de transmisión de 1000 Mhz. Usa cuatro pares trenzados en cables UTP de categoría 5. La transmisión a 1,000 Mbps sobre los 4 pares trenzados ha provocado muchos problemas.

Limitaciones de UTP: El UTP tiene una longitud de 100 metros. Una de las diferencias de UTP categoría 5, para Gigabit Ethernet es la utilización de cuatro pares trenzados en lugar de 2 pares trenzados. Lo que ha causado problemas en el desarrollo del estándar UTP. Algunos de los problemas son:

Atenuación: La transmisión de datos sobre 4 pares trenzados en cable UTP categoría 5 ha presentado pérdida de señal entre el transmisor y el receptor. Esta pérdida se conoce como atenuación; por lo que los diseñadores se han visto obligados a usar el rango más bajo de frecuencias para transmitir datos a la velocidad apropiada.

Ruidos: Se detectan ruidos cuando se opera con “full-duplex”, ya que el mismo alambre se usa para transmitir y recibir, lo que genera una pérdida de transmisión y recepción.

Interferencias: Son señales no deseadas que se producen entre dos alambres adyacentes, lo que es una dificultad para Gigabit sobre UTP. Por lo que se usan los cuatros pares de alambres causando posibles interferencias por cada par adyacentes a otro.

Irradiación de energía: Es necesario tener en cuenta esto porque los cables que deben usarse son sin malla protectora.

Estrategia de diseño de UTP: Un grupo de trabajo denominado "802.3 Task Force" desarrolló una estrategia para solucionar los problemas mencionados anteriormente. 1000 Base-T adoptó estas soluciones:

Niveles de Gigabit Ethernet: *Nivel 3 (del Modelo OSI)*, los dispositivos que se encuentran en este nivel son responsables de ejecutar el encaminamiento “ruteo”, es decir, el direccionamiento de los paquetes. Este nivel es conocido como el nivel de red. *Nivel 4*, es el nivel de transporte, en este nivel los dispositivos son responsables de reservar el ancho de banda para el transporte de los datos.

Calidad de servicio (QoS): Es una medida sobre la calidad de servicio de una red. Implica garantizar el ancho de banda así como la llegada de los paquetes en forma completa. Uno de los módulos en la implementación de la calidad es el Protocolo de Reservación de Recursos (RSVP); este es un protocolo que habilita una estación para requerir la reserva de un ancho de banda garantizado a través de la red. El RSVP opera en el nivel 4 del modelo OSI. Los “switches” y “routers” habilitados por RVSP reservan el ancho de banda requerido para sesión de ésta.

Clase de servicio (CoS): Implica la priorización del tráfico a través de la red. Las decisiones de demorar o lanzar un paquete puede ser priorizado por los “switches” y “routers”.

III.10 Interfase de Datos Distribuida por Fibra Óptica (FDDI)

FDDI es un estándar para transmisión de datos en Redes de Área Local que opera sobre fibra óptica a 100 Mbps. Fue definido en los años 80 por la ANSI ante la necesidad de contar con una tecnología para Redes de Área Local de gran ancho de banda, para alcanzar este objetivo fue necesaria la adopción de la fibra óptica como medio físico, a pesar de que se elevaran demasiado los costos de instalación, (Ciberhábitat, 2002).

Se puede considerar como una MAN debido a las distancias que puede soportar. Su principal utilidad es la interconexión entre ordenadores de alta velocidad y periféricos de todas las clases. Además FDDI se aplica como una red primaria, dorsal o anillo de alta velocidad de redes de cualquier tipo.

Sus características fundamentales son las siguientes:

- Protocolo de Control de Acceso al Medio (MAC) basado en el estándar IEEE 802.5 (“token ring”).
- Tiene la posibilidad tanto de usar par trenzado como fibra óptica.
- La longitud máxima del anillo de fibra es de 200 Km ó 100 Km si es doble.
- La velocidad es de 100 Mbps.
- Se pueden conectar hasta 500 dispositivos por anillo, es decir que se pueden tener hasta 1000 conexiones físicas, lo que implica tener una cuenta de doble anillo de 200 Km.
- Se puede proporcionar servicios de datos síncronos y asíncronos.

III.10.1 Componentes de la red

FDDI define el uso de un anillo doble de fibra óptica, por cada uno de los cuales el tráfico circula en un sentido diferente, [Figura 3.13]. Físicamente, cada anillo consiste en dos o más conexiones punto a punto entre estaciones adyacentes. Uno de los anillos recibe el nombre de *anillo primario* y se utiliza para la transmisión de los datos; el otro se denomina *anillo secundario* y generalmente se reserva su uso como circuito de respaldo, los componentes de este tipo de red son:

Las estaciones de clase B o de conexión simple (SAS): Es una estación conectada al anillo primario y en caso de que este fallara, podría quedar aislada la red.

Estaciones de clase A o de conexión doble (DAS): Se encuentran conectadas a los dos anillos. En caso de fallo no quedan aisladas, ya que las estaciones duales en los extremos del segmento de la red donde ocurrió el fallo son las que se encargan de restablecer el anillo.

Concentradores: Son nodos con puertos adicionales para estaciones simples. Un concentrador puede ser dual, previene que un fallo o el apagado de una SAS corte el anillo, esto es particularmente útil cuando las estaciones conectadas son computadoras personales o equipos similares que son encendidos y apagados frecuentemente, (Procedimientos-Uno S. L, 2003).

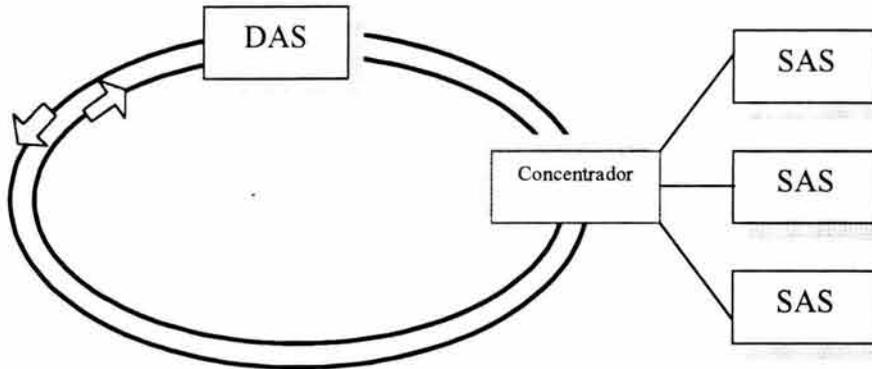


Figura 3.13 Componentes de una red FDDI.

III.10.2 Funcionamiento de FDDI

El hecho de poseer dos anillos hace que la red FDDI sea altamente tolerante a fallas. El control de la red es distribuido, razón por la cual si falla un nodo, el resto recompone la red automáticamente. En caso de que se desactivaran ambos anillos en el mismo punto por rotura u otros motivos, entonces habría que aislar el segmento del anillo en el que se ha producido la falla, de manera que las estaciones duales que se encuentran en cada uno de los extremos del segmento roto o donde se encuentra el problema se encarguen de restablecer el anillo. Lo hacen enlazando el anillo primario con el secundario, en su punto de conexión, de modo que se vuelve a tener un anillo cerrado en funcionamiento. Aunque algunas estaciones primarias podrían quedar aisladas.

En lo que respecta al funcionamiento del anillo se puede decir que por éste va circulando una trama llamada “testigo”, que da derecho a transmitir a aquella estación que haya capturado el testigo. Una vez capturado el testigo, la estación dispone de cierto tiempo para transmitir sus tramas, que se encargará de retirar de la red la propia estación emisora, tras lo cual habrá de liberar al testigo. Las tramas van circulando por la red pasando secuencialmente por las estaciones activas.

III.10.3 Trama FDDI

La normalización define el contenido del formato de la trama en términos de símbolos, donde cada símbolo corresponde con 4 bits de datos. Se usan símbolos debido a que, en la capa física, los datos se codifican en grupos de cuatro bits. Sin embargo, las entidades MAC deben tratar bits individuales, de modo que a veces se refiere a símbolos de cuatro bits y otras veces a bits individuales. Una trama distinta de una de testigo consta de los siguientes campos, [Figura 3.14] (González, 2000):

Preámbulo: Sincroniza la trama con el reloj de cada estación. La estación que originó la trama usa un campo de 16 símbolos libres (64 bits); estaciones sucesivas pueden cambiar la longitud del campo de acuerdo con los requisitos de temporización. El símbolo libre es un patrón completo de no datos. La forma real de un símbolo de no datos depende de la codificación de la señal en el medio.

Delimitador de comienzo (SD): Indica el comienzo de la trama. Se codifica como JK, donde tanto J como K son símbolos, no datos.

Control de trama (FC): Tiene el formato de CLFFZZZZ, donde C indica si la trama es síncrona o asíncrona; L indica el uso de direcciones de 16 a 48 bits; FF indica si es una trama de la Capa de Control de Enlace (LLC), de control MAC o reservada. Para una trama de control, los restantes 4 bits indican el tipo de trama de control.

Dirección de destino (DA): Especifica la estación o estaciones a las que va dirigida la trama. Puede ser una única dirección física, una dirección de grupo multidestino o una dirección de difusión. El anillo puede contener una mezcla de longitudes de dirección de 48 bits.

Dirección origen (SA): Especifica la estación que envió la trama.

Información: Contiene datos LLC o información relacionada con una función de control.

Secuencia de comprobación de trama (FCS): Comprobación de redundancia cíclica de 32 bits referente a los campos FC, DA, SA y de información.

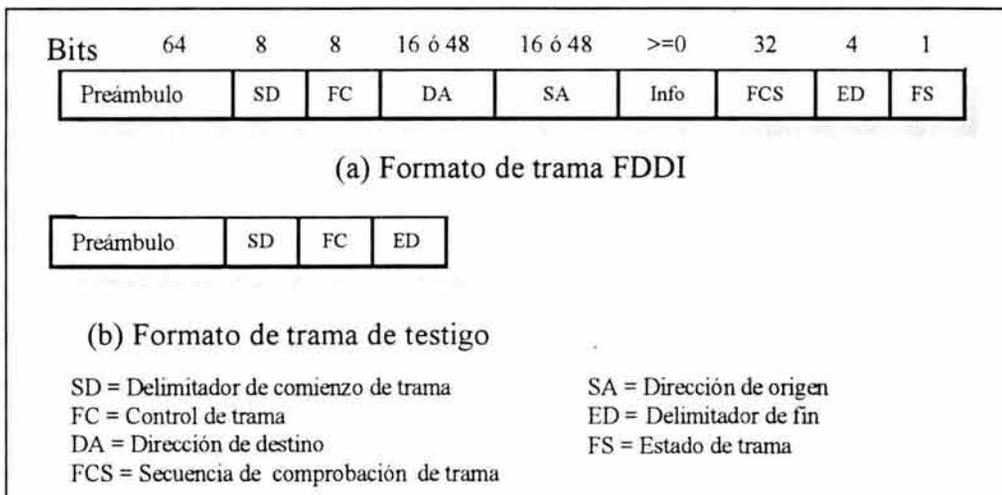


Figura 3.14 Formato de trama para FDDI.

Delimitador de fin (ED): Contiene un símbolo de no datos (T) y marca el final de la trama sin contar el campo FS.

Estado de trama (FS): Contiene los indicadores de detección de error (E), dirección reconocida (A) y trama copiada (C). Cada indicador se representa mediante un símbolo, que es R para "reinicio" o "falso", y S para "activo" o "verdadero".

Una trama de testigo consta de los siguientes campos:

Preámbulo: Tiene la misma función que en la trama general.

Delimitador de comienzo (SD): Tiene la misma función que en la trama general.

Control de trama (FC): Presenta el formato de bits 10000000 ó 11000000 para indicar que se trata de un testigo.

Delimitador de fin (ED): Contiene un par de símbolos de no datos (T) como fin de la trama de testigo.

III.10.4 FDDI II

En 1985 surgió la necesidad de una red local capaz de soportar simultáneamente voz y datos. El protocolo FDDI se reveló inadecuado para este tipo de aplicación, principalmente en redes con gran número de nodos.

Así, pues, se propuso una nueva versión de FDDI, principalmente a iniciativa de especialistas en telecomunicaciones, como la British Telecom y AT&T, también basada sobre bucles de fibra óptica. A fin de ofrecer una calidad de servicio adecuada para la voz, el protocolo FDDI II es una norma americana de la ANSI (Comité X3T9.5) que utiliza una técnica de conmutación híbrida. De esta forma, la norma FDDI II ofrece procedimientos de conmutación de circuitos para tráfico de voz y video y, de conmutación de paquetes, para los datos.

Tiene una arquitectura de circuitos conmutados para tráfico isócrono (tiempo de entrega fijo 25 ms para tráfico sensible a retardo) o asíncrono, la banda de paso está constituida por la trama asíncrona y 16 canales síncronos que contienen 96 grupos cíclicos ("cyclic groups") de 16 bytes cada uno.

El flujo síncrono alcanza, por consiguiente, $16 \times 96 \times 8 / 125 = 98.304$ Mbits, es incompatible con FDDI y es extremadamente costoso por doble circuitería (isócrono y asíncrono). Con el servicio isócrono se pueden coexistir varios ciclos en el anillo y 24 bytes del ciclo son usados para el control.

Soporta una distancia de 100 m (UTP), 500 m – 2 Km (fibra multimodo), transmisión asíncrona o síncrona usando "tokens". Utiliza un doble anillo a 100 Mbps, es inmune y no genera ruido electromagnético, (Todoteleco.com, 2001).

III.11 Cola Distribuida en Doble Bus (DQDB)

La tecnología DQDB ha tenido su origen en la Universidad de Western Australia. El Intercambio Síncrono de Colas de Paquetes (QPSX) fue desarrollado como una tecnología de distribución rápida de paquetes en 1985. En 1987, la unidad comercial de la Universidad (Unicom Research) se vinculó con Telecom Australia (Telstra) para desarrollar y comercializar la tecnología QPSX, la cual fue sometida a consideración por la IEEE por los términos de referencia de la norma 802.6. Casi inmediatamente la IEEE cambió el nombre de la tecnología por DQDB, (Correa, 2002).

III.11.1 Características

DQDB proporciona tres tipos de servicios: no orientados a conexión (datagramas), orientados a conexión e isócronos, se sugiere una longitud máxima de 160 Km, 512 nodos y una velocidad de 155.52 Mbps. La topología es en bus, normalmente utilizado en topología de bus lógico en anillo para poder reconfigurar el bus y reestablecer la operación en caso de avería en el bus. Los datos se transfieren en células con 48 octetos de carga útil y 5 octetos de cabecera, para compatibilidad con la tecnología de transferencia ATM, así como facilitar la interconexión de las redes MAN con las WAN emergentes.

Los límites de operación en DQDB se derivan del problema conocido como "falta de equidad": son atendidas más frecuentemente las estaciones más próximas a las cabeceras de los buses. Teniendo en cuenta que hay dos cabeceras, una en el extremo de cada bus, [Figura 3.15] sin embargo el rendimiento máximo se obtiene en las estaciones situadas en la mitad del bus.

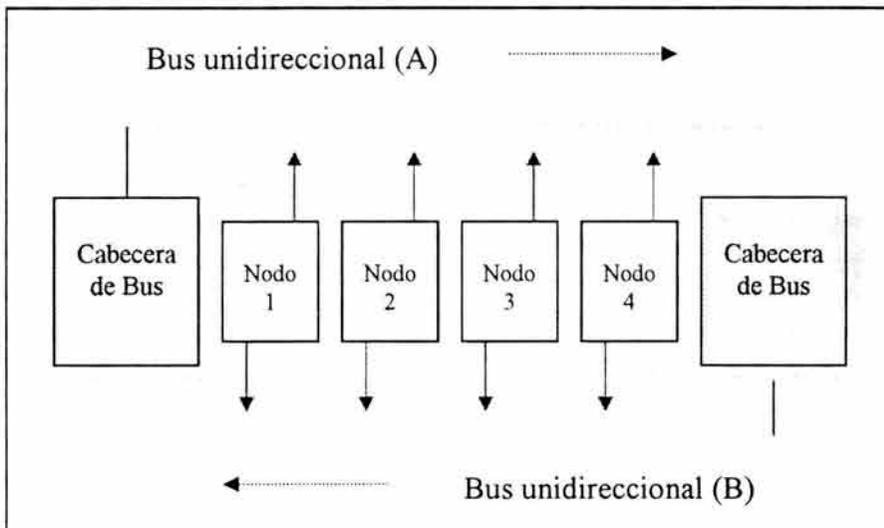


Figura 3.15 Estructura del Bus DQDB.

DQDB actualmente proporciona tecnologías de empaquetamiento rápido para la interconexión de redes LAN y de servicios de datagrama a 2 Mbps. Además es capaz de proveer transmisiones a alta velocidad, servicios de circuitos virtuales y servicio isócrono de transmisión de datos. Así mismo garantiza una trama fija de datos para distribución en aplicaciones como; teleconferencia e imágenes medicas. Las configuraciones en doble bus abierto o doble bus cerrado son posibles para DQDB. Donde las aplicaciones de datos son críticas es recomendable usar la configuración de doble bus cerrado para minimizar las fallas de tolerancia.

Si el bus está severamente dañado la red deberá ser reconfigurada hasta que el punto roto en el bus sea desviado, [Figura 3.16]. Incluso en una configuración de bus abierto existe un alto nivel de falta de tolerancia incluso desde nodos que estén lógicamente adyacentes en el bus y puedan ser desviados en el momento que una falla se presente en uno de los nodos. Los nodos adyacentes no deben ser afectados si tienen capacidad de conservar su cabecera de bus.

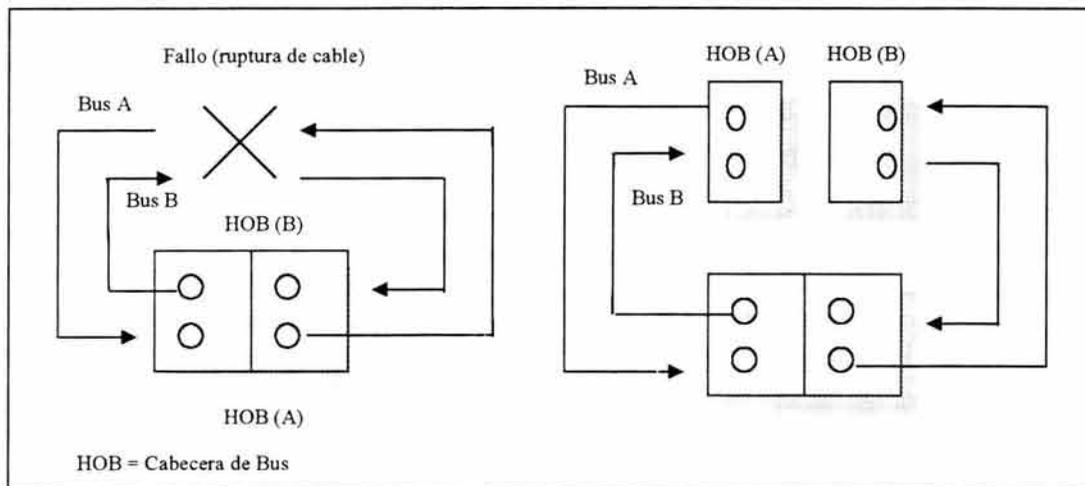


Figura 3.16 Recuperación de fallos en la topología de bus.

DQDB tiene muchas ventajas, éste ha sido aprobado como un estándar internacional (IEEE 802.6), que ofrece alta velocidad (de 2 Mbps a 300 Mbps), que permite la transmisión en diferentes medios, ofrece alto rendimiento independiente del número de estaciones encadenadas a la red. DQDB también brinda un alto nivel de seguridad para los datos.

La capa física especifica cómo utilizar los diferentes medios físicos y velocidades subyacentes. El estándar soporta diversos medios de transmisión, como los niveles 3 y 4 de PDH (34.368 Mbps y 139.264 Mbps, respectivamente), SONET Y SDH (51.84 Mbps y 155.52 Mbps para SONET y 155.52 Mbps para SDH) y DS3 (44.736 Mbps). Si bien DQDB no es hasta ahora uno de los protocolos de transmisión más populares y comerciales, seguramente en el futuro será una tecnología de amplio reconocimiento por sus capacidades de transmisión de paquetes a altas tasas de velocidad, a grandes distancias, garantizando una transmisión efectiva y confiable, (García, 2002).

III.12 Multiplexación en Longitud de Onda (DWDM)

DWDM es una tecnología óptica basada en la multiplexación de diferentes longitudes de onda (λ) generadas por diferentes emisores de luz dentro de una misma fibra óptica. De esta forma, se logra aumentar la capacidad de transmisión o ancho de banda de la fibra. Permite integrar, dentro de la misma fibra gran cantidad de enlaces independientes de alta velocidad, por ejemplo: ATM, Gigabit Ethernet, SDH, 100Base-T, etcétera.

Cuando el número de longitudes de onda que se multiplexan (también conocidos como canales) es superior a 8, esta tecnología se denomina Multiplexación en Longitud de Onda o DWDM, (Teldat.com).

Un sistema de transmisión convencional basado en fibra óptica está conformado por tres bloques:

1) La fuente que emite la señal en el rango óptico del espectro electromagnético, es decir, una fuente que emite señales luminosas y que consiste normalmente en un diodo láser.

2) El medio físico por donde se propaga y transmite esa señal luminosa, que es el cable de fibra óptica constituido por un material de un determinado índice de refracción (el núcleo) y revestido por otro material de distinto índice de refracción (el revestimiento).

3) Un dispositivo fotodetector situado en el extremo final de la fibra que capta la señal emitida por la fuente y que ha viajado a lo largo de la fibra óptica.

En DWDM, además de los bloques emisor, de transmisión y de recepción, hay un cuarto que adquiere una importancia crucial: el Amplificador de Fibra Óptica dopada con Iones de Erbio (EDFA).

El bloque emisor en DWDM está constituido por una serie de diodos láser que emiten señales luminosas a diferentes longitudes de onda; estos diodos son normalmente del tipo Regeneración Distribuida (DFB). Las tendencias en este contexto se dirigen a tratar de obtener arreglos "arrays" de láseres sobre un único sustrato como una solución para reducir costos fundamentalmente.

Estas diferentes longitudes de onda emitidas por los láseres se multiplexan mediante un equipo multiplexador y se transfieren a la fibra óptica (segundo bloque) dando lugar a diferentes canales que se pueden contemplar como diferentes fibras ópticas virtuales integradas dentro de la fibra óptica real.

Actualmente, el número de canales en los sistemas instalados es de 32 tras una secuencia que se inicia en 1993 con 4 canales para pasar en 1996 a 8 canales y a 16 en 1997. Existen proyectos de carácter experimental que utilizan más de 40 canales, llegando incluso a cerca de 80.

Las velocidades obtenidas se inscriben fundamentalmente en el entorno OC-48 de SONET con 2.5 Gbps, y en su equivalente STM-16 del entorno SDH, lo cual ha generado que OC-48 aparezca como una tecnología madura para DWDM.

Sin embargo, las tendencias se están orientando hacia niveles de “Optical Carrier” con velocidades asociadas más elevadas, como OC-192 de SONET y su equivalente STM-64 de SDH, que proporcionan velocidades de 10 Gbps y permiten afrontar la creciente demanda de ancho de banda de una manera más eficaz.

Con OC-192 se evitan los problemas y complejidad de ingeniería que supone tratar de ampliar el ancho de banda manteniéndose en OC-48 (se necesitaría en este caso aumentar considerablemente el número de elementos de red), pero impone restricciones en lo que respecta al tipo de fibra.

El tercer bloque que conforma el sistema DWDM está constituido por el conjunto de fotodetectores que reciben la radiación luminosa que ha viajado a través de la fibra. Las diferentes longitudes de onda que aparecen al final de la fibra se distribuyen mediante un dispositivo que puede ser un acoplador pasivo en estrella.

Cada receptor lleva asociado un filtro óptico sintonizable que permite eliminar las señales no deseadas (es decir, seleccionar un solo canal/longitud de onda) y minimizar el ruido generado por el amplificador EDFA encargado de regenerar las señales que han perdido potencia a su paso por la fibra.

Estos filtros están constituidos por un etalón de “Fabry-Perot” que consiste en dos espejos que forman una cavidad resonante en la que se puede seleccionar la longitud de onda. Cuando se modifica la distancia entre los espejos se modifica al mismo tiempo la longitud de onda de la luz que resuena en la cavidad, lo que constituye un medio para sintonizar el filtro.

Las distancias de transmisión que se consiguen son considerablemente elevadas gracias a la elevada potencia que proporciona el EDFA y el bajo nivel de ruido tanto para OC-48 como para OC-192. En este contexto se puede conseguir que 32 canales en OC-48 se transmitan a lo largo de 600 Kilómetros sin necesidad de regeneración; distancia que se convierte en 320 Kilómetros para OC-192.

Así, DWDM supone una solución para aumentar la capacidad de la red frente a otras alternativas utilizadas tradicionalmente por los operadores, como el aumento de la velocidad de transmisión en el escenario TDM, en base a la mejora de OC-48/STM-16 (correspondiente a SONET y SDH, respectivamente), de 2.5 Gbps, con la adopción de los actuales OC-192/STM-64, de 10 Gbps.

III.13 Problemas de las redes

Las limitaciones de algunas de las arquitecturas clásicas de redes son la capacidad de transmisión y de transferencia adecuada de tráfico. Otras redes presentan problemas en el soporte inadecuado para las aplicaciones del siglo XXI, requieren soportar aplicaciones de videoconferencia, multimedia, tiempo real, mecanismos de seguridad en la capa de red, debido a que las nuevas aplicaciones son más demandantes, requieren garantías en: los tiempos de respuesta, la disponibilidad de ancho de banda y seguridad. Por otro lado, se presenta la saturación del espacio de direcciones, es decir, la escasez de direcciones IP, lo cual limita el crecimiento de Internet y obstaculiza el uso de Internet a nuevos usuarios. El protocolo IP utilizado en la red Internet, no es fiable, ya que los paquetes/datagramas pueden ser entregados con errores, fuera de secuencia, o no ser entregados, (García, 1997).

Una cuestión importante es el multiplexado asíncrono, el cual requiere “hardware” excesivo, cada proveedor posee un sistema administrador de red propio, incompatibilidad entre proveedores, el ancho de banda depende del proveedor, la depuración de la red requiere de tiempo y gran cantidad de equipos, baja capacidad de aislamiento de los fallos en transmisión.

Por ejemplo, en las redes tipo X.25, existen las siguientes limitaciones arquitectónicas:

- En cada nodo de la red se hace necesario disponer de la totalidad de un paquete para verificar si ha sido recibido de forma correcta, esto es, sin errores, para encaminarlo al nodo siguiente de su ruta.
- Se requiere la ejecución de todos los procesos de control, tanto de errores (si alguna trama presentase errores a su recepción en algún nodo de la red, éste intentaría resolver el problema) como de flujo.
- Esta arquitectura ha sido concebida en su origen para trabajar con ETD a velocidades desde 2,400 Bps hasta 64 Kbps.
- A mayores velocidades se requeriría una capacidad de proceso en los nodos excesiva y poco práctica.
- Los procesos desarrollados en cada nodo de red son de una alta complejidad.

Para abordar el problema de la limitación del ancho de banda, han aparecido diversas técnicas:

- Arquitecturas de conmutación digital de circuitos como la RDSI-BE (Red Digital de Servicios Integrados- Banda Estrecha),
- Adaptación de las arquitecturas existentes: Fast Ethernet o Ethernet a 100 Mbps y AnyLan.
- Nuevas arquitecturas: DQDB (“Distributed Queue Double Bus”), FDDI (“Fiber Distributed Data Interface”).
- Arquitecturas de Conmutación Rápida de Paquetes: Retransmisión de tramas (“Frame Relay”).
- Arquitectura de retransmisión de células (“Cell Relay”) o tecnología ATM, utilizada en la Red Digital de Servicios Integrados -Banda Ancha (RDSI-BA).

 Capítulo 5 con más detalles.

* * *

Haciendo un breve resumen se puede decir que los métodos de comunicación de servicios son: síncrono, asíncrono e isócrono. PDH es un estándar para redes de telecomunicaciones, la idea básica es hacer una serie de multiplexaciones de señales provenientes de fuentes distintas, para así formar una señal con una tasa de transferencia superior, haciendo determinada cantidad de multiplexiones se van logrando las diferentes jerarquías propias de PDH.

SDH es otro estándar de transmisión síncrona para redes de alta velocidad y alta capacidad, diseñado para operar con ATM. Este estándar ha sido desarrollado para transportar tipos de tráfico como ATM o IP.

ATM es una técnica de conmutación rápida de paquetes, para conseguir esta conmutación de paquetes con funcionalidad mínima se basa en tener que segmentar toda la información que transmite a un tamaño estándar de celda pequeño para facilitar las operaciones de conmutación. Permite el manejo sencillo de tráfico de datos, audio y video. En ATM los canales se identifican por el ancho de banda variable asignado bajo demanda.

Con el desarrollo de las nuevas redes de comunicaciones se puede ver el problema de las redes múltiples. Esto se debe a que hay que mantener el antiguo servicio telefónico ordinario, la red antigua de circuitos conmutados, los nuevos servicios de datos, en consecuencia, mantener todas estas redes individuales es complicado. Como solución a esto, se busca una nueva red única para todos los servicios, debe tener una velocidad de transmisión elevada (comparada con las existentes) y debe permitir una gran variedad de servicios nuevos, a esta solución se le llamó RDSI-BA. ATM es el modo de transporte en una red RDSI-BA, tiene su propio modelo de referencia, diferente del modelo OSI y también del modelo TCP/IP.

El crecimiento permanente de las redes necesita encontrar tecnologías más rápidas para acomodar los anchos de banda necesarios para soportar aplicaciones que utilizan audio y video, para abordar este problema, han aparecido diversas técnicas como: la RDSI-BA, Fast Ethernet, Gigabit Ethernet, DQDB, FDDI, DWDM, etcétera.

En el siguiente capítulo hablaremos de la administración de redes y algunas de sus aplicaciones en las telecomunicaciones, así como los diversos factores que intervienen a la hora de administrar una red.

CAPÍTULO 4:

APLICACIÓN DE LA ADMINISTRACIÓN DE REDES A LAS TELECOMUNICACIONES

IV.1 Introducción

La combinación de las telecomunicaciones y computadoras ha sido la base para la organización actual de los sistemas computacionales. Y con la explosión de las redes LAN y WAN sobre TCP/IP, las redes corporativas y el ambiente cliente-servidor, los administradores de redes necesitan soluciones para minimizar el tiempo de caída de las mismas y maximizar su productividad.

¿Y por qué administrar una red?. Porque las operaciones de una empresa dependen más de las redes y las redes son cada vez más complejas. Dentro de los objetivos de la administración encontramos lo siguiente: Asegurar que los usuarios de una red reciban el servicio con la calidad que ellos esperan, la planeación estratégica de la ingeniería, operaciones y mantenimiento de una red y sus servicios para ayudar al personal encargado a enfrentar las complejidades de la red y asegurar que la información se mueva a través de ella con la máxima eficiencia y transparencia para los usuarios.

IV.2 Conceptos de Centros de Operación de Red (NOC)

Los Centros de Operaciones de Red, conocidos como NOC por sus siglas en Inglés (“Network Operation Center”) son cualquier centro al que se le haya dado la tarea de administrar los aspectos operacionales de una red. El NOC es el encargado de monitorear el comportamiento de la red así como darle el mantenimiento necesario, mantener funcionando de manera eficiente la interconexión de las redes locales, los enlaces de área amplia y la columna vertebral (“backbone”), proporcionar apoyo a los administradores de redes locales para solucionar sus problemas de intercomunicación con otras redes; el NOC también se encarga de estudiar el desempeño de la red y participar en las tareas de configuración, mantenimiento e implementación de las nuevas tecnologías. El objetivo primordial del NOC es mantener en óptimas condiciones la operación de la red y de los dispositivos conectados a ella.

IV.2.1 Actividades del NOC

Las actividades más importantes que desarrolla un Centro de Operación de Red son las siguientes:

Monitoreo: El monitoreo es una de las partes fundamentales de la administración de las redes. Sus tareas comprenden, entre otras cosas, la extracción e interpretación de datos relacionados con el estado y el desempeño de los dispositivos conectados a la red. Mediante su correcta interpretación, y llevando un registro histórico de los acontecimientos que se van dando a lo largo del tiempo, el administrador de red podrá determinar de manera más rápida el comportamiento de ciertos equipos e incluso, adelantarse y predecir el deterioro del nivel de servicio en alguna parte de la red.

Tarificación: Se refiere a contabilizar el tráfico generado en la red. Los sistemas de monitoreo recolectan esta información para ser almacenada en una base de datos que es accedida por programas desarrollados en el Centro de Operación de Red.

Generación de estadísticas: Su función es informar a los administradores de red, el desempeño de sus enlaces y la capacidad con la que se están ocupando. De esta manera, cada administrador va a poder contar con un historial del desempeño y ocupación de su enlace; lo cual contribuye a la correcta planeación de su crecimiento.

Administración de equipos de ruteo: Otra actividad que se realiza en el NOC, es la administración de los equipos de ruteo. Estos dispositivos son los encargados de dirigir la información de un lado a otro por la ruta más óptima. Por otro lado, la administración de estos dispositivos contempla, también, el manejo de sistemas de seguridad como muros de fuego ("firewalls") y listas de acceso. Para esto el NOC cuenta con sistemas que guardan un registro de los usuarios que establecieron comunicación con los equipos de ruteo, ya que naturalmente este tipo de accesos deben ser restringidos. Así pues, solo el personal del Centro de Operación de Red puede tener acceso para hacer cambios en las configuraciones, asegurando así su buen funcionamiento.

Seguimiento de reportes ("Troubleshooting"): El Centro de Operación de Red realiza la atención de reportes de fallas. Una falla en la red, significa que algún dispositivo dentro de la misma no se desempeña como se espera y que por lo tanto se le debe poner atención hasta que se normalice su funcionamiento. El NOC se encarga de minimizar el número de fallas y reducir el tiempo de resolución de las mismas.

Las actividades básicas a desarrollar durante el seguimiento de reportes son:

- Detección de la falla.
- Diagnóstico de la falla.
- Determinación de la falla.
- Resolución de la falla.

En la detección de la falla: Se cuenta con sistemas que despliegan en monitores, de manera gráfica o textual, los problemas existentes en la red.

En el diagnóstico de la falla: Intervienen una serie de herramientas de prueba (tanto de "software" como de "hardware") que proporcionan información necesaria para determinar qué es lo que está provocándola.

En la determinación de la falla: Cuenta mucho la experiencia del personal del Centro de Operación de Red y de la ayuda de los sistemas de manejo de reportes, que llevan la historia de los casos resueltos con anterioridad. Estos sistemas cuentan con bases de conocimiento que se van enriqueciendo con las experiencias de los operadores que constantemente resuelven problemas en la red, y pueden proporcionar información relativa a la solución de problemas recurrentes.

Resolución de la falla: Una vez que se han detectado las causas que ocasionaron las fallas, el siguiente paso será la resolución del problema en la red. Con esto, se garantiza la rápida solución de los problemas que se presentan comúnmente en las redes de datos, (UNAM, 2002).

IV.3 Conceptos de “Call Center”

Un Centro de Llamadas o atención denominado también (“Call Center”), es un lugar en donde se recogen las llamadas masivas con destino a una empresa o servicio y que, al mismo tiempo, sirve para realizar llamadas salientes. Para muchas empresas se ha convertido en el principal medio de contacto con sus clientes, (Huidobro, 2000).

El Centro de llamadas (“Call Center”) es una solución que se deriva del concepto de la Integración Computador-Teléfono (CTI), es decir, la interacción física y funcional entre un sistema telefónico y un sistema informático que facilita el intercambio de información, teniendo esto en cuenta, podemos definir un “Call Center” como: el conjunto tecnológico y administrativo que permite unificar la inteligencia y potencia de procesamiento de los sistemas informáticos y las facilidades de la conmutación de llamadas telefónicas, (Arenas, 2000).

IV.3.1 Arquitectura Integración Computador-Teléfono (CTI)

Opera de la siguiente manera: Un llamante conectado a la Red Pública Telefónica marca el número con el cual quiere comunicarse, la central telefónica transfiere la llamada al Sistema Interactivo de Respuesta de Voz (IVR) conectado a ésta, para que le ofrezca (en una estructura de menús) los diferentes servicios de información al llamante (incluida la atención personalizada de un agente).

Si el llamante escogiera la opción de ser atendido de manera personalizada, entonces el Sistema Interactivo de Respuesta de Voz ejecutará dos acciones concurrentes: por una parte, pedirá al servidor CTI (conectado a la central telefónica mediante enlace de datos) transferir la llamada que está atendiendo, a un anexo telefónico (en el escritorio del agente) y al mismo tiempo suministrará la identificación del llamante a fin de que el servidor CTI extraiga de la base de datos toda la información concerniente y la envíe a la estación de trabajo del agente cumpliendo la función denominada "screen-pop". De esta forma, en la estación de trabajo del agente se recibirá la llamada telefónica del usuario y aparecerá en la pantalla de la computadora del agente toda la información del llamante que mantiene la base de datos de la organización.

La recepción de llamadas telefónicas se hace mediante un número de red inteligente (por ejemplo, 9XX) que la empresa contrata y es único para todo el territorio nacional; este número tiene su terminación en otro de 9 cifras perteneciente a la Red Telefónica Conmutada (número de cabecera), pudiendo ser distinto según la procedencia de la llamada, la hora del día o del año. La diferencia entre los distintos números o líneas 9XX radica en como se paga por cada modalidad, siendo a veces con costo por ambas partes o solo para el usuario que llama. En la contratación se paga una cuota de alta inicial y otra mensual (más alta si se elige el número), y un costo en función del número de llamadas realizadas y su duración.

IV.3.2 Componentes de un “Call Center”

En la configuración de un “Call Center” se pueden distinguir los siguientes componentes, [Figura 4.2]:

Central Telefónica (PBX): La centralita telefónica es el elemento básico de toda la infraestructura. Su misión es conectarse a la Red Telefónica Conmutada (RTC) y administrar las extensiones telefónicas corporativas internas, facilitando la comunicación de éstas entre sí y con el exterior (líneas).

Servidor CTI: Coordina todos los componentes “hardware” y “software” del “Call Center” (une la infraestructura informática corporativa y la telefónica), [Figura 4.1]. Cuando la llamada llega a la operadora, en su pantalla aparece la plantilla con toda la información del cliente. Así, se libera al operador de tareas repetitivas (identificación del cliente) y le permite centrarse en el objetivo establecido con el cliente. Es este servidor el que, por ejemplo, define y adscribe a los agentes telefónicos al correspondiente Distribuidor de Llamadas Automático (ACD), imparte órdenes para el envío de información a los diferentes puestos de los agentes, o almacena y estructura la información para los diferentes reportes de operación que se requiera.

- Identificación de llamadas
- Encaminamiento de llamadas
- Transferencia sincronizada de voz y datos al puesto de agente
- Gestión de funciones telefónicas
- Llamadas salientes
- Seguimiento: workflow

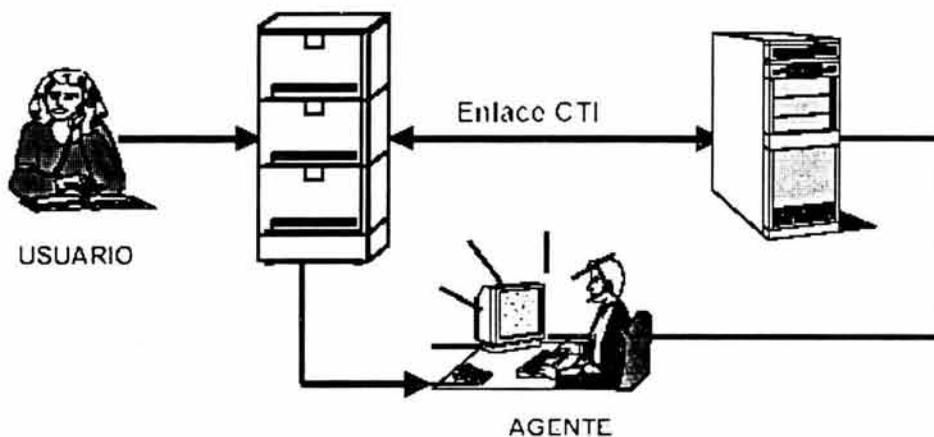


Figura 4.1 Enlace PBX-Ordenador.

Distribuidor de Llamadas Automático (ACD): Este equipo permite administrar grupos de agentes con distintas tareas y competencias, así como crear colas de tamaño variable para administrar los clientes que esperan ser atendidos. Todo ello tiene como objetivo fundamental incrementar la eficiencia y la productividad, repartiendo el trabajo equitativamente entre los operadores.

Unidad de Respuesta de Voz (VRU): Sus funciones son muy diversas y abarcan desde el ofrecer información a través de mensajes simples (“telephone notice board”) hasta aplicaciones interactivas (“telephone orders”). Resulta un elemento clave para desarrollar servicios automáticos sin sobrecargar a los operadores (por ejemplo, cuando el centro de servicios no está siendo atendido por personal alguno).

Sistema Interactivo de Respuesta de Voz (IVR): Conjunto de “hardware” y “software” que se encarga de la administración de llamadas entrantes (“inbound”) en una organización. Es éste el sistema que permite y facilita la entrega de mensajes hablados a los llamantes de tal forma que éstos puedan acceder a la información residente en las bases de datos de las organizaciones. El IVR es el elemento al cual se le asignan los trabajos de suministro de información rutinaria, dejando para los agentes la atención especializada y específica de los requerimientos de los llamantes.

Sistema de Correo de Voz (VMS): Soporta funcionalidades de contestador avanzado y la posibilidad de Marcación Interior Directa (DDI).

Servidores de Bases de Datos: En estos servidores se almacena la información de los clientes de una organización.

Estación de trabajo de los agentes: Cada uno de los puestos de operación donde se ubican los agentes telefónicos para realizar su trabajo de interacción con los llamantes.

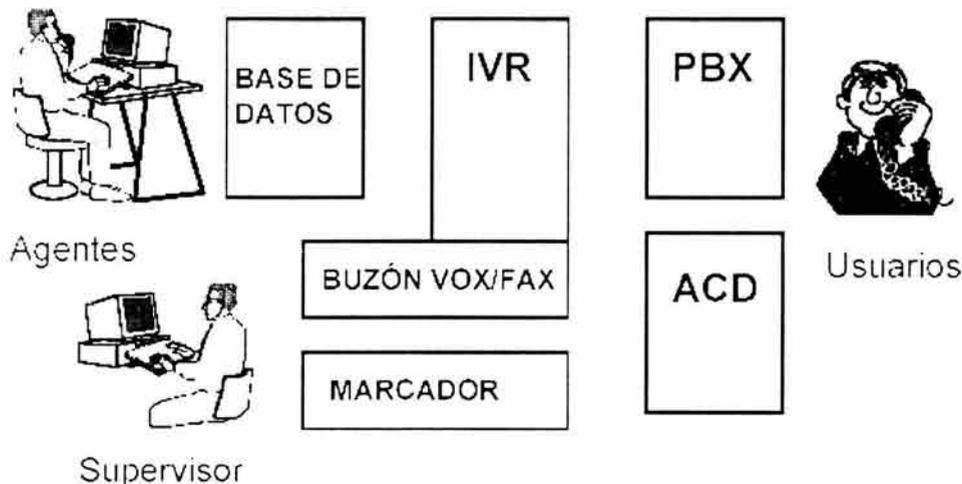


Figura 4.2 Componentes de un Call Center.

IV.3.3 Tipos de “Call Center”

Existen varios modos de realizar un “Call Center”, dependiendo de si la PBX está disponible o no:

Configuración “Stand alone”: No necesita una PBX externa y se caracteriza por maximizar el rendimiento de la inversión ofreciendo todas las funciones de un Centro de Llamadas avanzado.

Configuración “con PBX”: El servidor CTI está conectado a una PBX a través de varios tipos de conexión utilizando protocolos de comunicaciones telefónicas.

Según la topología de la conexión podemos distinguir tres tipos:

1. “Call Center” Distribuido: El soporte del estándar H.323 para la telefonía IP (VoIP) y del protocolo de intercambios de señalización SS7 permite realizar el Centro de Atención al Cliente Virtual. Para evitar el cese del servicio en caso de bloqueo, es posible equiparse con un sistema de respaldo que reemplace al sistema primario de manera transparente (“clustering”). Un servicio especial realinea los datos variables del sistema primario en el sistema de respaldo (configuración y estadísticas) y una señal de control especial (“watchdog”), permite encontrar el fallo o el bloqueo. En este caso, un dispositivo conmuta todas las líneas de una máquina a otra con el fin de garantizar el mismo servicio que la máquina primaria, quizás con un número de líneas de operadores menor.

Estándar H.323

La unión Internacional de Telecomunicaciones (ITU) tiene un número de recomendaciones para las series H. La recomendación particular de la serie H para VoIP es: H.323. La especificación H.323 fue aprobada en 1996 por la ITU. La versión dos fue aprobada en 1998 el estándar es extenso e incluye tanto equipos de computo personales como equipos multiusuario. H.323 también tiene un control de dirección de llamadas, manejo de multimedia y ancho de banda con interfases que permiten conectar Redes de Área Local con redes de otro tipo.

H.323 ha sido de hecho el estándar para la interoperabilidad entre diferentes productos en tiempo real para la comunicación sobre IP. La comunicación en tiempo real puede ser voz, video, etcétera. Organizaciones como IBM, Intel, Microsoft, Netscape y Cisco, forman parte del comité H.323.

H.323 es un estándar que especifica los componentes, protocolos y procedimientos que proporcionan servicios de comunicación multimedia (audio en tiempo real, video y comunicación de datos), sobre paquetes en red, incluyendo IP basado en redes. H.323 es parte de las recomendaciones para la familia de ITU-T llamadas H.32X que proporciona servicios de comunicación multimedia en una gran cantidad de redes. El Estándar incluye componentes para activar, mantener y terminar una conexión de voz, videoconferencia, etcétera.

2. PBX digital: Es un servicio completamente “software” (Soft-PBX) que actúa como una matriz de conmutación entre las extensiones y las líneas externas. Todas las operaciones telefónicas son realizadas a través del módulo PBX, el cual interactúa con los otros módulos de “software”, particularmente con aquellos que administran el “hardware” y los canales de comunicación. Las funciones principales son:

Transferencia Ciega (“flash hook”): El operador selecciona el número al que la llamada tiene que ser transferida y cuelga sin comprobar si hay una respuesta.

Transferencia comprobada: En este caso, el operador comprueba no sólo si hay respuesta si no también la persona a la que la llamada ha sido transferida, por ejemplo, para informarle de la razón de la llamada.

Respuesta por ausencia: Esta función es para contestar directamente desde el teléfono propio una llamada entrante de otro teléfono, por ejemplo; de un compañero que se ausenta momentáneamente.

Música de espera: La PBX puede elegir música de una fuente externa o interna (grabadora, memoria ROM) y ponerla en línea mientras el cliente espera.

No molestar: Cuando esta función está activa, en vez de sonar el teléfono el sistema lanza un mensaje predefinido, o bien permite dejar un mensaje.

Desvío si ocupado: Cuando la línea está ocupada, la siguiente llamada se envía a otro número de teléfono, bien sea interno o externo.

Conferencia: Esta función se utiliza para crear o mantener conferencias, cada teléfono dependiendo de la accesibilidad autorizada, puede crear y/o mantener conferencias.

Intrusión (Silencio): Esta función es utilizada normalmente por el supervisor del “Call Center” mientras los operadores se están formando, y consiste en que el supervisor puede escuchar la conversación que está siendo mantenida.

Menú personalizado: Es posible para usos especiales, asociar códigos numéricos a aplicaciones particulares desarrolladas en el sistema.

3. ACD Multimedia: Se trata de un servicio optimizado que cubre todo lo relacionado con el cliente: con una sola herramienta, el operador es capaz de administrar todos los canales de comunicación, reduciendo el tiempo de respuesta a los problemas, algunas de sus funciones y ventajas son:

Aumento de la eficiencia: Uno de los aspectos más críticos a la hora de evaluar el funcionamiento de un “Call Center” es la división adecuada del trabajo entre los diferentes agentes.

El servicio de ACD reparte los contactos entre los agentes uniformemente, supervisa la administración de los grupos de agentes dependiendo de las capacidades del personal y su localización. Todo ello permite ajustar los recursos para atender las necesidades específicas de los clientes. Además, el servicio ACD multimedia redistribuye en los agentes disponibles las llamadas entrantes (“inbound”) procedentes de la PBX, la web y el correo electrónico, y las llamadas salientes (“outbound”) son generadas automáticamente por el proceso automático de marcación. Esta característica permite al supervisor decidir si algún grupo de operadores debe recibir más llamadas de otro grupo, suspendiendo o reduciendo la prioridad de las acciones que llegan del módulo principal. Todos los datos estadísticos relativos al tráfico telefónico se almacenan en una base de datos y pueden ser visualizados o impresos en tiempo real.

Respuesta audible: El servicio VRU (Unidad de Respuesta de Voz) es responsable de todos los servicios que tienen que ser ofrecidos sin el soporte de ningún operador. El cliente llamante es recibido en un entorno con el que interactúa de manera organizada gracias al tono multifrecuencia, que genera su teléfono, o comando de voz. De acuerdo con las elecciones realizadas por el cliente, el sistema escoge el mensaje apropiado; el usuario puede en cualquier momento interrumpir cada mensaje mandado, para acortar la interacción. La aplicación VRU soporta un número amplio de aplicaciones, algunas de las cuales son las siguientes:

- Síntesis de números y fechas dinámicas.
- Reconocimiento de Voz Automático multilingüe (ASR): Este servicio permite reconocer, independientemente de la voz del usuario, números, palabras e incluso frases específicas en un diccionario durante la etapa de configuración.
- Reconocimiento del Cliente (SR): Permite reconocer unívocamente al cliente que llama basándose en su tono de voz.
- Síntesis de Texto multilingüe (TTS): El mensaje de voz es sintetizado directamente de un texto.

Mensajería unificada: Es capaz de dar uniformidad a todos los mensajes, para utilizarlos con una única herramienta. Cualquier mensaje puede ser recibido en formato electrónico manejable en el escritorio como una cuenta única. Teniendo acceso a una Unidad de Respuesta de Voz especial y navegando por un menú interactivo, es posible escuchar un mensaje de voz del correo electrónico sintetizado gracias al servicio de Texto a Voz, e incluso el contenido de un fax.

Campanas de Telemarketing: Otra función propia de un centro de llamadas es la de generar llamadas salientes (emisión) usando una lista de números a contactar, que son marcados automáticamente y solo cuando se tiene éxito se traspasa la llamada a uno de los agentes libres, esta operación tiene un alto riesgo pues puede que no exista un agente libre en este momento, lo que obliga a cancelar la llamada e intentarlo de nuevo más tarde, (Huidobro, 2000).

Voz sobre el protocolo IP (VoIP): El “Call Center” es capaz de recibir todas las llamadas de teléfono vía Internet y debe estar preparado para administrarlas, utilizando las mismas herramientas y procedimientos, que si llegan a través de la Red Telefónica Conmutada.

VoIP: Especifica la transmisión de tráfico de voz en “paquetes IP”, usando una red de transmisión de datos para telecomunicaciones. Los términos Voz sobre IP e IP para telefonía son usados para describir los diferentes servicios en tiempo real, tales como voz, video y fax. Especialmente la voz, la cual es manejada sobre redes TCP/IP.

¿Qué se Requiere para usar Telefonía IP?.

Cuando se usa telefonía IP o VoIP, se requieren terminales, [Figura 4.3]. Esas terminales pueden ser “hardware” o “software”, normalmente conectadas a redes telefónicas públicas o privadas, y en algunos casos las puertas de enlace (“gateways”) son requeridas, o bien las terminales pueden ser conectadas directamente hacia la red IP. En este caso las terminales ya traen implementado: un codificador y decodificador con condiciones de direccionamiento.

En terminales basadas en sistemas de telefonía clásica, los datos son direccionados a través de circuitos y los datos son acomodados en pequeños paquetes, cada uno con su propia etiqueta de dirección asegurando una correcta entrega.

La telefonía IP tiene la capacidad de acomodar todas las posibles terminales con líneas existentes a través de puertas de enlace (“gateways”) tanto en telefonía tradicional como en telefonía inalámbrica.

Los paquetes y programas que actualmente se utilizan en la telefonía IP contienen funciones para codificar y decodificar información, direccionar rutas adecuadas y realizar funciones multimedia, que permitan la optimización de los recursos.

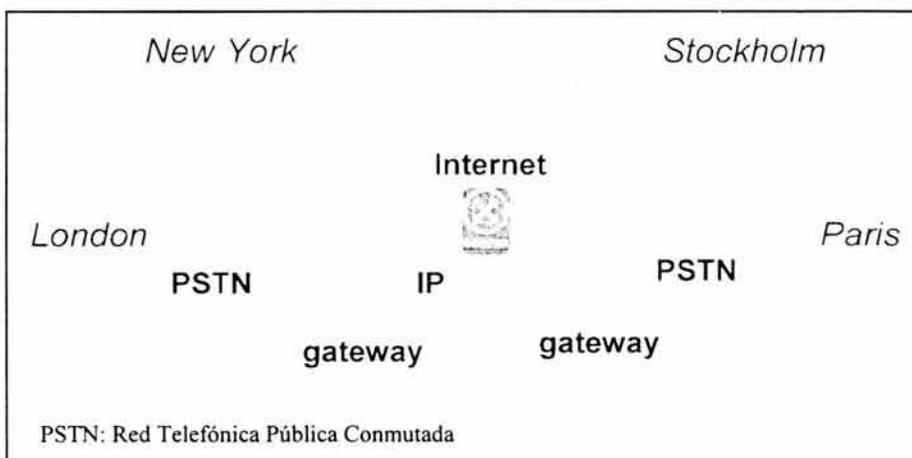


Figura 4.3 Telefonía IP.

IV.4 Administración de Redes TCP/IP

Los protocolos de administración de redes fueron desarrollados para permitir a los administradores manejar los dispositivos, dar seguimiento a los eventos críticos de la red y coleccionar información relacionada con las tendencias de crecimiento de las rutas de comunicación así como del desarrollo de la red y todo desde una estación de administración centralizada. El primer protocolo de administración de redes no propietario que ha sido ampliamente aceptado fue desarrollado por la comunidad Internet para el uso del conjunto de protocolos TCP/IP. Inicialmente, se crearon para satisfacer necesidades básicas. Por ejemplo, para realizar el manejo centralizado del crecimiento local de direcciones IP asociadas a ruteadores en una red global Internet.

El grupo de estudio conocido como Fuerza de Trabajo de Ingeniería en Internet (IETF) fue asignado al problema del manejo de ruteadores en Internet. Este grupo diseñó una plataforma de trabajo que vino a constituir la fundación del conjunto de protocolos de manejo, Protocolo Simple de Administración de Red (SNMP). Dos de los criterios más importantes, que son utilizados en los protocolos de manejo de red, y que son parte del diseño de la plataforma de trabajo SNMP, son [Figura 4.4]:

1. El protocolo no debe aumentar significativamente el tráfico en la red para satisfacer las necesidades de administración.
2. El agente de protocolo, en el dispositivo de manejo, no debe disminuir las capacidades de operación básicas o primarias que deba satisfacer el dispositivo en el trabajo que tenga asignado. Un mínimo de ciclos de CPU y de memoria deben ser utilizados para propósitos de manejo o administración.

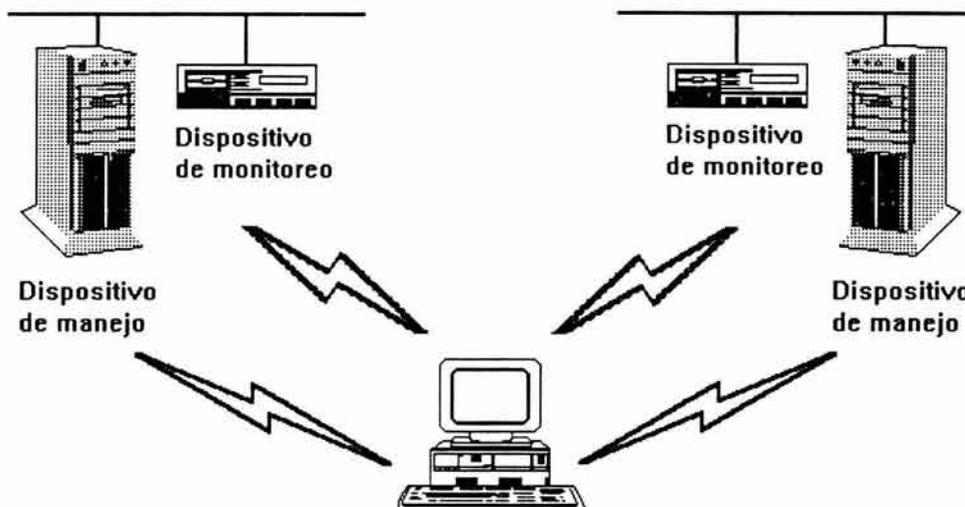


Figura 4.4 Organización y Administración.

IV.5 Sistema de Administración de Redes (NMS)

Un sistema de administración de red es una colección de herramientas para el monitoreo y control de redes, está compuesto por [Figura 4.5]:

Estación de Administración: Es un dispositivo que sirve como interfase entre la persona encargada de la administración de la red y el sistema de administración de red. Esta estación debe tener como mínimo:

- Un conjunto de aplicaciones de administración para análisis de datos, recuperación de fallas, detección de alarmas, estadísticas, etcétera.
- Una interfase a través de la cual la persona encargada de la administración de la red pueda monitorear y controlar la red.
- La capacidad de trasladar los requerimientos del administrador a los dispositivos remotos que conforman la red.
- Una base de datos de información de administración de la red extraída a partir de las bases de datos de todas las entidades administradas en la red.

Agentes: Son un elemento clave de una plataforma, como: concentradores, ruteadores, puentes y nodos, pueden estar equipados con un agente de “software” el cual puede ser manejado desde una estación de administración. Estos elementos se almacenan en unas estructuras de datos llamadas MIB. El agente responde a solicitudes de información y de acción que provienen de la estación de administración, y puede proveer asincrónicamente información importante a la estación de administración.

Base de Información de Administración (MIB): Las características de los componentes de la red son representadas mediante objetos, (normalmente, son enteros, pero también pueden almacenar cadenas de caracteres o estructuras más complejas como tablas). Cada objeto es, en esencia, una variable de datos que representa un aspecto del agente en cuestión. La colección de objetos se define como MIB. La estación de administración ejecuta las funciones de monitoreo recuperando el valor de los objetos MIB, además, la estación de administración puede ejecutar una acción que se ejecute en un agente, o puede cambiar la configuración original de un agente modificando el valor de variables específicas.

Las variables MIB registran el estado de cada red conectada, las estadísticas de tráfico, el total de errores encontrados y el contenido actual de las estructuras internas de datos, (Comer, 1995).

Protocolo de Administración de Red: Es el encargado de enlazar la estación de administración y los agentes. El protocolo utilizado para la administración de redes TCP/IP es el Protocolo Simple de Administración de Red (SNMP).

Para redes basadas en el Modelo OSI, se usa el Protocolo de Información de Administración Común (CMIP). Una posterior versión de SNMP llamada SNMPv2 pretende administrar redes TCP/IP y OSI.

La esencia de SNMPv2 radica en que es un protocolo de administración que es utilizado para intercambiar información de administración.

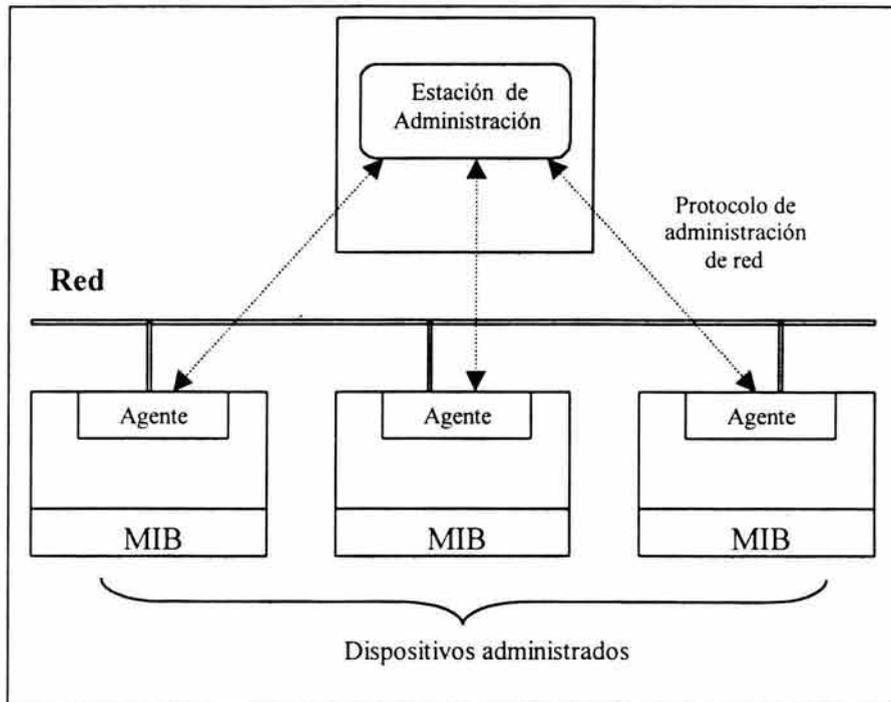


Figura 4.5 Sistema de Administración de Redes (NMS).

Cada componente en la red mantiene una base de datos local (MIB) con información relevante para la administración del comportamiento de la red.

El estándar SNMPv2 define la estructura de esta información y los tipos de datos aceptables; esta definición se conoce como Estructura de Información de Administración (SMI). El SMI presenta el marco general dentro del cual se define y construye el MIB, identifica los tipos de datos que son utilizados en el MIB y cuáles recursos dentro del MIB son representados y nombrados. Existen tres elementos claves en la especificación del MIB en la actualidad, éstos son:

- En el nivel más bajo, especifica los tipos de datos que pueden ser almacenados.
- En el nivel medio, especifica una técnica formal para definir objetos y tablas de objetos.
- En el nivel más alto, provee un esquema para asociar un identificador único con cada objeto en el sistema.

IV.5.1 Protocolo Simple de Administración de Red (SNMP)

Diseñado en los años 80's, su principal objetivo fue el integrar la administración de diferentes tipos de redes mediante un diseño sencillo y que produjera poca sobrecarga en la red.

SNMP opera en el nivel de aplicación, utilizando el protocolo de transporte TCP/IP, por lo que ignora los aspectos específicos del "hardware" sobre el que funciona. La administración se lleva a cabo al nivel de IP, por lo que se pueden controlar dispositivos que estén conectados en cualquier red accesible desde la Internet, y no únicamente aquellos localizados en la propia red local. Evidentemente, si alguno de los dispositivos de encaminamiento con el dispositivo remoto a controlar no funciona correctamente, no será posible su monitorización ni reconfiguración.

El protocolo SNMP está compuesto por dos elementos: el agente ("agent"), y el administrador ("manager"). Es una arquitectura cliente-servidor, en la cual el agente desempeña el papel de servidor y el administrador hace el de cliente.

El agente es un programa que ha de ejecutarse en cada nodo de red que se desea administrar o monitorizar. Ofrece una interfase de todos los elementos que se pueden configurar. Estos elementos se almacenan en unas estructuras de datos (MIB). Representa la parte del servidor, en la medida que tiene la información que se desea administrar y espera comandos por parte del cliente.

El administrador es el "software" que se ejecuta en la estación encargada de monitorizar la red, y su tarea consiste en consultar los diferentes agentes que se encuentran en los nodos de la red y los datos que estos han ido obteniendo.

La posibilidad de ampliación del protocolo está directamente relacionado con la capacidad del MIB de almacenar nuevos elementos. Si un fabricante quiere añadir un nuevo comando a un dispositivo, como puede ser un ruteador, tan sólo tiene que añadir las variables correspondientes a su base de datos (MIB). Casi todos los fabricantes implementan versiones agente de SNMP en sus dispositivos: ruteadores, concentradores, sistemas operativos, etcétera, (Guerrero, 1998).

Se definen seis mensajes que pueden enviarse sobre el protocolo SNMP intercambiados entre los agentes y los administradores, y son los siguientes, [Figura 4.6]:

1. **Get Request:** Es la solicitud de un administrador al agente SNMP para que envíe los valores contenidos en el MIB de una o mas variables.
2. **Get Next Request:** Es una petición del administrador al agente SNMP para que envíe los valores del MIB que se refieren al siguiente objeto del especificado anteriormente.
3. **Get Response:** Es la respuesta del agente SNMP a la petición del administrador.
4. **Set Request:** Es una petición del administrador al agente SNMP para que éste cambie algún valor contenido en el MIB que se refiera a un objeto determinado.

5. **Inform Request:** Mensaje de administrador a administrador donde se describe el MIB local.
6. **Trap:** Es un mensaje espontáneo del agente SNMP al administrador, cuando éste detecta una condición predeterminada, como la conexión o desconexión de una estación, o la caída de un enlace, etcétera.

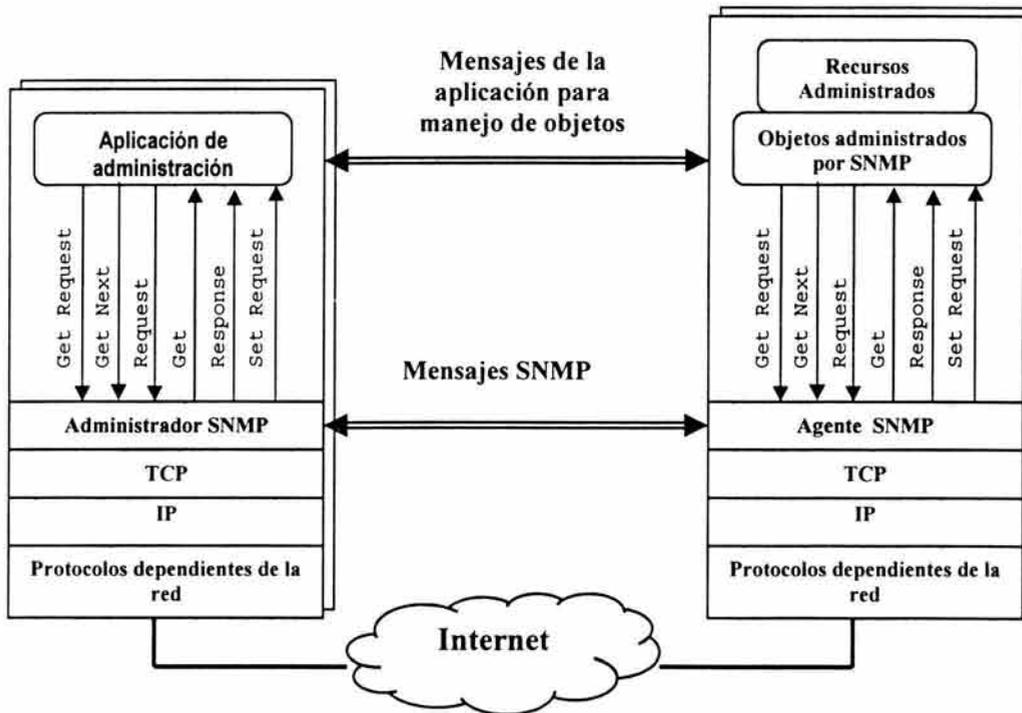


Figura 4.6 Funcionamiento de SNMP.

SNMP está orientado a monitorear y configurar el equipamiento físico de una red (puentes, ruteadores, concentradores y estaciones de trabajo). Cabe mencionar que el SNMP no sólo sirve para monitorear y/o configurar variables de los equipamientos de la red física sino también para mostrar el tráfico histórico en forma gráfica (con ayuda de las plataformas de administración) acerca de lo se ha "tarificado" por los equipos de la red.

SNMP fue diseñado específicamente para ser un protocolo de transporte independiente. Lo que significa que las solicitudes de SNMP sobre los agentes pueden hacerse utilizando cualquier protocolo de transporte como TCP/IP o cualquier otro.

SNMP al pertenecer a una arquitectura tipo TCP/IP no es abierto y por lo tanto es mucho menos vulnerable.

IV.5.2 Concepto de MIB I

La Base de Información de Administración (MIB I), es un conjunto de variables, llamadas objetos, almacenadas y organizadas de manera jerárquica, definido en el RFC 1156. Los MIB's son accedidos por protocolos de red como el SNMP. La comunicación entre el protocolo y el MIB (elemento de almacenamiento virtual), es a base de consulta-respuesta, (Sampieri, 2000).

A través del MIB se tiene acceso a la información para la administración, contenida en la memoria interna del dispositivo en cuestión. MIB es una base de datos completa y bien definida, con una estructura en árbol, adecuada para manejar diversos grupos de objetos (información sobre variables/valores que se pueden adoptar), con identificadores exclusivos para cada objeto, (Huidobro, 2002). La MIB I constituye la primera MIB normalizada. Está formada con objetos de los protocolos de TCP/IP. En la siguiente tabla se especifican los grupos que la forman, con el número de objetos que forma cada grupo, (Barba, 2001):

Grupo	Número
System	3
Interfaces	22
ATT	3
IP	33
ICMP	26
TCP	17
UDP	4
EGP	6
	144

Tabla 1: Esquema de grupos de la MIB I.

El objeto (o variable) administrado, es una característica específica de algún elemento administrado. Existen dos tipos de objetos administrados:

1. Escalares: definen una sola instancia del objeto.
2. Tabulares: definen múltiples instancias de objetos que tienen una relación entre sí y están agrupados en el MIB.

Para identificar a cada uno de los objetos administrados se creó un identificador único del objeto (OID). Este identificador se crea siguiendo el árbol jerárquico del MIB, de manera descendente. Se toma el número de cada punto intermedio, hasta llegar al objeto o instancia de objeto que se desea obtener. Puede ser escrito con números o con los nombres de cada objeto, pero es más común con números.

Como ejemplo de Identificador del Objeto (OID) podemos ver el OID que pertenece al objeto: atBcastin (3), [Figura 4.7]. Con nombres de objetos queda como sigue: *ISO.Organización-identificada.DoD.Internet.Privado.Empresa.Cisco.Variables-Temporales.Apple-talk.AtBcastin* o su equivalente con números: 1.3.6.1.4.1.9.3.3.3.

IV.5.2.1 Árbol MIB I

El árbol MIB I, [Figura 4.7] comienza en un punto indefinido, seguido de tres opciones que son: CCITT, ISO e ISO-CCITT, que representan las principales Organizaciones de Estándares. La mayor parte del “software” necesita un punto raíz (.) para localizar el objeto en el MIB, si no se incluye el punto raíz, se asume que la ruta es relativa desde (ISO), por ser la opción más usual, la cual tiene otras 4 opciones, DoD se refiere al Departamento de Defensa de Estados Unidos. Así mismo, éste tiene una opción, que es Internet, del cual se desprenden 6 opciones donde se encuentra una, llamada Privado. Dentro de ésta opción encontramos una más, Empresa, dentro de la cual están definidos los MIBs de todas las empresas que los han diseñado para sus productos. Empresas como: Cisco, 3Com, HP, Microsoft, Sun, etcétera.

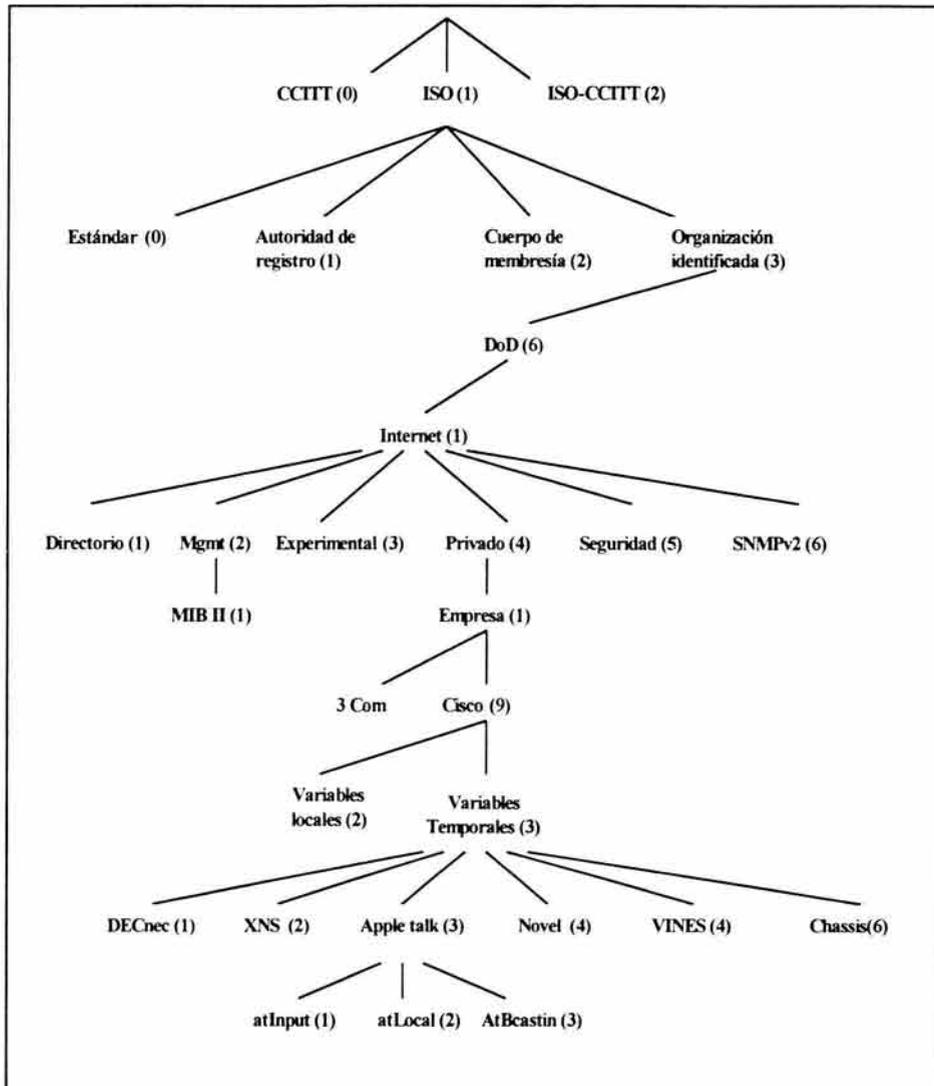


Figura 4.7 Árbol MIB I.

Otra opción importante dentro de la ramificación de Internet, es Mgmt (“Management” o Administración), dentro de la cual, está definido el MIB II.

IV.5.2.2 RFC 1156

El RFC 1156, llamado Base de Información Administrable para Redes en Internet basadas en TCP/IP, es un documento donde se define la primera versión de la Base de Información Administrable (MIB I).

Además de este documento, existen otros dos que complementan la definición de una estructura para administrar redes basadas en TCP/IP, que son: el documento que define la Estructura de Información Administrable (SMI) definido en el RFC 1155, y el documento que define al protocolo inicial de administración de redes TCP/IP (SNMP) definido en el RFC 1157.

En esta especificación del MIB se definen las variables necesarias para el monitoreo y control de varios componentes en redes. No todos los grupos de variables definidas son obligatorios para todos los componentes de redes.

No se puede definir la información que formará parte del MIB arbitrariamente. Así que, para verificar que la información es útil, se definieron una serie de criterios:

- Un objeto necesita ser esencial para identificar una falla o configuración de administración.
- Solo se permiten objetos de control que no manejen información confidencial. Debido a que el protocolo actual no es lo suficientemente seguro.
- Debe existir evidencia de que la información fue requerida por su uso actual y su utilidad.
- Se hizo el intento de limitar el número de objetos a 100, para facilitar a los proveedores definir dichos objetos dentro de su “software” y “hardware”.
- Para evitar variables redundantes, no se permitió que objetos que pueden ser derivados de otros objetos fueran incluidos.
- Fue excluida la implementación de objetos específicos.

Los Objetos dentro del MIB son definidos usando la Notación Uno de Sintaxis Abstracta (ASN.1). Cada objeto tiene un nombre (“name”), una sintaxis (“syntax”) y un código (“encode”). El nombre es un identificador del objeto, y es asignado administrativamente, el cual especifica el tipo de objeto. La sintaxis de un tipo de objeto define la estructura de datos abstractos correspondiente al tipo de dato. Y por último, el código de un tipo de objeto es simplemente el tipo de objeto representado usando la sintaxis del tipo de objeto.

IV.5.3 Concepto de MIB II

En marzo de 1991 hubo nuevas revisiones que dieron lugar a una nueva especificación de base de datos denominada MIB II. Fue a partir de ahí que diversos fabricantes se dedicaron a la obtención de MIBs particulares que permitían la compatibilidad entre plataformas de administración de entornos de red heterogéneos. (Barba, 2001).

Un proveedor también puede definir objetos para introducirlos al MIB y administrar así sus productos. MIB II define aspectos generales de productos de cualquier empresa, y está definido en el RFC 1213, (Sampieri, 2000).

IV.5.3.1 Árbol del MIB II.

La colección de objetos administrables por SNMP están definidos en el MIB. Estos objetos están agrupados en 10 categorías, las cuales corresponden a los 10 nodos definidos bajo el lenguaje ANS.1 en el árbol del MIB II, [Figura 4.8]:

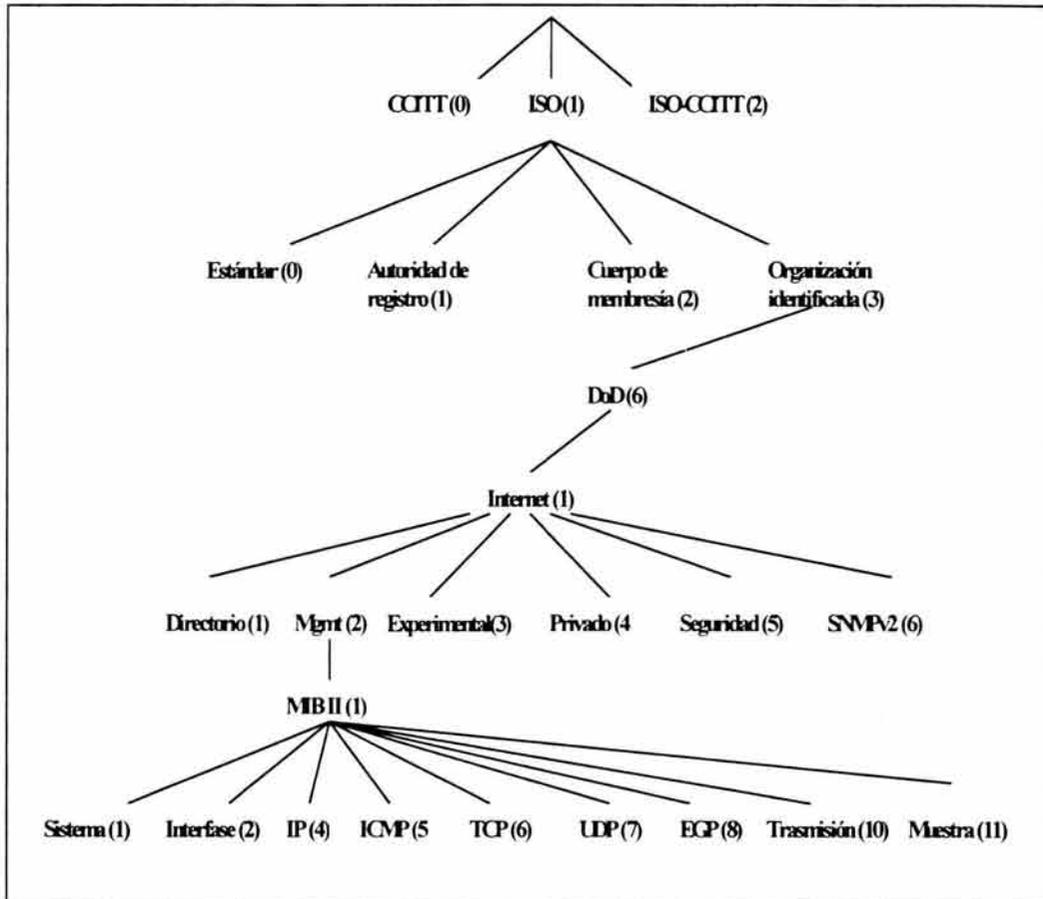


Figura 4.8 Estructura del árbol MIB II.

En la MIB II se realizaron una serie de modificaciones sobre la primera versión. También se define un nuevo grupo para cada tipo específico de interfase, así como un nuevo grupo con objetos de SNMP, (Barba, 2001).

Grupo	Número
System	7
Interfaces	23
AT	3
IP	38
ICMP	26
TCP	19
UDP	7
EGP	18
Transmission	0
SNMP	30
	171

Tabla 2: Esquema de grupos de la MIB II.

A continuación se presenta una breve descripción de los objetos definidos en el extremo inferior del árbol, donde están los objetos más comúnmente utilizados, [Tabla 2]:

- **Sistemas** (“Systems”): Incluye nombre, localización y descripción del equipo, la identidad del vendedor y el tiempo desde la última reinicialización del sistema de administración.
- **Interfases** (“Interfaces”): Una única o múltiples interfases de red y sus medidas de tráfico, local o remota.
- **ATT** (“Address Translation Table”): Contiene la dirección de la red y las equivalencias con las direcciones físicas.
- **IP** (“Internet Protocol”): Proporciona las tablas de rutas, y mantiene estadísticas sobre los datagramas IP recibidos.
- **ICMP** (“Internet Communication Management Protocol”): Cuenta el número de mensajes ICMP recibidos y los errores.
- **TCP** (“Transmission Control Protocol”): Facilita información acerca de las conexiones TCP, retransmisiones, etcétera.
- **UDP** (“User Datagram Protocol”): Cuenta el número de datagramas UDP, enviados, recibidos y entregados.
- **EGP** (“Exterior Gateway Protocol”): Recoge información sobre el número de mensajes EGP recibidos, generados, etcétera.
- **Transmisión** (“Transmisión”): Reservado para MIB específicos.
- **SNMP**: Estadísticas de tráfico SNMP.

IV.5.3.2 RFC 1213

El RFC 1213 está titulado como Base de Información Administrable para Redes basadas en TCP/IP y es comúnmente conocido como MIB II. En este RFC se describen los cambios que han surgido para cada objeto definido en el RFC 1155, así también se describen los nuevos objetos que han sido definidos.

Algunos de los cambios realizados en el MIB II son los siguientes:

- Para prevenir futuros cambios en el MIB, se ha implantado un nuevo término que puede ser usado cuando se describe un objeto: "deprecated", que significa no aprobado. De esta forma un objeto no aprobado puede mantenerse en el MIB, pero es uno de los que probablemente será removido en la siguiente versión del MIB.
- En el MIB I se mal interpretó la manera en que los datos definidos como cadenas serían desplegados al usuario. Se tenía la idea de desplegar la información como un texto convencional en el MIB. Pero como era introducido como tipo de dato "datatype", no funcionó como se esperaba.
- En cuanto a la dirección física de los equipos, permite regresar las direcciones físicas tal cual son.
- Para cada objeto del MIB I se han definidos nuevos objetos (o instancias) y se han corregido errores detectados.
- Se agregaron nuevos grupos de objetos como por ejemplo: el grupo SNMP, donde se definen los objetos que describen el funcionamiento del protocolo SNMP en cada equipo.

IV.5.4 Categorías de MIB

MIB describe los objetos, o las entradas, que deben ser incluidas en las base de datos del agente SNMP por esta razón, los agentes SNMP son referidos algunas veces como MIBs. Los objetos en un MIB deben estar definidos de la manera en que los desarrolladores del "software" de la estación conocen a disposición (los nombres de los objetos y sus valores correspondientes).

Actualmente existen tres categorías de la especificación MIB:

1. Estándar: Ésta especificación incluye un conjunto común de objetos aceptados y ratificados por el grupo de estándares Internet. El primer estándar MIB I que se dio a conocer constaba de 114 objetos, este fue mejorado posteriormente y presentado como MIB II conteniendo 172 objetos. La información que proveen estas especificaciones MIB esta dirigida a ruteadores de manejo IP.

RMON ("Remote Monitoring") MIB esta actualmente en proceso de ratificación por la comunidad Internet para que constituya un estándar MIB. RMON posee funciones diferentes a MIB II. Puede contener objetos para el monitoreo de los medios de transmisión de red, como pueden ser los relacionados con la utilización del medio, el número total de paquetes transmitidos sin errores de información variada.

RMON también puede utilizarse para realizar el monitoreo de dispositivos que no tienen un agente SNMP.

2. Experimental: Ésta categoría incluye información específica relacionada con otros aspectos de la red y de los dispositivos de manejo considerada como de gran valía y que no existe en otros estándares MIB. Una vez que la especificación experimental de MIB sea reafinada y llevada a niveles competitivos de eficiencia, será reclasificada como estándar.

3. Privado (o de empresa): Ésta se ha diseñado para uso individual de compañías que requieren coleccionar datos particulares de sus propios dispositivos de red. Permite que se definan objetos propios, que pueden ser específicos y no estar definidos en la categoría estándar.

IV.6 Plataformas de Administración de redes

La administración de redes es un servicio que emplea una variedad de herramientas, aplicaciones y dispositivos para ayudar a los administradores de la red, en la supervisión y mantenimiento de la red.

Dependiendo de las topologías y protocolos, las redes pueden ser distintas de una forma u otra y cada sistema individual es distinto en la forma en que debe administrarse. Las tareas de administración varían dependiendo, entre otras cosas, del número de usuarios a administrar, los tipos de periféricos conectados al conmutador, las conexiones de red y el nivel de seguridad necesaria.

Las plataformas de administración son el elemento más visible de la administración de una red y la clave del correcto funcionamiento de los sistemas de comunicaciones. Su ubicación física, el personal, el mantenimiento, la configuración de elementos, etcétera, son básicos para que no haya mayores problemas, (Barba, 2001).

Las plataformas de administración de redes son sistemas de “software” diseñados para realizar las actividades de administración de red, [Figura 4.9]. Las principales plataformas de administración de redes son:

- OpenView, de Hewlett-Packard.
- CiscoWorks, de Cisco.
- Sun Solstice, de Sun Microsystems.
- SistemView para AIX, de IBM.
- Tivoli Net View, de IBM.
- Spectrum, de Cabletron.

Estas plataformas proporcionan la arquitectura de “software” para las aplicaciones de administración de redes que realizan una gran variedad de tareas. No se pueden agrupar en una sola categoría. Algunas presentan un mapa de la red y comprueban el estado de todos los dispositivos de la red, lo que proporciona una función de administración de fallos.

Algunas herramientas de administración del rendimiento diseñan la utilización de los enlaces de la red y envían advertencias si se producen errores en alguna interfase de Red de Área Local. Sin embargo, otras vigilan la seguridad de la red y envían advertencias a través del correo electrónico, (Cisco, 2002).

Las plataformas de administración utilizan una integración de aplicaciones para poder adaptarse al entorno cambiante y complejo de los elementos de red que se quieran administrar. Entre las aplicaciones más usuales que se incorporan, destacan los navegadores u hojeadores de MIB (MIB "Browser") como interfases de usuario del protocolo SNMP; el "discover" que permite autodescubrir equipos y topologías de la red; la programación de sondeos de variables de la MIB; la programación de acciones ante alarmas, y finalmente, los visualizadores gráficos de variables de MIB, (Barba, 2001).

Las plataformas de administración SNMP (OpenView, CiscoWorks, Sun Solstice, Tivoli Netview y Cabletron Spectrum), proporcionan un control global de todas las subredes de una Red de Área Extensa pero la escala de tiempo en la que se lleva a cabo la monitorización debe ser necesariamente elevada. Esto se debe al esquema administrador/agente en el que se basan y en el uso del Protocolo de Datagrama de Usuario (UDP) como control de transporte.

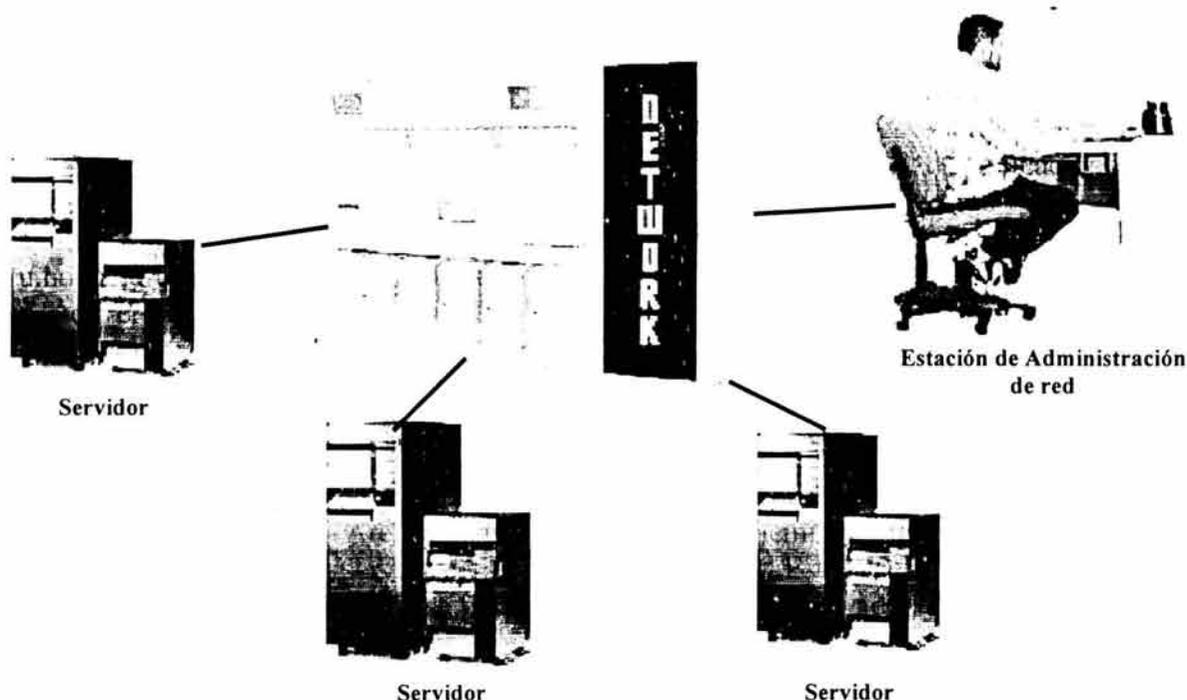


Figura 4.9 Administración de redes.

IV.6.1 OpenView, de Hewlett-Packard

OpenView, de Hp ofrece una solución de administración de red para administración local y redes multifabricantes de área extendida. Incorpora herramientas para el desarrollo de aplicaciones de administración OSI. La plataforma de administración OpenView proporciona utilerías genéricas SNMP y soporta muchas aplicaciones de HP y terceros. (Barba, 2001).

Al instalar OpenView lo primero que hace es un autodescubrimiento de la red a la cual se está conectado con tal de detectar los nodos, ruteadores, y otros dispositivos de nivel 3 del Modelo OSI con los cuales se tiene conectividad directa. Es posible añadir mas nodos aunque no estén conectados directamente a un servidor.

Con Hp OpenView se pueden realizar tareas como:

- Monitorizar y ver las propiedades de cada una de las interfases.
- Abrir Telnet, el cual es un programa que permite acceder a ordenadores distantes en Internet a los cuales se tiene acceso. Una vez que se ha accedido a un sistema distante, se pueden descargar ficheros y realizar las mismas funciones que si se estuviese directamente conectado al ordenador distante.
- Conectarse mediante el Protocolo de Transporte de Hipertexto (http), que es el conjunto de reglas utilizadas por los ordenadores para transferir ficheros hipertexto y páginas web, por Internet.
- Mostrar alarmas específicas de un nodo, etcétera.

Unas de las cualidades principales de Hp OpenView es que es capaz de monitorear cualquier equipo que responda a peticiones SNMP o incluso de forma muy limitada a equipos que respondan a peticiones ICMP, en este caso sólo se puede saber si el equipo está conectado o no (en muchos casos es más que suficiente), pero no es suficiente en determinados casos en los que se necesita una información más detallada y precisa de un equipo o nodo.

IV.6.1.1 Características HP OpenView

Utiliza una amplia variedad de protocolos, incorpora la aplicación de administración de red a nivel nodo (NNM) para redes TCP/IP.

Esta herramienta ofrece una plataforma integrada para la administración de los recursos de red, a través de impresionantes interfases gráficas. Entre otras utilidades, dispone de herramientas para localizar los nodos de la red en los que se están ejecutando agentes SNMP. Otra característica importante es la capacidad de integrar productos de otros fabricantes, como el CiscoWorks de Cisco, (Guerrero, 1997).

IV.6.2 SunNet Manager, de SUN Microsystems

Esta herramienta ofrece una plataforma integrada para la administración de los recursos de red, a través de impresionantes interfases gráficas. Entre otras utilidades, dispone de herramientas para localizar los nodos de la red en los que se están ejecutando agentes SNMP.

IV.6.2.1 Características de SunNet Manager

Los agentes que actúan con SunNet Manager son del tipo:

- Dispositivos de red tales como “routers” IP.
- Niveles de protocolo de comunicaciones e interfases tales como Internet MIB (Base de información de administración para la administración de redes sobre TCP/IP) a través de SNMP, Ethernet, FDDI y X25.
- Llamada a Procedimiento Remoto (RPC): Es una infraestructura cliente/servidor que incrementa la interoperabilidad, portabilidad y flexibilidad de una aplicación al permitir que ésta pueda distribuirse sobre diversas plataformas heterogéneas. Reduce la complejidad del desarrollo de aplicaciones que abarcan diferentes sistemas operativos y protocolos de red, al aislar al programador de los detalles de estos entornos.
- Estadísticas de recursos y sistema:
 - a) Mecanismos del sistema tales como el uso de la Unidad Central de Proceso (CPU) y canales de retención momentánea de memoria libre.
 - b) Disco y sistema de ficheros.
 - c) Aplicación, bases de datos y estadísticas de servicios de red tales como el protocolo de Sistema de Archivo de Red (NFS) que permite compartir sistemas de ficheros en una red, está diseñado para ser independiente de la máquina, el sistema operativo y el protocolo de transporte. Esto es posible porque se implementa sobre Llamada a Procedimiento Remoto (RPC).
- Otra característica importante es la capacidad de integrar productos de otros fabricantes, como el CiscoWorks de Cisco.

IV.6.3 System View para AIX, de IBM

AIX es un sistema operativo abierto de IBM basado en una versión de Unix, desarrollada y mantenida desde hace más de diez años por IBM. El origen de la plataforma de administración IBM System View es la plataforma IBM Netview/6000 que a su vez partió de una licencia de HP OpenView v.3 con algunas mejoras.

IV.6.3.1 Características de SystemView

El diseño de IBM Netview/6000 para AIX añadió una nueva componente al entorno tradicional de administración IBM, que consiste en las siguientes entidades:

- “Focal Point” (“Host” basado en Netview).
- “Entry Point” (para dispositivos con la Arquitectura de Sistemas de Redes [SNA], es el protocolo de red de IBM que permite la comunicación entre sistemas).
- “Service Point” (para dispositivos no SNA).

Esta nueva componente se denomina “Collection Point”, actúa como un sistema de administración de elementos independientes que recibe datos usando protocolos nativos aparte de SNA. Otra característica destacable de la plataforma de administración IBM System View es que no soporta el Protocolo de Información de Administración Común (CMIP).

IV.6.4 Tivoli NetView, de IBM

Tivoli Systems se fundó en 1989 y fue adquirida en 1996 por IBM, Tivoli NetView encuentra redes TCP/IP, muestra la topología de las redes, correlaciona y administra eventos y problemas de SNMP, controla el estado de la red, y recopila datos sobre el rendimiento.

IV.6.4.1 Características de Tivoli NetView

- Proporciona una solución de administración distribuida escalable.
- Recopila información útil para la administración de sistemas comerciales clave.
- Se integra con otros proveedores, como CiscoWorks.
- Mantiene el inventario de dispositivos para la administración de recursos.
- Evalúa la disponibilidad e identifica las causas de falla para la administración y el control de problemas.
- Ofrece informes sobre análisis y tendencias de redes.

Al brindar los medios para recopilar información clave de la red e identificar y solucionar problemas, Tivoli NetView permite a los administradores de red centralizar la administración de los servidores y dispositivos de “hardware” de la red.

IV.6.5 Spectrum, de Cabletron

La primera versión de Spectrum de Cabletron data de 1992, pero no fue hasta 1994 que las primeras versiones potentes de Spectrum se dieron a conocer. Los componentes que forman el núcleo de la plataforma son el módulo SpectroSERVER y los clientes SpectroGRAPH. El SpectroSERVER consta de tres componentes: La Máquina Virtual de Red (VNM), una base de datos y un administrador de dispositivos de comunicaciones. El cliente SpectroGRAPH proporciona las capacidades de la interfase gráfica de usuario.

IV.6.5.1 Características de Spectrum

- Actualmente no soporta el protocolo ICMP.
- No implementa el entorno de operación de Agente de Petición de Objeto (ORB) el cual es la parte medular de un sistema con la Arquitectura de Agente Común de Petición de Objeto (CORBA) que establece estándares para la comunicación de objetos a través de procedimientos/métodos remotos.

IV.6.6 CiscoWorks, de Cisco

CiscoWorks es una nueva familia de productos de administración para manejo de redes y dispositivos. Basado en estándares de Internet y otras tecnologías. Es un sistema de administración de redes que provee una serie de herramientas para administrar ruteadores, conmutadores de paquetes y servidores de acceso. Está basado en el Protocolo de Red de Administración Simple (SNMP) para proveer administración completa de soluciones Cisco dentro de diversas redes heterogéneas.

Permite al administrador mantener una base de datos con todas las configuraciones de los ruteadores e incluso monitorizar gráficamente los paneles traseros con todas sus conexiones.

CiscoWorks crea un mapa de la topología de la red que muestra un vista jerárquica de la red en códigos de colores, estos códigos muestran el estado en tiempo real de todos los componentes de la red, también almacena todos los errores y cambios significativos proporcionando una forma rápida para la revisión de la red.

IV.6.6.1 Características de CiscoWorks.

- Autodescubrimiento automático y mapeado de los componentes de la red.
- Permite administrar todos los componentes críticos de la red desde un sistema simple.
- Despliega una gráfica del estado de los componentes de la red en tiempo real.
- Cuenta con un sistema de alarmas.
- Proporciona estadísticas de tráfico, de la utilización del ancho de banda, y otras actividades de la red.
- El monitoreo de todos los puertos es posible bajo esta plataforma de administración.

CiscoWorks puede funcionar como una aplicación independiente de administración o se puede integrar con “software” de administración de redes como por ejemplo, OpenView, (Cisco Systems, 1999).

* * *

Entre los aspectos más importantes del presente capítulo se tiene lo siguiente: Los Centros de Operaciones de Red, son cualquier centro al que se le haya dado la tarea de administrar los aspectos operacionales de una red. El objetivo primordial del NOC es mantener en óptimas condiciones la operación de la red y de los dispositivos conectados a ella.

Un “Call Center”, es un lugar en donde se recogen las llamadas masivas con destino a una empresa o servicio y que, al mismo tiempo, sirve para realizar llamadas salientes.

Los protocolos de administración de redes fueron desarrollados para permitir a los administradores manejar los dispositivos, dar seguimiento a los eventos críticos de la red y coleccionar información relacionada con las tendencias de crecimiento de las rutas de comunicación así como del desarrollo de la red.

Un sistema de administración de red es una colección de herramientas para el monitoreo y control de redes. SNMP está orientado a monitorear y configurar el equipamiento físico de una red. También para mostrar el tráfico histórico en forma gráfica (con ayuda de las plataformas de administración) acerca de lo se ha tarifado por los equipos de la red. SNMP fue diseñado específicamente para ser un protocolo de transporte independiente. Lo que significa que las solicitudes de SNMP sobre los agentes pueden hacerse utilizando cualquier protocolo de transporte como TCP/IP o cualquier otro.

MIB I, es un conjunto de variables, llamadas objetos, almacenadas y organizadas de manera jerárquica. Los MIB son accedidos por protocolos de red como el SNMP. La administración de redes es un servicio que emplea una variedad de herramientas, aplicaciones y dispositivos para ayudar a los administradores de la red, en la supervisión y mantenimiento de la red, las plataformas de administración son el elemento más visible de la administración de una red y la clave del correcto funcionamiento de los sistemas de comunicaciones. Su ubicación física, el personal, el mantenimiento, la configuración de elementos, etcétera, son básicos para que no haya mayores problemas.

En el siguiente capítulo abordaremos la problemática existente actualmente en las redes de computadoras, haciendo un recuento de lo que se tenía en el pasado y las posibles tendencias hacia el futuro.

CAPÍTULO 5:

PROBLEMAS ACTUALES DE LAS REDES DE TELECOMUNICACIONES

V.1 Introducción

El crecimiento explosivo de redes que enlazan todo el planeta, computadoras que se comunican a velocidades de millones de bits por segundo, telefonía celular, localización global de personas, redes personales de comunicación, televisión de alta definición, redes telefónicas interconectadas con redes de televisión por cable, realidad virtual, satélites, supercarreteras de información, etcétera. Los avances científicos logrados en las telecomunicaciones han requerido muchos años de experiencia, de innovación y de expansión y se han convertido en una parte fundamental en la vida diaria. Hoy en día es imposible concebir muchas actividades humanas cotidianas sin el apoyo de las telecomunicaciones: fax, teléfono celular, televisión a colores, radiolocalización de personas, redes de computadoras, etcétera.

En los últimos años, los avances logrados en el desarrollo de computadoras de alta velocidad y bajo costo ha hecho surgir muchas posibilidades de crear nuevas y potentes aplicaciones. Con la rápida evolución y despliegue de grandes y complejos sistemas de información automatizados, ha surgido la necesidad de contar con computadoras, bases de datos y redes potentes que apoyen a las aplicaciones de los sistemas de información.

V.2 El pasado

La industria de las computadoras y las comunicaciones está sufriendo uno de los cambios más intensos y drásticos de su corta historia. En los años cuarenta, con objetivos de carácter militar, siendo de importancia secundaria el beneficio social que las comunicaciones tendrían como consecuencia; en los sesenta era muy satisfactorio poder conectar aparatos telefónicos en ambos extremos de un canal de satélite y sostener con inteligibilidad razonable una conversación telefónica; en los noventa se incorporaron los satélites a sistemas integrales de transmisión de información, con una gran variedad de medios de comunicación, tales como fibras ópticas y cables metálicos, permitiendo la satisfacción de una amplia gama de necesidades de comunicación entre las cuales están la transmisión de datos, las teleconferencias y, desde luego, las transmisiones de conversaciones habladas. Ahora se reconoce que lo que ha sido suficiente en el pasado no bastará en el futuro.

V.2.1 T1/E1 y X.25

Durante la década de los 70's y principios de los 80's, muchas personas esperaban que las redes digitales que estaban surgiendo, centradas en los sistemas T1/E1, siguieran siendo suficientes para manejar la mayor parte de aplicaciones de usuario. Después de todo, estos sistemas ofrecen tasas de transferencia de 1.5 a 2.048 millones de bits por segundo (Mbps) respectivamente, y han demostrado su capacidad para satisfacer las necesidades de casi todas las aplicaciones de usuario (que por lo regular requieren redes de comunicaciones que permiten tasas de transferencia de unos cuantos kilobits por segundo [Kbps]). No obstante, algunas personas en ese "pasado distante" se dieron cuenta de que las aplicaciones futuras iban a requerir capacidades de transmisión mucho mayores.

El creciente uso de, y experimentación con, aplicaciones que integran voz, video y gráficos reveló que las aplicaciones del futuro necesitarían redes que operan con velocidades del orden de multimegabits por segundo. Desde luego, las necesidades de comunicaciones de tales aplicaciones sobrepasarían la capacidad de las instalaciones de comunicaciones de esa época.

Durante los años sesenta y ochenta se consideró también que X.25 era una solución efectiva para transportar tráfico de datos de un usuario final, a través de una red, hasta otro usuario final, y X.25 ha dado muy buen servicio a la industria durante dos décadas. Sin embargo, la tecnología X.25 se diseñó para las Redes de Área Extensa (WAN) de baja capacidad, no para aplicaciones de alta velocidad; por ejemplo, tasas de Megabits de las Redes de Área Local (LAN), (Black, 1999).

V.2.2 Interconexión de Redes de Área Local

Muchas aplicaciones de usuario que se crearon a principios de la década de 1980 comenzaron a operar en Redes de Área Local de alta capacidad, y la revolución en la industria de las computadoras personales (PC) dio origen a una amplia variedad de nuevas aplicaciones que funcionaban bien con la tecnología LAN, la cual se expandió rápidamente. Al tiempo que estas LAN se interconectaban para compartir recursos e intercambiar datos, las compañías telefónicas estaban mejorando su tecnología de área extensa instalando fibras ópticas en sus líneas troncales. La idea era mejorar la calidad y rapidez de sus redes para facilitar la tarea de interconectar las LAN y, desde luego, tratar de que los usuarios siguieran utilizando sus servicios. Las compañías telefónicas instalaron también equipos más rápidos y suministraron servicios de 45 Mbps (en Norteamérica) y 140 Mbps (en Europa) a los usuarios.

Desafortunadamente, parte de las labores de interconexión de LAN y casi todo el desarrollo de los equipos de alta velocidad se efectuaron sin pensar en la necesidad de usar protocolos estandarizados entre el "hardware" y "software" de los diferentes fabricantes. La consecuencia fue que muchos sistemas que se venden actualmente no pueden comunicarse fácilmente entre sí, aunque proporcionen servicios similares. El resultado es un entorno excesivamente complejo y costoso que implica extensas y tardadas operaciones de conversión para lograr que los sistemas heterogéneos se comuniquen entre sí.

Aunque el problema de compatibilidad de los sistemas siguió prevaleciendo, el usuario final no resultaba afectado directamente y los servicios de 45 Mbps y 140 Mbps proporcionaban suficiente ancho de banda para casi todas las empresas grandes. Sin embargo, para las empresas más pequeñas tales servicios eran demasiado costosos. Arrendar un circuito de alta velocidad para conectar dos computadoras a un costo de varios miles de dólares por mes simplemente rebasaba el presupuesto de un gran número de usuarios potenciales de redes. Para un número creciente de usuarios y proveedores de telecomunicaciones, los sistemas instalados en los años ochenta parecían ya suficientes para satisfacer las necesidades de las aplicaciones tanto de los usuarios como de los fabricantes. Por ello, a mediados de la década de 1980 se iniciaron esfuerzos por atender las necesidades de aplicaciones futuras.

V.3 Características fundamentales de las redes tradicionales

Dos características fundamentales de las redes tradicionales, son las siguientes:

1. Medio físico compartido (“shared media”).
2. Ancho de banda compartido (“shared bandwidth”).

V.3.1 Medio físico compartido

Por el medio de transmisión circula todo el tráfico de la red, y no sólo el que va destinado a la estación que está conectada a él. Todas las estaciones reciben todo el tráfico de la red, con los potenciales problemas de seguridad y confidencialidad de los datos que ello representa.

Compartir el medio de transmisión significaba en las primeras implementaciones de Ethernet, tanto 10Base5 como 10Base2, compartir los problemas, ya que cualquier incidente ocurrido al cable implicaba la caída de toda la red.

En Token Ring, así como Ethernet 10BaseT, el empleo de concentradores, si bien no elimina la caída de la red en determinadas situaciones, pero simplifica la determinación del problema, al igual que su reparación ya que, normalmente, el concentrador facilita la información sobre el nodo o la sección de cable causante del fallo, y con su desconexión se soluciona el problema. Desaparece la necesidad de tener que correr físicamente todo el cable para la localización del error.

V.3.2 Ancho de banda compartido

Indica que el ancho de banda disponible se reparte entre todas las estaciones conectadas a la red. En las redes con ancho de banda compartido todas las estaciones reciben las transmisiones de cualquier otra estación. El modo de operación empleado es “half duplex”, es decir, en un momento dado, sólo puede haber una única estación transmitiendo datos.

Todos los nodos de la red tienen que competir entre ellos para poder acceder al medio y, por lo tanto, poder transmitir. Ello da como resultado el empleo de diferentes métodos de acceso, para resolver esta característica de las redes de ancho de banda compartido se utilizan los denominados protocolos MAC, que proporcionan un mecanismo de arbitraje para acceder a la red.

Cuanto mayor es el número de nodos conectados la red, menor es el ancho de banda disponible para cada nodo [Figura 5.1], pudiendo llegar a saturarse la red con un número no demasiado elevado de nodos.

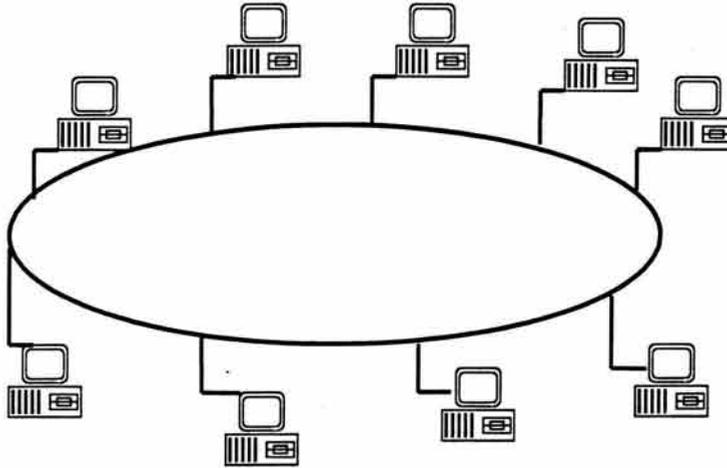


Figura 5.1 Red Colapsada trabajando al máximo de su capacidad de tráfico.

El método tradicional para solucionar problemas básicos de ancho de banda ha consistido fundamentalmente en la segmentación de la red mediante el uso de puentes (“bridges”). Una red colapsada soportando el 100% de su capacidad de tráfico, se puede descomponer en varios segmentos de forma que la carga de cada uno de ellos sea menor, [Figura 5.2].

Para llevar a cabo esta segmentación es conveniente realizar un estudio detallado de la distribución de tráfico de la red que nos proporcione información para agrupar los nodos en diferentes segmentos de la forma más adecuada a la distribución obtenida. Una segmentación arbitraria sin ningún tipo de estudio puede aportar más inconvenientes que ventajas, (Caballero, 1998).

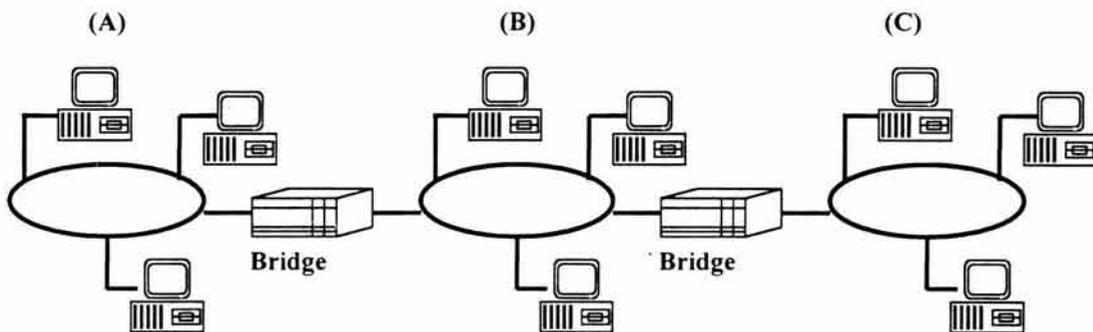


Figura 5.2 La red una vez segmentada soportando un tráfico menor.

V.4 El futuro se ha convertido en el presente

En unos cuantos años, las aplicaciones futuras se han convertido en las aplicaciones actuales. La industria de las comunicaciones se está desplazando hacia las potentes redes de Gigabits que soportan cualquier tipo de aplicaciones. Es más, por primera vez en la historia de la industria de las computadoras y las comunicaciones, la administración de redes de todo el mundo está adoptando un conjunto de estándares a nivel mundial para usarlos en redes multimedia de alta capacidad. Esta tendencia mejorará los servicios que recibe el usuario final y redundará en importantes aumentos en la productividad y una reducción en el costo de los negocios, (Black, 1999).

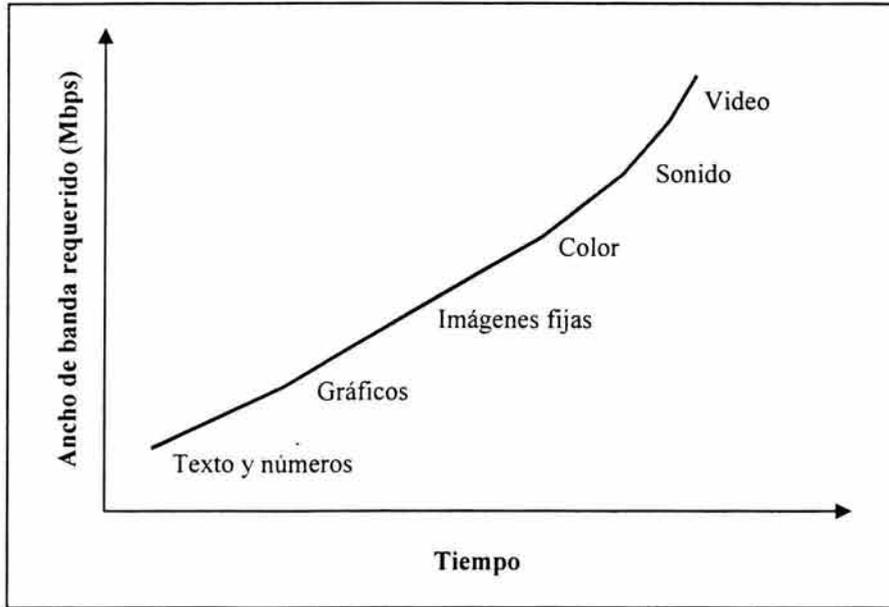
V.4.1 La necesidad de mayor capacidad para comunicarse

En los inicios de la computación, un enlace de red o de comunicaciones que operaba a velocidades del orden de 300 a 600 bits por segundo se consideraba adecuado para manejar casi todas las aplicaciones de usuario. Se puede considerar la industria hace unos años: un canal de 9.6 Kbps con módems conectados se consideraba una tecnología de alta velocidad un tanto esotérica. Para la mayoría de los usuarios, el canal de 9.6 Kbps era sin duda una función de apoyo de comunicaciones de “alta capacidad” para una computadora personal o estación de trabajo.

Las cosas en la industria cambian con gran rapidez, hoy en día, una velocidad de 9.6 Kbps es insuficiente para muchas aplicaciones. Por ejemplo un lector podría conectarse a una red y recuperar un mapa meteorológico. A una velocidad de transferencia de 9.6 Kbps, se requerirían unos 40 segundos para llenar la pantalla con un mapa en blanco y negro de baja calidad. Es preciso esperar varios minutos para que se transmita en su totalidad un mapa a color de alta definición. Este retardo podría ser aceptable para algunos usuarios y algunas aplicaciones, pero evidentemente no es una forma muy productiva de trabajar.

La recuperación y exhibición de un mapa meteorológico en realidad no requiere demasiado ancho de banda. La necesidad de contar con más capacidad, más allá de esta sencilla transmisión de imágenes en blanco y negro, está creciendo a medida que se crean más y más aplicaciones que manejan imágenes a color, voz y video, se está volviendo indispensable una infraestructura de comunicaciones de Multimegabits.

En la [Figura 5.3] se muestran las necesidades acumuladas de ancho de banda para estas nuevas aplicaciones. En la década de 1980 la mayor parte de las aplicaciones manejaba texto y números casi no se necesitaban redes de alta capacidad para apoyar las transmisiones de este tráfico entre las aplicaciones de usuario. En unos cuantos años han surgido aplicaciones que manejan gráficos de mapa de bits, color, sonido e incluso video. Las necesidades acumuladas de ancho de banda para que una de estas aplicaciones envíe y reciba este tipo de imágenes a otra aplicación similar se están acercando al nivel de Multimegabits.



Nota: El aumento en las capacidades con el tiempo crea un aumento acumulado en el ancho de banda.

Figura 5.3 Creciente necesidad de mayor capacidad.

Las técnicas de compresión son limitadas en cuanto a su capacidad para reducir el número de bits que representan una imagen. Por más efectivas que sean las técnicas de compresión, no se puede seguir dependiendo de ellas para disfrazar lo limitado de la capacidad del canal de comunicaciones. La fibra óptica ofrece el ancho de banda que se necesita.

V.4.2 Lo que las aplicaciones van a necesitar

Un estudio realizado por el Centro de Investigación Xerox Palo Alto (PARC) muestra que una amplia gama de aplicaciones necesita una gran capacidad de comunicación (ancho de banda grande).

En la tabla 1, se listan varios tipos de aplicaciones que requieren un ancho de banda grande. En general, se trata de aplicaciones de transmisión de video o imágenes fijas de alta calidad a todo color.

Hasta hace poco, parecía poco probable encontrar soluciones de red económicas para apoyar estos tipos de aplicaciones, pero se han logrado avances importantes en la técnicas de compresión que permiten a algunas tecnologías actuales manejar ese tipo de aplicaciones.

Descripción del medio	Intervalo de velocidades sin compresión (Mbps)	Intervalo de velocidades con compresión (Mbps)
Video NTSC [▼] con calidad de difusión	120	3-6
Video NTSC con calidad de estudio	216	10-30
Video de alta definición con calidad de difusión	1500	20-30
Visualización de imágenes con pleno movimiento a 60 cps, 1000*1000 pixeles	1500-2500	50-200
Imágenes fijas binarias monocromáticas [▲] , 600*600 puntos/pulgada, 135 pp/min	120	5-50
Imágenes fijas a todo color [♦] 400*400 pixeles/pulgada, 60 pp/min	500	45

Tabla 1: Necesidades de diversas aplicaciones (transmisión de imágenes) y ancho de banda requerido, (Black, 1999).

La tabla 1, también muestra las necesidades de los diversos tipos de aplicaciones para tráfico tanto comprimido como sin compresión. La Tecnología de Televisión de Alta Definición (HDTV) requiere 1500 Mbps para tráfico no comprimido e incluso 20-30 Mbps. Resulta interesante que la imágenes fijas tienen necesidades de ancho de banda muy grande en comparación con las imágenes en movimiento.

La razón es que la exhibición de las imágenes fijas requiere muy alta definición, más alta que la de las imágenes en movimiento, porque el ojo humano tiende a “estudiar” la imagen con más detenimiento, que en el caso de una imagen en movimiento. Además, las impresoras de muy alta velocidad actuales imprimen a tal ritmo (cerca de dos páginas por segundo) que tienen una tasa de cuadros apenas unas 15 veces más lenta que la de video NTSC.

En síntesis el estudio de PARC indica que para que video de alta calidad pueda residir en la estación de trabajo de un usuario, la industria va a necesitar un enlace de por lo menos 100 Mbps en dicha estación. Si bien podría parecer que la televisión y las imágenes a color representan el límite de lo que se va a exigir a las redes de Gigabits, están apareciendo varias otras aplicaciones que requieren esta capacidad; las conferencias multimedia son una de ellas.

▼ National Television Standards Committee

▲ Derivado de caracteres del Sistema de Copiadora Electrónica Xerox Docutech

♦ Estimaciones según los autores de las características de copiadoras a color distribuidas de alto desempeño hipotéticas

Las teleconferencias pueden ahorrar a una empresa una cantidad considerable de dinero en gastos de viaje, alojamiento y tiempo perdido, y algunos han reducido drásticamente sus presupuestos en esta área. Sin embargo, cada conferencia multimedia de alta calidad debe operar en el nivel de Megabits y las conferencias individuales entre dos personas requieren la misma cantidad de ancho de banda.

Otra aplicación que requiere gran ancho de banda que está surgiendo apenas, es un concepto llamado realidad virtual. Si bien las implementaciones iniciales de la realidad virtual han sido un tanto frívolas, la tecnología tiene un potencial tremendo. Exploradores, geólogos, auscultadores médicos y demás pueden utilizar sistemas de visualización para facilitar su trabajo y actividades. Es evidente que los sistemas de realidad virtual operarán en el nivel de Megabits.

Más allá de las necesidades brutas de ancho de banda de estas aplicaciones, también se está haciendo obvio que algunas aplicaciones requieren más control sobre diversas operaciones que hasta ahora se han relegado al control del administrador de red. Por ejemplo, algunos usuarios necesitan saber cuánto retardo de la red habrá entre dos aplicaciones en comunicación.

Igualmente importante para algunas aplicaciones es la capacidad para controlar la pérdida de tráfico, así como la recuperación después de una falla. Incluso el control de los tiempos de preparación de red/usuario está adquiriendo importancia para ciertas aplicaciones, lo mismo que la capacidad para predecir el tiempo de preparación en relación con la cantidad de tráfico y de retardo.

V.5 Limitaciones de las actuales LAN

A pesar del notable avance de las actuales tecnologías LAN, el ancho de banda (por grande que sea) siempre tiene que ser compartido entre todas las estaciones. En el mejor de los casos, el ancho de banda asignado para cada estación es el resultado de la velocidad de la LAN dividido por el número de estaciones. Pero ésta no es la única limitación de las LAN segmentadas:

- Se considera que se está llegando al límite de las LAN con tecnología de bus compartido como las Token Ring y Ethernet, no pudiendo soportar un crecimiento indefinido de sus estaciones.
- Los ruteadores que conmutan y filtran mensajes entre las LAN están basados en una tecnología de conmutación de paquetes poco escalable en velocidad y número de puertos.
- El aumento progresivo de la potencia de las estaciones de trabajo, velocidades de bus de memoria, capacidad de los servidores, etcétera, las convierten en máquinas capaces de manipular información por encima de 100 Mbps.
- Las nuevas aplicaciones multimedia necesitan anchos de banda elevados y requieren calidades de servicio específicas.

Por estos motivos, la tendencia actual es hacia las LAN conmutadas que proporcionan de forma nativa soportes multimedia, alta escalabilidad y unos anchos de banda que van desde 10 Mbps a 1 Gbps sobre diferentes tipos de cableado.

V.5.1 Interconectividad de Redes de Área Local

Una de las fuerzas impulsoras de varias de las tecnologías de comunicaciones que están surgiendo es la necesidad que tienen muchas empresas de conectar dos o más redes LAN entre sí a través de las WAN. Desde luego, al administrador de redes le gustaría disfrutar de interconectividad “sin costuras” entre dichas redes.

Esta necesidad se está volviendo ubicua dentro de la industria de las computadoras y las comunicaciones. La necesidad de interconectividad de las LAN es el resultado del rápido crecimiento del número de Redes de Área Local instaladas y el número de computadoras personales (y otros dispositivos) conectadas a esas LAN. La base instalada de LAN en el mundo sigue creciendo, lo mismo que las conexión de computadoras personales y estaciones de trabajo a estas LAN.

V.6 Nuevas implementaciones de Redes de Área Local

La creciente potencia de las computadoras nos sigue permitiendo crear aplicaciones cada vez más potentes y productivas. Pero si queremos que dichas aplicaciones se comuniquen de forma efectiva entre sí, es indispensable que las redes intermedias cuenten con la capacidad necesaria para apoyar las interacciones sin que se noten “las costuras”, (Black, 1999).

V.6.1 LAN conmutadas

Las redes locales de medio físico compartido deben implementar un mecanismo que arbitre el acceso al medio y, consiguientemente, la capacidad de transmisión queda dividida. Estos sistemas cuentan con un inconveniente añadido de que todas las tramas pasan por todas las estaciones lo que significa no pocos inconvenientes respecto a la confidencialidad.

Si se quieren evitar estos problemas y a la vez aumentar la capacidad agregada de toda la red, se pueden utilizar conmutadores (“switches”) que proporcionen anchos de banda dedicados a cada una de las estaciones conectadas.

V.6.2 Metas de las nuevas tecnologías de comunicaciones

Las tecnologías emergentes de comunicaciones apoyan redes integradas de alta capacidad que involucran computadoras de distintos fabricantes y paquetes de “software” que operan con diferentes proveedores de servicios de comunicaciones. Hoy en día, muchos paquetes de comunicaciones varían dependiendo del proveedor de la red en la que operan. Un objetivo clave de las nuevas tecnologías es crear un conjunto de procedimientos y normas que se apliquen igualmente en todas las redes de todos los proveedores.

Desde luego, la creación de redes integradas empleando interfases y protocolos comunes, aunque sin duda resultará benéfica, no es la única meta de estas nuevas tecnologías.

Otro objetivo importante es ofrecer más capacidad de rendimiento (en bits por segundo) para aplicaciones de usuario y realizar las operaciones de red con mayor rapidez a favor de las aplicaciones.

Esto implica que las tecnologías emergentes se han diseñado para ofrecer alto rendimiento, con velocidades de transmisión muy altas y con retardos muy bajos. Otra meta importante es apoyar cualquier tipo de aplicación, como voz, video, música, facsímil y telemetría. Un término apropiado para este servicio es redes multiaplicación, aunque casi todo el mundo usa el término de redes multimedia. La implementación económica de las redes multimedia está resultando ser uno de los mayores retos que enfrenta la industria.

Desde el punto de vista del proveedor de redes, otro objetivo importante de las tecnologías de comunicación que están surgiendo (al menos de algunas de ellas) es proporcionar más y mejores herramientas de administración de redes.

A primera vista, este factor tal vez no signifique mucho para un usuario final, pero dichas herramientas permiten al proveedor de redes monitorear minuciosamente los recursos de red y ofrecer un servicio robusto y relativamente libre de errores a las aplicaciones de usuario.

En contraste con los sistemas basados en T1/E1, que tienen funciones de administración de redes muy limitadas, las nuevas tecnologías de comunicaciones utilizan cerca del 5% del ancho de banda de la red para la administración. Puesto que los canales de comunicaciones son de fibras ópticas, se cuenta con suficiente ancho de banda par apoyar esta importante operación.

Por último, otra de las principales metas de varias de las tecnologías de comunicación emergentes es el suministro de interconexiones “sin costuras” entre el “hardware/software” de las redes y entre redes mismas.

Se usa el término “sin costuras” para denotar que un usuario final (o incluso un administrador de red) no es consiente de que el tráfico de usuarios se transporta por equipos de diferentes fabricantes y por diferentes redes.

Las redes pueden ser locales o remotas, e incluir equipo y “software” de un solo fabricante o de muchos. No obstante, las operaciones son transparentes para el usuarios (e, idealmente, para un administrador de red).

V.7 Interconexión de redes LAN Y WAN

Uno de los problemas que han recibido considerable atención en los últimos años es la necesidad de interconectar Redes de Área Local y de Área Extensa. Hasta hace poco, había sido relativamente fácil definir las WAN y las LAN y señalar sus diferencias. Esto ya no es tan fácil, porque los términos: área extensa y área local no tienen los significados que alguna vez tuvieron. Podría ser útil comparar y contrastar estos dos tipos de redes, [Tabla 2]:

Redes de Área Extensa (WAN):

- Computadoras con múltiples usuarios conectados entre sí.
- Las máquinas están dispersas en una región geográfica “extensa”.
- Los canales de comunicación entre las máquinas generalmente pertenece a un tercero (por ejemplo, la compañía telefónica, una red pública de datos, una portadora de satélite).
- Los canales tienen una capacidad relativamente baja (midiendo el rendimiento en Kilobits por segundo [Kbps]).
- Los canales son relativamente propensos a errores (por ejemplo, una tasa de errores de 1 en cada 100,000 bits transmitidos).

Redes de Área Local (LAN):

- Computadoras con múltiples usuarios conectados entre sí.
- Las máquinas están dispersas en una región geográfica “pequeña”.
- Los canales de comunicación entre las máquinas suelen ser propiedad privada.
- Los canales tienen una capacidad relativamente alta (midiendo el rendimiento en Megabits por segundo [Mbps]).
- Los canales son relativamente libres de errores (por ejemplo, una tasa de errores de 1 en cada 10^9 bits transmitidos).

Tabla 2: Comparación y contraste de las LAN y WAN, (Black, 1999).

Por ejemplo, una LAN en la década de los 80's generalmente estaba limitada a un edificio o un campus universitario, donde los componentes no estaban a más de unos cuantos cientos de metros unos de otros. Hoy en día las LAN pueden abarcar muchas decenas de kilómetros. No obstante, ciertas características son exclusivas de cada una de estas redes. El proveedor de una WAN generalmente es una compañía independiente. Por ejemplo, muchas WAN se denominan redes públicas porque la compañía telefónica o una Red Pública de Datos (PDN) es propietario y administrador de los recursos, y renta estos servicios a los usuarios.

En contraste, una LAN generalmente es de propiedad privada. Una empresa compra y administra los cables y componentes. Las LAN y WAN también pueden contrastarse por su capacidad en (bits por segundo): la mayor parte de las WAN generalmente operan en el nivel de Kbps, mientras que las LAN operan en el nivel de Mbps. Otra característica importante que distingue estas redes es la tasa de errores. Las WAN suelen ser más propensas a errores que las LAN a causa de la mayor amplitud geográfica y relativa hostilidad del terreno (fenómenos meteorológicos, etcétera) sobre el que deben tenderse los medios. En contraste, las LAN operan en un ambiente relativamente benigno, porque los componentes de comunicación de datos se alojan en edificios en los que intervalos de humedad, temperatura y electricidad están controlados.

V.7.1 Costos de conectar LAN dispersas

En los últimos años, las LAN y WAN se han interconectado con puentes, ruteadores, puertas de enlace (“gateways”) y redes de conmutación de paquetes. Estas unidades de interconexión de redes se conectan a las LAN y WAN a través de canales de comunicación dedicados (líneas arrendadas). Como práctica general, las líneas arrendadas se tienden de extremo a extremo entre los equipos que están en las instalaciones de los clientes (CPE). El usuario recibe una línea arrendada dedicada y dispone de toda la capacidad de transmisión las 24 horas del día (con algunas excepciones). Por tanto, el usuario paga por el circuito sea cual sea su utilización. Además, si se necesita una conexión a otro lugar más (a otra ciudad del país), se deberá rentar otra línea arrendada a las portadoras comunes, también bajo un régimen continuo de extremo a extremo.

El empleo de estas líneas para conectar unidades de interconexión de redes, así como Redes de Área Local y de Área Extensa, es un proceso muy costoso. Por añadidura, surgen problemas de confiabilidad porque las líneas arrendadas individuales de punto a punto no tienen capacidad de respaldo. Además, el procesamiento tan exhaustivo del tráfico (ediciones, verificaciones de errores) han creado retardos inaceptables para ciertas aplicaciones. Una mejor estrategia es crear una red portadora LAN/WAN que proporcione tecnologías de conmutación eficientes para fines de respaldo y también para circuitos de alta capacidad: una red que permita a los usuarios compartir las costosas líneas arrendadas. Este concepto se denomina Red Privada Virtual (VPN).

V.7.2 La Red Privada Virtual (VPN)

La VPN se llama así porque un usuario individual comparte canales de comunicación con otros usuarios. Se colocan conmutadores en estos canales para que un usuario final pueda tener acceso a múltiples sitios terminales. Idealmente, los usuarios no se dan cuenta de que están compartiendo una red con otros, de ahí el término red privada virtual: el usuario cree que tiene una red privada, aunque no es así.

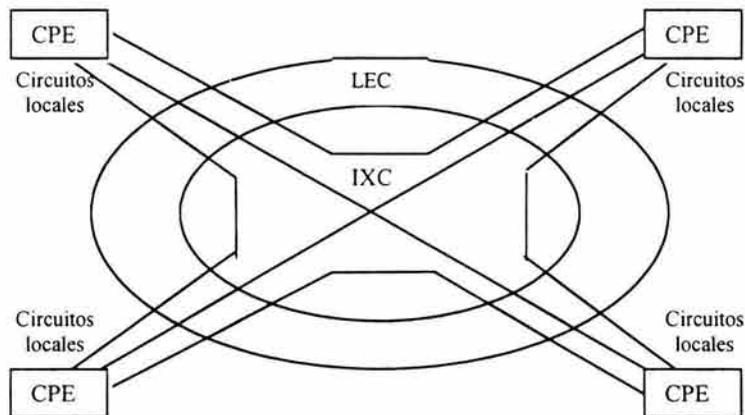


Figura 5.4 Líneas arrendadas (4 nodos).

En la figura anterior, [Figura 5.4] cuatro sitios cliente están conectados al equipo de las instalaciones del cliente (CPE, que suele ser un ruteador o algún otro tipo de unidad de interconexión de redes) a través de circuitos locales con portadoras de intercambio (IXC). Las portadoras de intercambio local (LEC) terminan sus circuitos locales en el CPE y la IXC. En este ejemplo, una red de líneas arrendadas totalmente interconectada requiere seis líneas arrendadas IXC, doce líneas dedicadas a la IXC (circuitos locales) y doce puertos de ruteador (tres en cada ruteador).

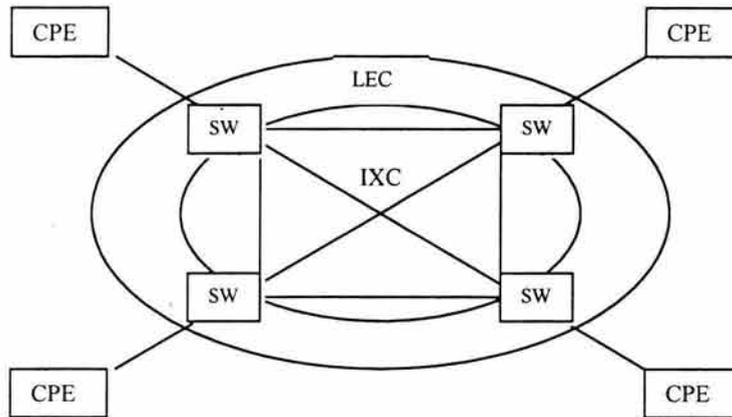


Figura 5.5 VPN (4 nodos).

En contraste, si se utiliza una VPN, el CPE sólo requiere un circuito local dedicado al conmutador de VPN (sw, "switch"). A partir de ahí, el proveedor de la VPN crea una red totalmente interconectada. Aunque no siempre es así; el proveedor de la red determina qué construcción tiene la columna vertebral ("backbone") de la red.

Este enfoque permite encaminar el tráfico a diferentes puntos extremos y no obliga a los dispositivos de usuario final a ocupar permanentemente líneas arrendadas privadas. En la [Figura 5.5] se puede ver que la VPN requiere de seis líneas IXC pero sólo cuatro puertos de ruteador y sólo cuatro circuitos locales dedicados.

VPN es un término relativamente nuevo en la industria de las computadoras y las comunicaciones, pero describe un concepto ya viejo. Las ideas en que se basa la VPN nada tienen de nuevo. Las redes públicas X.25 han ofrecido servicios VPN desde hace años y los servicios T1 conmutados también ofrecen funciones tipo VPN. Sin embargo, varias tecnologías emergentes ofrecen VPN más potentes que las tecnologías viejas.

V.8 Soluciones propuestas

Se han propuesto varias soluciones, algunas de ellas basadas en redes privadas virtuales, para aliviar y/o resolver los problemas en las redes actuales. Algunas de ellas se complementan entre sí, mientras que otras compiten. La siguiente tabla resume los tipos de tecnologías emergentes de comunicación:

- **Retransmisión de Tramas (Frame Relay).**

Un rápido servicio de retransmisión, con soporte mínimo de red que ofrece ancho de banda sobre pedido.

- **Fast Ethernet y Ethernet Conmutada.**

Variación de alta velocidad de Ethernet que utiliza conmutadores de punto a punto, así como medios y esquemas de codificación basados en FDDI.

- **Cola Distribuida en Doble Bus (DQDB).**

Tecnología rápida para apoyar aplicaciones multimedia en Redes de Área Metropolitana (MAN).

- **Servicio de Conmutación de Datos Multimegabits (SMDS).**

Sistema de transporte público de alta velocidad basado en tecnología DQDB.

- **Modo de Transferencia Asíncrono (ATM).**

Circuito virtual de alta velocidad con tecnología de retransmisión de celdas.

- **Red Óptica Síncrona (SONET) o Jerarquía Digital Síncrona (SDH).**

Sistema de portadora síncrona de alta velocidad basada en el uso de tecnología de fibras ópticas y una jerarquía de multiplexación digital definida.

- **Sistemas inalámbricos (y móviles).**

Amplia formación de sistemas inalámbricos diseñados para manejar principalmente voz y datos de baja velocidad, aunque están apareciendo sistemas que apoyan las aplicaciones multimedia.

- **Banda ancha residencial.**

Diversas opciones de técnicas de codificación y cableado que llevan canales de más alta capacidad a los hogares.

- **Señalización de banda ancha.**

Tecnología de señalización de segunda generación (basada en RDSI y SS7) que se usa para establecer y eliminar circuitos virtuales.

- **Red inteligente (IN).**

Extensión de las redes y bases de datos SS7 actuales para proporcionar al usuario funciones rápidas, avanzadas y personalizadas.

Tabla 3: Tipos de tecnologías emergentes de comunicación (Black, 1999).

La tecnología de retransmisión de tramas (“Frame Relay”) propone resolver el problema del cuello de botella de las WAN ofreciendo un “servicio de paquetes rápido” (en realidad un servicio de tramas rápido). La estrategia es proporcionar apoyo de red mínimo dependiendo del usuario para la recuperación en caso de haber problemas. Además, la retransmisión de tramas ofrece servicios de ancho de banda por demanda. Actualmente, la retransmisión de tramas está dirigido a las aplicaciones de datos, pero ya se ha utilizado en algunas aplicaciones de voz.

Los términos Ethernet rápida o Fast Ethernet y Ethernet conmutada (“Switched Ethernet”) a menudo se utilizan de manera indistinta. Juntos, estos términos describen una tecnología de LAN diseñada para apoyar individualmente estaciones de trabajo de usuario cuyos requisitos de capacidad varían entre 10 Mbps y 100 Mbps, en contraste con el esquema de compartir estos anchos de banda con múltiples estaciones de trabajo.

DQDB es un estándar del IEEE (IEEE 802.6) que ofrece un protocolo de Cola Distribuida en Doble Bus muy rápido que apoya redes integradas para aplicaciones multimedia. Se ha dado este nombre al estándar porque se diseñó para interconectar Redes de Área Local dentro de una de Área Metropolitana.

El Servicio de Conmutación de Datos Multimegabits (SMDS), se basa en la tecnología DQDB y proporciona un sistema de transporte público de alta velocidad. Las compañías telefónicas de Estados Unidos y varios proveedores de portadoras públicas europeas están ofreciendo SMDS como un servicio para aplicaciones de datos de alta velocidad que requieren ráfagas de transmisión con alto ancho de banda para aplicaciones como transferencia de archivos, Diseño Asistido por Computadora/Fabricación Asistida por Computadora (CAD/CAM) y transmisión de imágenes.

La Red Óptica Síncrona (SONET), Jerarquía Digital Síncrona (SDH) son un sistema de portadora de alta velocidad (en términos telefónicos, un sistema de transporte) basado en temporización síncrona, en el cual los dispositivos de red se sincronizan con uno o más relojes maestros. Este sistema utiliza tecnología de fibras ópticas y está diseñado para apoyar sistemas de portadora actuales como T1, T3, E1, E3 y también tráfico de Redes de Área Local y de Retransmisión de Tramas y celdas. Se creó pensando en que tarde o temprano sustituirá los sistemas de portadora T1/T3 y E1/E3.

Las tecnologías inalámbrica y móvil son sistemas que suministran recursos de comunicación utilizando ondas de radio de alta frecuencia. En la actualidad, estas tecnologías representan una mejora de la infraestructura de comunicaciones existente, como los circuitos locales y los servicios telefónicos locales. Obviamente, estas tecnologías ofrecen un mecanismo muy flexible para manejar usuarios móviles, y se están convirtiendo en competidores fuertes de otras tecnologías.

El término banda residencial se acuñó para describir una amplia variedad de tecnologías que llevan más ancho de banda al circuito del suscriptor local (al hogar) para apoyar aplicaciones como video por demanda, transferencia de archivos grandes y navegación interactiva en Internet.

La señalización de banda ancha es una tecnología utilizada por una red para establecer los recursos (conexiones) que apoyan las necesidades del usuario final. Las diversas organizaciones de normas y grupos comerciales definen de manera distinta el término “banda ancha”.

La Red Inteligente (IN) es una extensión y una evolución de la arquitectura SS7 diseñada para proporcionar un conjunto estandarizado de protocolos (que operan encima de SS7) para ayudar al suministro rápido de servicios (por ejemplo, funciones de llamada) al usuario, (Black, 1999).

El Modo de Transferencia Asíncrono (ATM) forma parte de la solución RDSI-BA. Se trata de una tecnología de retransmisión de celdas que incluye servicios de multiplexación y conmutación de alta velocidad para aplicaciones de voz, datos y video.

Después de un análisis, se puede comprobar que no es sino el resultado de la evolución de algunas tecnologías precedentes y la mejora de las infraestructuras básicas de comunicaciones.

Tecnologías Precedentes: ATM es la conjunción de dos tecnologías de Multiplexación por División de Tiempo (TDM) implementadas con éxito en las Redes de Área Extensa (WAN) durante los últimos años.

La tecnología ATM puede verse como la conjunción tecnológica de las redes de conmutación de circuitos y las de conmutación de paquetes [Figura 5.6], heredando las características más deseables de cada una de ellas.

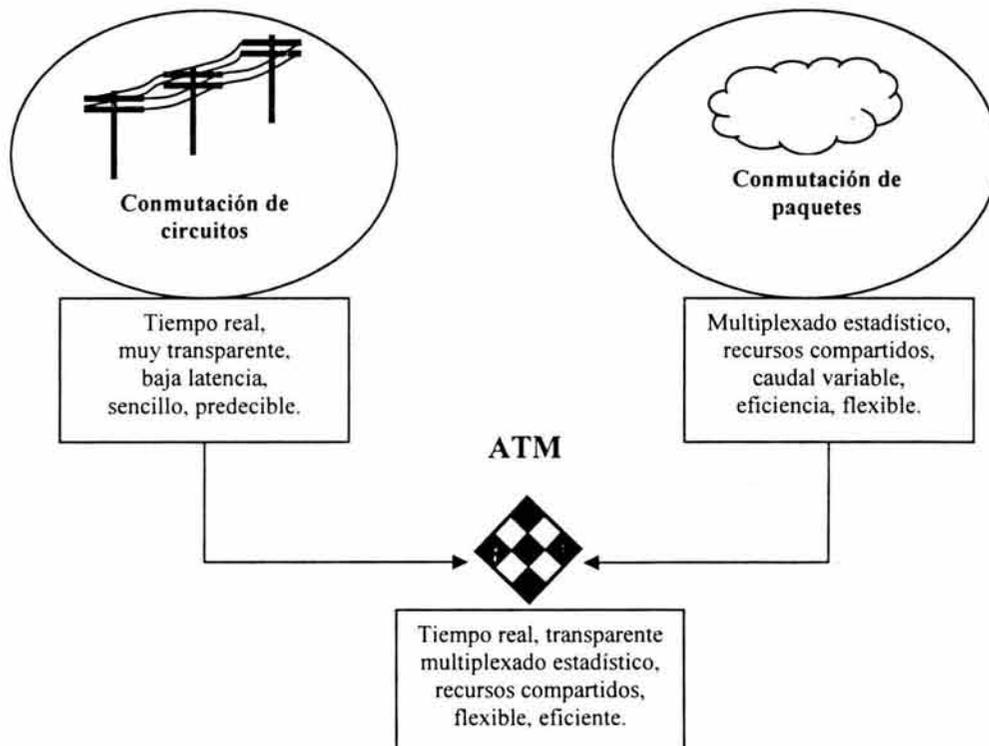
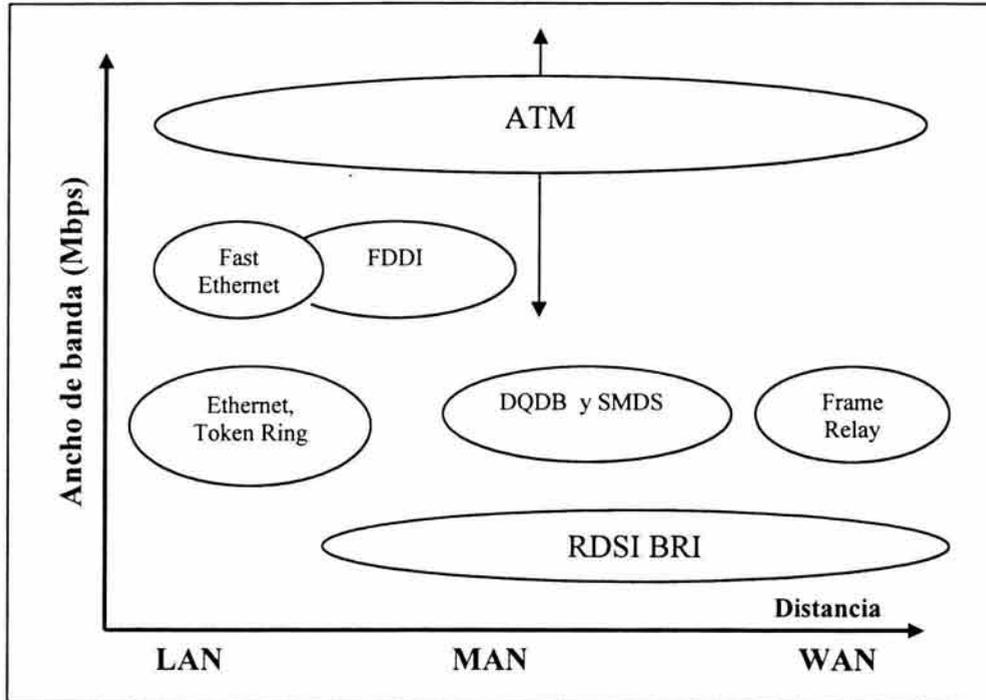


Figura 5.6 Conjunción tecnológica de ATM.

V.8.1 Consideraciones de desempeño y distancia

La figura siguiente [Figura 5.7], representa una perspectiva del despliegue de las principales tecnologías emergentes desde el punto de vista de la distancia y el ancho de banda.



Nota:

- MAN y SMDS pueden alcanzar mayores velocidades.
- MAN y SMDS se pueden extender a WAN.
- Las flechas indican tendencias de la tecnología ATM.

Figura 5.7 Tecnologías de red.

Las LAN Ethernet y Token Ring están limitadas en cuanto a distancia a unos cientos de metros, y en cuanto a capacidad, a 16 Mbps. FDDI ofrece mayor capacidad que estas LAN (100 Mbps) y también puede cubrir distancias geográficas mayores (una topología de anillo de 200 Km), Fast Ethernet puede operar también a 100 Mbps, pero está restringida a una distancia de unos 200 metros. Todas estas tecnologías están restringidas en cuanto a su capacidad de transmisión y la posibilidad de abarcar áreas geográficas amplias.

DQDB (en su implementación con el Servicio de Conmutación de Datos Multimegabits [SMDS]), ofrece una combinación interesante de distancia y capacidad: puede abarcar un área geográfica extensa en Redes de Área Local convencionales. Aunque no existe una razón técnica por la que no pueda abarcar un área geográfica grande, se diseñó como una red para un área geográfica más o menos restringida, como una ciudad.

Frame Relay está dirigido a las Redes de Área Extensa, así que no está restringido por la distancia. Sin embargo, la capa física se está implementando en las tecnologías de portadora de T1, T3, E1 y E3. Por lo tanto, casi ninguna de las implementaciones de Frame Relay opera a más de 45 Mbps.

La tecnología ATM no está restringida a una velocidad de línea específica y el estándar no exige alguna solución de capa física específica; además, no está limitada por la distancia. De hecho, esta tecnología puede verse como una solución de conmutación y columna vertebral para Redes tanto de Área Extensa como de Área Local. Se muestra en la parte más alta del ancho de banda [Figura 5.6] porque se pretende que opere encima de fibra óptica de alta velocidad y SDH/SONET, pero implementaciones recientes están colocando ATM en medios de más baja velocidad, como par trenzado, a velocidades más modestas, como 12 Mbps. La interfase de tasa básica (BRI) de RDSI está siendo ofrecida por compañías telefónicas como servicio de 64 Kbps a hogares o empresas. Se posiciona como una alternativa a los módems de más baja velocidad, que ahora operan en los niveles de 30 Kbps o menos.

V.8.2 Redes de banda ancha

Muchas de las tecnologías emergentes se designan como redes multimedia de banda ancha. El propósito de una red multimedia de banda ancha es proporcionar un servicio de transporte para cualquier tipo de aplicación [Figura 5.8], de ahí el término “red multimedia”. Una red multimedia de banda ancha apoya el servicio telefónico, de video, de datos, las compras a distancia, CAD/CAM, etcétera.

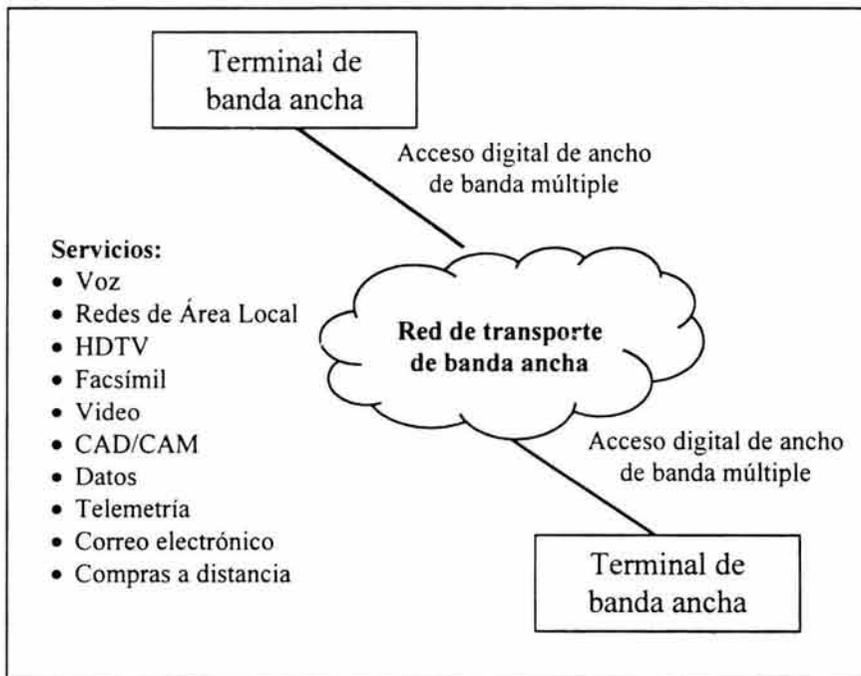


Figura 5.8 Apoyo a aplicaciones con redes de banda ancha.

Estas tecnologías emergentes generalmente se clasifican como redes de banda ancha. El término “banda ancha” se ha usado desde hace varios años y se han propuesto varias definiciones:

- La primera definición fue: una red que utiliza tecnología analógica de alta frecuencia como mecanismo de transporte para el tráfico de usuarios.
- Otra definición es: cualquier red que opera por encima del intervalo de frecuencias de la voz (0-4 KHz).
- Una definición más es: cualquier red que opera por arriba de la tasa primaria de RDSI (1.544 Mbps en Norteamérica y 2.048 Mbps en Europa).

V.8.3 Obtención de servicios para redes: ancho de banda por demanda

Un factor clave en el uso de estas tecnologías emergentes es un concepto llamado ancho de banda por demanda. El término significa que un usuario pueda solicitar y recibir capacidad de red (ancho de banda) dinámicamente. La herramienta para obtener ancho de banda por demanda se denomina tasa de información comprometida (CIR) o tasa de información sostenida (SIR). Se trata de una herramienta utilizada por las redes SMDS, Frame Relay y ATM para:

- Regular el flujo de tráfico de usuario,
- ofrecer al usuario ciertas opciones en cuanto a tasa de rendimiento,
- determinar ciertas estructuras de precios por el servicio.

Varias de las nuevas redes dan al usuario un servicio garantizado (en relación con el rendimiento) si la tasa de entrada del usuario no rebasa cierta CIR predefinida.

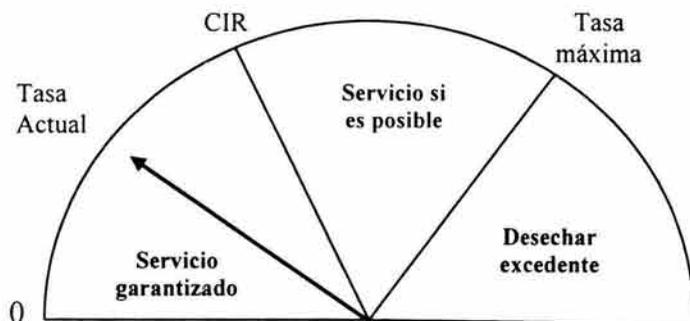


Figura 5.9 Empleo del CIR/SIR para decisiones de servicio (ancho de banda por demanda).

En la figura anterior [Figura 5.9] en tanto la flecha del cuadrante permanezca por debajo de esa CIR, el usuario tendrá garantizados los servicios de la red. Si el usuario excede la CIR durante cierto tiempo, la red no deberá desechar el tráfico que rebasa la CIR si ese tiempo no es muy largo. No obstante, cualquier tráfico enviado que exceda la CIR podría desecharse.

La palabra “podría” implica que lo más probable es que la red no deseche el tráfico si cuenta con suficientes recursos para transportar el tráfico de usuario durante el tiempo que se excede la CIR.

En la mayor parte de las implantaciones, la tasa actual de la entrada de un usuario podría exceder no sólo un breve “flujo en ráfaga” más allá de la CIR, sino también una tasa máxima permitida: una “tasa de exceso”. Si ocurre esta situación, la red podría desechar todo el tráfico en exceso por arriba de esta tasa.

Sea cual sea la tecnología que se escoja como mecanismo para la interfase usuario-red, el usuario deberá estudiar con detenimiento el método exacto por el cual suministra ancho de banda por demanda.

V.8.4 Dónde se proporcionan los servicios

Las operaciones entre el usuario y la red consisten en una serie de convenciones y protocolos mediante los cuales el usuario y la red envían y reciben tráfico entre sí. Este tráfico asume la forma de paquetes de control y carga útil de usuario. Se llama así porque es la carga útil de usuario la que reeditarán los ingresos para compensar los costos de operar la red y pagar dividendos a los dueños y accionistas de la red (o al menos, eso es lo que el proveedor espera).

Esta interfase también da convenciones para que el usuario y la red estipulen/negocien ciertas características de Calidad de Servicio (QoS). Por ejemplo la negociación de un retardo, CIR o rendimiento que se implementa en esta interfase.

Varias de las tecnologías más nuevas definen las operaciones entre redes. La interfase entre redes es muy importante, ya que todas las organizaciones permiten a sus usuarios iniciar una sesión en una red y luego comunicarse con otra organización que está en otra red. Aunque es muy probable que al usuario no tenga que preocuparle directamente las operaciones, convenciones y protocolos entre redes, sí son una cuestión importante para los administradores de redes.

Se requieren diferentes operaciones entre diferentes redes. Por ejemplo, las redes no necesitan proporcionar ciertos tipos de mecanismos de control de flujo en las fronteras entre redes, aunque dichos mecanismos sí son necesarios en la frontera entre el usuario y la red.

Por último, también se necesita un conjunto de convenciones y protocolos dentro de la red, si bien muchas redes se han implementado con protocolos propios dentro de la nube de redes, este enfoque está cambiando, y cada vez más se usan convenciones y protocolos estandarizados hasta definir cómo una red interna se comunica entre sus conmutadores. Así las tecnologías emergentes pueden consistir en tres conjuntos principales de protocolos y convenciones [Figura 5.10], (Black, 1999):

1. Los que se usan entre el usuario y la red.
2. Los que se usan dentro de la red .
3. Y los que se usan entre redes.

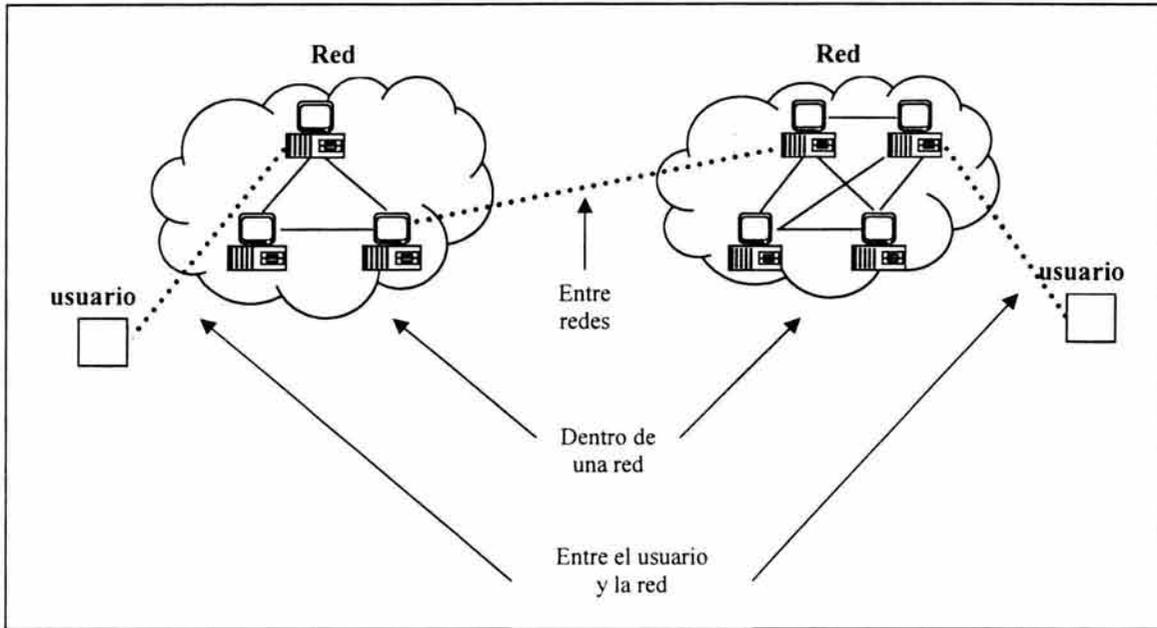


Figura 5.10 Dónde se proporcionan los servicios.

V.9 Tendencias en la tecnología

En el año de 1938 gracias a la transmisión radiofónica de una novela, el sueño de las telecomunicaciones dejaba de serlo, sólo quedaba esperar la evolución de los sistemas, dispositivos y técnicas para la transmisión de información a largas distancias de modo instantáneo. Esperar que la dinámica de lo cotidiano la envolviera.

A fines del siglo pasado era posible identificar unos cuantos acontecimientos científicos que a la larga seguramente generarían un importante cambio en el área. Hoy el número de acontecimientos, decisiones, inventos y desarrollos que contribuyen al avance de las telecomunicaciones es enorme y, de hecho, aumenta día con día. Parecería mentira, pero en un siglo (1850-1945) hubo menos cambios que los que ocurrirán en la próxima década o posiblemente en el próximo año.

El resumen de los acontecimientos científicos que ha permitido el desarrollo de las telecomunicaciones podría sonar pretencioso; sin embargo, mencionar todo lo que tecnológicamente se ha hecho para lograr el manejo de información que tenemos en la actualidad sería una labor ardua y casi imposible.

V.9.1 “Hardware” y “software”

Desde la proliferación comercial de las computadoras y las redes de comunicaciones en la década de 1960, la tendencia en las redes públicas y privadas ha sido tratar de proporcionar servicios más rápidos al usuario. Una razón es el creciente uso de “hardware” para proveer tales servicios. En la década de 1970, la arquitectura de comunicaciones de una computadora era casi exclusivamente “software”. Típicamente, la capa física (utilizando el Modelo de referencia OSI) consistía en “hardware”, y las capas de enlace de datos y de red estaban constituidas por “software”. El “software” se escribía en lenguaje de máquina o código de ensamblador a fin de operar con la mayor eficiencia y rapidez posible. Al comenzar a surgir estándares a fines de los años sesenta y principios de los ochenta, se hizo implantar en “hardware” algunas de las funciones de las capa de enlace de datos. Este paso fue fortalecido por el éxito del estándar de Control de Enlace de Datos de Alto Nivel (HDLC) publicado por la ISO, y dio pie a productos de “hardware” que podían adquirirse comercialmente los cuales podían ofrecerse en juegos de chips junto con “firmware”.

A fines de los años ochenta y principios de los noventa, algunos diseñadores y miembros de los organismos de estándares se dieron cuenta de que (en algunos sistemas estándares) había varias operaciones redundantes en las capas de enlace de datos y en la red. Por ejemplo, a veces había (y todavía hay en muchos sistemas) servicios de verificación de errores, control de flujo y determinación de secuencia en ambas capas. Por ello, se crearon nuevos estándares que eliminaran parte de esta redundancia.

V.9.2 Computadoras

En ningún lugar es más evidente el avance de la tecnología que en la creciente potencia de la Unidad Central de Proceso (CPU) y en la velocidad de la memoria de las computadoras. En unos pocos años, la potencia de cómputo ha aumentado exponencialmente varias veces. La primera computadora reconocida del mundo, ENIAC, creada en 1946, procesaba 100,000 instrucciones por segundo. El progreso entre 1945 y 1955 fue relativamente lento. Sin embargo, con el salto que representó la aparición de la tecnología de transistores, para 1975 una IBM 370 modelo 168 podía procesar dos millones de instrucciones por segundo. A partir de entonces, la potencia de cómputo de las máquinas ha aumentado a un ritmo fantástico. En consecuencia, muchos de los conceptos de las nuevas tecnologías avanzadas se están volviendo posibles gracias a la velocidad de estas nuevas máquinas.

La rapidez de los procesadores está aumentando a pasos agigantados. De hecho algunas máquinas, como las computadoras personales, están experimentando obsolescencia aproximadamente cada seis meses (desde el punto de vista del procesador). Además de los incrementos tan extraordinarios en las velocidades de cómputo logrados en los últimos años. La industria ha logrado también avances notables en la reducción de los costos de las computadoras. Desde 1975 hasta el presente, los costos han caído a un ritmo sorprendente. Esta rápida caída en los costos de cómputo ha propiciado el uso de tecnología avanzada y aplicaciones más potentes.

V.9.3 Canales de transmisión

El cimiento de buena parte de tecnologías emergentes es la fibra óptica. Una serie de avances realmente extraordinarios en los últimos años han abatido los costos y aumentado la capacidad de la fibra óptica. Los sistemas basados en tecnología óptica han aumentado drásticamente su capacidad, y al mismo tiempo han reducido su costo.

A medida que la tecnología ha madurado y ha aumentado la producción en masa de los sistemas, el costo del uso de esta tecnología ha caído exponencialmente desde 1975. Hace varios años, un sistema de 40 Mbps se consideraba de muy alta velocidad. Hoy en día son comunes los sistemas comerciales de 2.5 Gbps, y de 10 Gbps.

El progreso en la tecnología de portadoras de ondas luminosas llega en un momento fortuito, porque la industria ha estado progresando a un ritmo acelerado en el área de los gráficos de video generados por computadora.

Para que un verdadero entorno multimedia trabaje de forma eficiente y efectiva, son indispensables los gráficos de video de alta calidad. El uso de una estación de trabajo integral para voz, datos e imágenes de video es inevitable. No obstante, las tendencias deberán continuar durante los próximos años para que esta estación de trabajo integral se convierta en una herramienta práctica y económica en el trabajo.

V.9.4 Ethernet

Es la evolución de conmutación en la Red LAN y la consolidación en el "Backbone" LAN lo que ha traído repentinamente a éstas redes al borde de la convergencia una vez más. Es en esta época cuando existen cruciales diferencias.

En este tiempo las redes de datos tienen mayor capacidad, mayor complejidad y manejabilidad. Las Redes LAN han sido más rápidas e inteligentes, el siguiente paso es mejorarlas y hacerlas aún más inteligentes con las siguientes características:

- Calidad de servicio negociable.
- Tecnología apropiada para tráfico sensible al retardo y baja latencia.
- Características de administración más complejas.
- Un gran salto en cuanto a velocidad.

Entre tanto, las diferencias tradicionales entre las aplicaciones de voz y datos han desaparecido. Esto se usó para decir que la voz era manejada en tiempo real y la computación por lotes. Sin embargo, la computación cada vez está más cerca de los requerimientos de usuarios para aplicaciones en tiempo real y ser cada vez más interactiva. Las aplicaciones de voz se han diversificado para incluir almacenamiento y envío o aplicaciones de mensajes como correo de voz ("voice mail").

V.9.5 Aplicaciones multimedia

Las aplicaciones multimedia han dado mucho de que hablar en términos de tecnología. Ahora, se requiere una unión entre datos, voz e imagen para finalmente, combinarlos todos de manera eficiente para hacer más robustos los sistemas y resolver problemas de aplicación de los usuarios. A pesar de que multimedia es un entorno relativamente nuevo, algunas aplicaciones están mostrando claramente sus beneficios.

V.9.5.1 Voz y video en la red

La educación a distancia es sólo una parte de las diversas aplicaciones. Hay otras aplicaciones que pueden tomar “vida” en cuanto el video y la voz se puedan transmitir tan bien como se hace con los datos en los actuales equipos de escritorio. Esto es especialmente cierto para el video sobre una LAN; ahora LAN ofrece un mayor ancho de banda, que el que tradicionalmente han usado las interfases de la generación previa en sus comunicaciones. Esto ha mejorado las actuales aplicaciones. Algunas de las mejoras incluyen:

- Nuevos servicios de información como por ejemplo, la posibilidad de conocer información financiera.
- Videoconferencia en equipos de escritorio.

Estas aplicaciones traen un nuevo juego de requerimientos para la red. Éstas comparten un pequeño retraso en la transmisión. Por ejemplo, cuando los datos (o voz en la forma de datos digitales) entran a un ruteador, éste tiene que esperar por todo el paquete para ser cargado antes de que el ruteador lo reenvíe. Hay retrasos en el equipo de cómputo, desde que la máquina tiene que esperar por el paquete de datos para que sea construido antes de ser enviado hasta otro tipo de retrasos inherentes a la transferencia. El diseño de la red debe tomar en cuenta esos retrasos y tratar de eliminarlos.

La mayoría de las plataformas que hay en la red, tienen su mayor retraso acumulado cuando los paquetes cruzan a través de los puentes (“bridges”); pero en la medida que esos retrasos se puedan controlar como se hace en los ruteadores, esos sistemas serán más eficientes. Los paquetes en las redes tradicionales de datos tiene que esperar en una “cola” mientras los enlaces de la red están ocupados, esto retrasa la transmisión y hace menos eficiente la red.

Los problemas en el tráfico de multimedia son dos:

1. El retraso hace imposible que los enlaces corran en tiempo real, como lo demanda el video.
2. Los paquetes retrasados por tiempo indeterminado en las “colas” significa que por ejemplo, un paquete importante consiga meterse detrás de los paquetes menos importantes que aún están esperando para ser cambiados, como puede ser la transferencia de un archivo que no es urgente.

Al introducir video y voz en aplicaciones por la red, se requiere elevar los requerimientos de garantía de calidad de servicio en la red para garantizar las transferencias en forma adecuada, clara y confiable. “VoiceLAN” proporciona la solución a esos problemas.

V.9.5.2 “Voice LAN”

Existe una nueva expresión emergente “Voice LAN”, y es el hecho de que ahora la voz puede ser tratada tan sólo como una aplicación más en el mundo de la tecnología de la información. Esta es una afirmación importante, y ha sido posible gracias al rápido incremento en el desempeño de los ordenadores personales, ambos como servidores y clientes.

Los beneficios de traer voz sobre la Red LAN e integrarla con las plataformas de escritorio son muchas:

- Cómputo colaborativo: Mensajes de voz y datos pueden ser combinados dentro de una sola conversación entre múltiples usuarios.
- Los usuarios puede editar documentos con anotaciones de voz.
- La red puede enrutar y retransmitir mensajes de voz como lo hace hoy con archivos y el correo electrónico.
- Las aplicaciones de PC pueden ser integradas con el resto de las aplicaciones de tecnología de la información, debido a que el rastreo de llamadas es más eficiente.
- Incrementar la productividad a través del uso de “pizarrones blancos” usando voz y caracteres sobre la pantalla, compartidos por participantes en conferencia de llamadas.
- Mejorar el sistema de respuesta telefónica recuperando datos sobre el teléfono.
- Mejorar las comunicaciones corporativas y entrenamiento a través de mensajes de voz/datos transmitidos de forma masiva.
- Mejorar la administración de la red.
- Eficiencia de costos y protección de la inversión en tecnología de la información.
- Disponibilidad para integrar con el Internet, lo cual significa hacer un uso mayor de la telefonía estilo Internet.
- Soluciones más intuitivas para usuarios ayudándolos a ser más productivos.

Un completo alojamiento de nuevas aplicaciones de beneficios potenciales para el negocio, son una realidad. Estas aplicaciones, incrementarán más allá de lo normal el desempeño de los usuarios, hacer más complejo el uso de la red, y lo más importante es llevar al negocio a una eficiencia en relación a sus costos; a través de consolidar los equipos de administración, por medio de un uso más efectivo de la red y a través de un alojamiento de otros factores.

V.9.6 Ideas recientes sobre RDSI

Tal como una solución ampliamente propuesta en los inicios de la década de los ochenta, cuando la Red Digital de Servicios Integrados (RDSI) parecía algo que pudiera proporcionar una oportunidad para las PBX de tomar responsabilidades sobre las redes de datos. Este acercamiento rindió virtualmente cero dividendos. Aunque RDSI sonó promisorio, su impacto actual ha sido mínimo.

Parte de la razón para este concepto, es la forma en que los operadores de servicios públicos de hoy, se concentraron en su propia economía de escala en la red pública, simplemente asumieron que RDSI fue apropiado para el negocio. El resultado de esta estrategia fue un circuito expansivo con un cierto monto de integración, pero no suficiente. La demanda por líneas digitales fue baja y no había muchas para configurar una red; en el mejor de los casos, los operadores de servicios estuvieron ofreciendo RDSI.

Parcialmente debido a las limitaciones de los ofrecimientos de RDSI, la convergencia a través de las PBX y los teléfonos alámbricos, fueron la peor idea en el peor momento; las redes eran lentas, los ordenadores de escritorio ya habían alcanzado el punto en el que la transferencia de archivos a 64 Kbps fuera impráctico, la PBX en ningún momento estuvo cerca de desenvolverse como un “host” para la administración de la red y otro “software” cliente-servidor que rápidamente lo colocara como el administrador de la Red LAN.

V.10 Problemática en redes de voz

La telefonía IP o Voz sobre IP (VoIP) conjuga dos mundos históricamente separados: la transmisión de voz y la de datos. Se trata de transportar la voz, previamente convertida a datos, entre dos puntos distantes. Esto posibilitaría utilizar las redes de datos para efectuar las llamadas telefónicas, y yendo un poco más allá, desarrollar una única red que se encargue de cursar todo tipo de comunicación, ya sea vocal o de datos.

Las redes desarrolladas a lo largo de los años para transmitir las conversaciones vocales, se basaban en el concepto de conmutación de circuitos, es decir, la realización de una comunicación requiere el establecimiento de un circuito físico durante el tiempo que ésta se sostiene, lo que significa que los recursos que intervienen en la realización de una llamada no pueden ser utilizados en otra hasta que la primera no finalice, incluso durante los silencios que suceden dentro de una conversación típica.

En contraposición a esto tenemos las redes de datos, basadas en el concepto de conmutación de paquetes, o sea, una misma comunicación sigue diferentes caminos entre origen y destino durante el tiempo que dura, lo que significa que los recursos que intervienen en una conexión pueden ser utilizados por otras conexiones que se efectúen al mismo tiempo.

Las redes de conmutación de paquetes también tienen desventajas, transportan la información dividida en paquetes, por lo que una conexión suele consistir en la transmisión de más de un paquete. Estos paquetes pueden perderse y además no hay una garantía sobre el tiempo que tardarán en llegar de un extremo al otro de la comunicación. Estos problemas de calidad de servicio telefónico a través de redes de conmutación de paquetes van disminuyendo con la evolución de las tecnologías involucradas, y poco a poco se va acercando el momento de la integración de las redes de comunicaciones de voz y datos.

V.10.1 Calidad en la voz

La medida relativa de percepción de calidad de voz en los extremos de la red, es una nueva cuestión en la comunicación, donde la calidad es ubicada en términos de pérdida de paquetes o errores de bit. El propósito de la Telefonía IP es proporcionar un nivel de calidad de recepción de voz que al menos iguale el nivel que se tiene en la Red Telefónica Pública Conmutada (PSTN).

La calidad de voz [Figura 5.11] es más exacta cuando se liberan los datos y esto lleva muchos factores entre ellos resaltan: retraso, pérdida de paquetes, ancho de banda y tipo de “codecs” así como, la implantación de la aplicación. Hay muchos factores que influyen la percepción de calidad de voz.

Los más importantes son:

- Retraso de paquetes.
- Variación en el retraso.
- Pérdida de paquetes.
- Ancho de banda.

Otros factores importantes para la calidad de voz son:

- Codificación silenciosa.
- Eco.

Es posible tener dos sistemas: uno para un mejor sonido y otro para garantizar la calidad de transmisión.

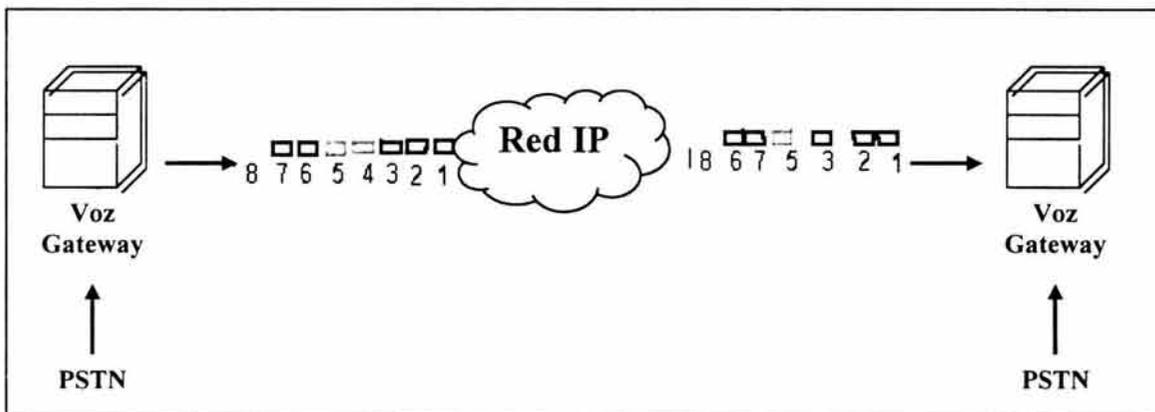


Figura 5.11 Calidad de Voz.

V.10.2 Percepción de la calidad de voz

La calidad de voz es una cuestión que se está usando para la comunicación y que se requiere para que dicha comunicación se dé. El diagrama de la [Figura 5.12] es el resultado de pruebas donde las personas han percibido una buena calidad en la recepción de voz y esto es considerado como una buena conclusión en relación a lo que la transmisión de voz demanda para VoIP y para cualquier transmisión de información por voz.

El diagrama demuestra el nivel de calidad de voz percibida durante las transmisiones en relación a la pérdida de paquetes y los retrasos en la llegada de la información.

La gráfica muestra:

- Área aceptable (buena calidad), <5% de pérdida de paquetes y <200 ms en el retraso.
- Área aceptable (baja calidad), <10% de pérdida de paquetes y <400 ms en el retraso.
- Área no aceptable, >10% de pérdida de paquetes y >400 ms en el retraso.

Para una buena calidad, el retraso debe ser menor a 200 ms y la pérdida de paquetes debe ser menor al 5%.

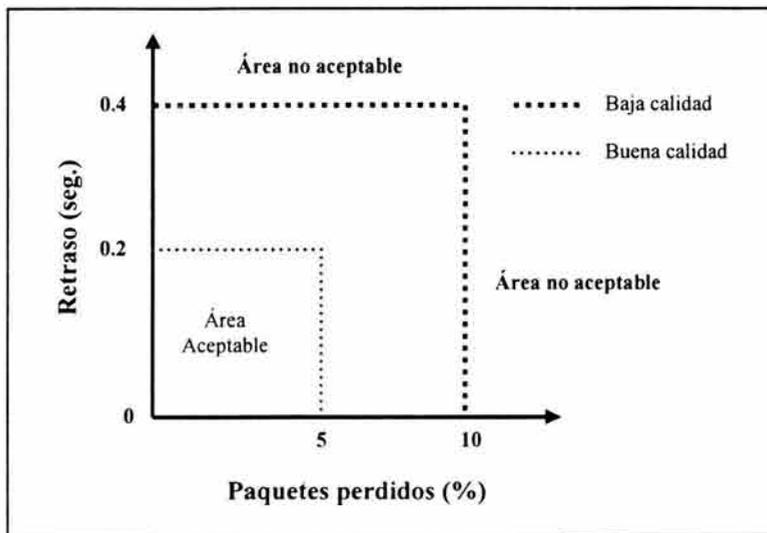


Figura 5.12 Percepción de la calidad de voz.

V.10.3 Retraso de paquetes y sus variaciones

La aplicación VoIP es requerida considerando el hecho de que el flujo original de paquetes será retrasado y algunos paquetes individuales serán retrasados más que el resto de los paquetes. Algunos paquetes se pueden perder al sobrepasar la capacidad de los ruteadores o también debido al viaje alterno en rutas que causa la pérdida de paquetes de forma irreversible. El sistema VoIP es otra aplicación de IP y usa la red como su propia interfase, pero esto no puede permitirse en una conexión segura libre de errores.

El eco es un problema serio en la comunicación de voz; se determina de forma primaria en los primeros 50 milisegundos de iniciada la transmisión, por lo tanto los sistemas VoIP deben cuantificar el valor del eco e implementar después, una forma de cancelarlo en la transmisión. El problema de saturación al hablar es el problema que afronta uno de los usuarios que llama a otro en una transmisión de voz; esto es significativo si se llega a tener un retraso en la transmisión mayor a 250 milisegundos. El objetivo es reducir el retraso de las transmisiones de tal forma que se tenga una buena calidad en la transmisión de un paquete de información en la red.

Si los paquetes transmitidos son retrasados en su totalidad, éstos llegarán algún tiempo después de ser enviados. Sin embargo, este retraso nunca es constante y varía de paquete a paquete. Esta variación es llamada “jitter” y se mide como la máxima diferencia en retraso a partir de un valor promedio de retraso. La variación (“jitter”) es la desviación o desplazamiento de los pulsos en una señal de alta frecuencia digital. Como su nombre sugiere, la variación puede ser minuciosa en los pulsos que se consideren inseguros. La desviación puede ser en términos de amplitud, fase o en el ancho de banda del pulso. Otra definición es que “es el período de frecuencia desplazado de la señal desde su ubicación ideal”.

La variación puede introducir chasquidos u otros efectos indeseables en las señales de audio y por consiguiente, pérdida de datos transmitidos entre los equipos que conforman la red. El valor de la variación depende de la aplicación que se esté dando.

Los siguientes valores son los más significativos en la medida de la variación (“jitter”):

- Retraso en una LAN de una sola ruta, 10 ms.
- Variación en una LAN, 1 ms.
- Retraso en una WAN de una sola ruta, 100 ms.
- Variación en una WAN, 10 ms.
- Los retrasos de Internet están sobre 100 ms, típicamente son 300 ms o más.

El retraso y variación [Figura 5.13] son causados por diferentes partes en un sistema de Telefonía IP, como por ejemplo, los “codecs”, el sistema operativo en la terminal y en la puerta de enlace (“gateway”) y el propio manejador del IP. La “variación” es generada por interferencia electromagnética y su mezcla con otras señales.

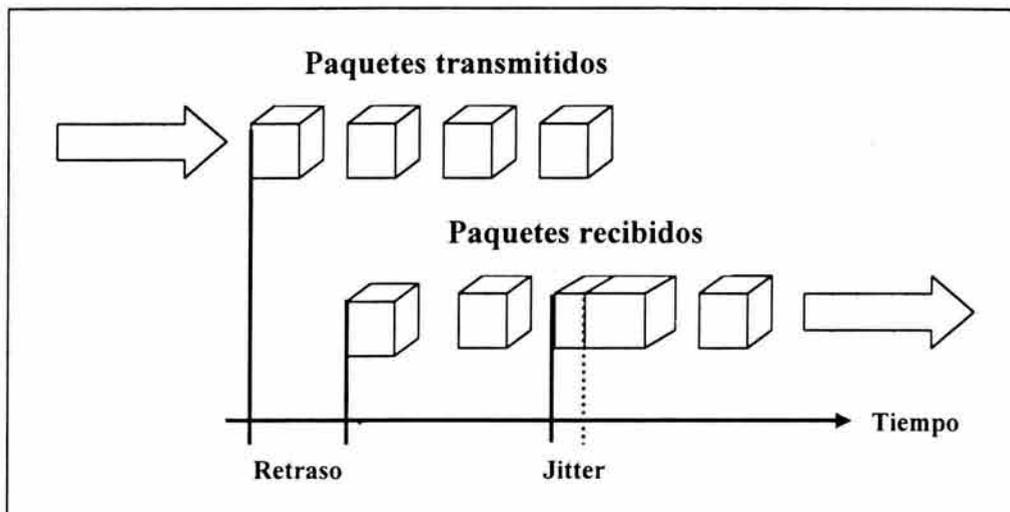


Figura 5.13 Retraso y Variación.

V.10.4 Almacenamiento momentáneo de paquetes (“buffering”) y pérdida de paquetes

En estricto sentido, el flujo de datos es almacenado temporalmente antes de su decodificación. Esto permite recibir los datos de una forma ordenada. El tamaño correcto del canal de retención momentáneo (“buffer”) depende del valor de la variación (“jitter”) y existen varias implantaciones ya elaboradas las cuales usan tamaños de “buffer” dependiendo de las condiciones de la red. Hay dos tipos de manejo de variación del “buffer”:

1. Fixed play-out delay (el “buffer” almacena cada uno de los paquetes por un tiempo específico).
2. Adaptive play-out delay (este tiempo se ajusta de acuerdo a la variación del retraso de la red).

Las redes IP no pueden garantizar que todos los paquetes serán liberados en el orden requerido debido a la variación de los retrasos. Bajo cargas pico y durante períodos de congestión causados por ejemplo por fallas en el enlace o por problemas de capacidad, los paquetes pueden ser abandonados.

Esto debido a lo crítico de los tiempos en las transmisiones de voz; sin embargo, los esquemas normales de retransmisión basados en TCP no están disponibles. Un número de accesos o aproximaciones son usados para compensar cada paquete perdido incluyendo la interpolación de voz por una retransmisión del paquete perdido enviando información redundante. Una pérdida de paquetes mayor al 10%, generalmente no es aceptable.

Es importante considerar que un almacenamiento temporal de datos (“buffering”) [Figura 5.14] no previene pérdidas en la transmisión, ya que sí se pueden presentar en un proceso real de transmisión.

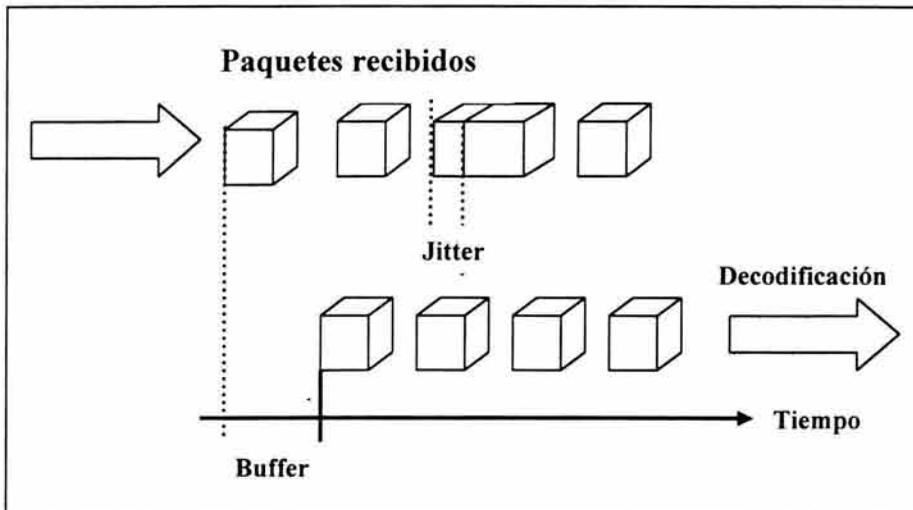


Figura 5.14 Almacenamiento momentáneo de paquetes.

V.10.5 Retrasos en VoIP

Para VoIP los retrasos son debidos a:

- Los procesos de codificación y decodificación toman tiempo de proceso en los extremos de la conexión.
- El proceso de enmarcado (“framing”) toma cierto tiempo.
- Hay retrasos asociados con la transmisión.
- Hay retrasos causados por el uso de una variación del canal de retención momentáneo (“buffer”).

Para VoIP la gran diferencia entre una “buena” y una “mala” red es el valor del retraso (“delay”) y la variación (“jitter”). En el peor de los casos se tiene alto retraso en la red y/o un alto valor de variación; una alta variación del “buffer” es usada resultando en un cierre de retraso intolerable.

Para Internet, el mejor caso es con un tiempo de 180 ms y el peor caso es con 330 ms. Lo recomendado para una Red de Área Local son 90 ms y 140 ms.

V.10.6 Retrasos en la Red Telefónica Pública Conmutada (PSTN)

En PSTN los valores están listados sólo como alta o baja frecuencia de retraso porque ITU-T tolera diferentes retrasos sobre diferentes valores en frecuencia (baja y alta, respectivamente). El Organismo ITU-T recomienda el máximo retraso entre dos abonados de 150 ms y para conexiones internacionales un máximo de 400 ms para permitir al satélite realizar la conexión. Un módem de telefonía digital de intercambio (por ejemplo, una PBX) tiene un retraso menor a 10 ms.

V.11 Problemática en la administración de redes

Los sistemas de administración son un aspecto clave para aprovechar plenamente las ventajas de las redes actuales, por otra parte cada vez más grandes y complejas. El ideal de la administración de sistemas es la administración integrada, es decir, controlar todos los recursos con independencia de su origen o tipo, lo cual permitiría un acceso completo a entornos multifabricante y con una administración flexible.

Los fabricantes ofrecen soluciones no siempre compatibles entre sí que, en ocasiones, no responden a las necesidades de los usuarios dado que éstas pueden ser diversas. En el mundo actual, en el que la informática gira en torno al concepto de red, el trabajo de los administradores de sistemas es muy complejo. Su misión consiste en mantener en funcionamiento recursos tales como ruteadores, concentradores, servidores, así como cada dispositivo crítico que conforma la red.

Hay gran cantidad de motivos por los cuales un administrador necesita monitorizar entre otros: la utilización del ancho de banda, el estado del funcionamiento de los enlaces, la detección de cuellos de botella, detectar y solventar problemas con el cableado, administrar la información de encaminamiento entre máquinas, etcétera. La monitorización de la red es también un buen punto desde el cual comenzar el estudio de los problemas de seguridad.

En muchos casos, la red de una organización está enlazada mediante costosos enlaces a Redes de Área Extensa (WAN) o con la Internet, y cuyos costos dependen del volumen de tráfico. Es muy importante mantener un registro estadístico del tráfico que circula por estos enlaces. Ésta situación es bastante común en Europa, donde los enlaces X.25 son todavía de uso corriente. La tarificación de este tipo de líneas se realiza en función del número de paquetes enviados y recibidos.

Otros tipos de enlaces, como los punto a punto (Frame Relay), son de tarifa plana. En éstos la compañía telefónica ha de garantizar un ancho de banda, el cual es importante monitorizar.

V.11.1 Tendencias

El incremento de ancho de banda y la mejora sustancial de la calidad de servicio. Todas estas innovaciones han dejado anticuadas las plataformas de administración existentes que en vano intentan asimilar la aparición precipitada de nuevos dispositivos como conmutadores locales, arquitecturas tipo cliente/servidor, servicios como Frame Relay y tecnologías como ATM por citar sólo algunos de los cambios más relevantes. A pesar de los esfuerzos por adaptarse en tiempo real, la mayor parte de sistemas de administración ha incumplido parcialmente sus objetivos de entregar nuevas versiones totalmente acomodadas a estos nuevos entornos, e incluso se comenta que algunas de ellas puede tardar varios años en actualizarse, (Caballero, 1998).

V.11.2 Avances en la administración de redes LAN

Las redes LAN han desarrollado un complejo y flexible sistema de administración de red del cual las redes de voz podrían tomar ventaja, mientras la administración de las redes LAN avanza de manera considerable, la administración de la voz permanece, relativamente, sin cambios. Visto desde otro enfoque, las redes de voz tienen fortalezas de las cuales las redes de datos podrían obtener beneficios, las redes de voz tradicionalmente han sido poderosas sobre el monitoreo de tráfico y costos, por ejemplo.

Una convergencia entre las dos redes, es una proposición obvia, una vez que comparten la misma topología en el “backbone”, ambas son digitales (o pueden serlo), y el sistema de telefonía podría beneficiarse de las capacidades agregadas y flexibilidad de los niveles de grupos de trabajo que hoy disfrutaban los usuarios de redes de ordenadores. En el pasado, sin embargo, la observación de que el cableado telefónico es tendido en cada escritorio dentro de los edificios lleva al error de creer que las redes de voz podrían ser un vehículo para entregar más que comunicaciones de voz, si una apropiada solución técnica pudiera ser encontrada.

V.12 Seguridad en redes

El tema de la seguridad es importante dentro de todas las redes de comunicaciones y, especialmente, en las organizaciones que tratan con datos sensibles y además sus redes tienen un tamaño grande o contienen muchas interconexiones con otras redes.

Desde los inicios de los centros de proceso de datos y hasta hace pocos años, la preocupación por la seguridad de la información se destinaba, casi exclusivamente, a cuidar los accesos físicos de personas no autorizadas y a los respaldos de los dispositivos magnéticos que contenían la información en previsión de fallos en el “hardware”. A medida que se extendió el uso distribuido de la informática por toda la organización, comenzó a temerse por los accesos no autorizados a la información confidencial.

En la segunda mitad de la década de los ochenta comenzó a popularizarse entre informáticos toda una jerga médica aplicada al mundo de los ordenadores, haciéndose habituales términos como virus, antivirus, puertas traseras (“backdoors”), caballos de troya, etcétera. Habían aparecido los virus informáticos que comenzaron a infectar a miles de ordenadores personales causando incalculables destrozos en muchas organizaciones, algunas de las cuales prometerían no volver a arrancar sus ordenadores en viernes si era día 13. Las patologías provocadas por las infecciones informáticas han dado un toque de atención ante la promiscuidad en las copias de programas o la ejecución frívola de productos obtenidos a través de redes.

La habilidad de los “crakers”, la simplicidad de muchos sistemas de los protocolos de comunicaciones y la debilidad de muchos sistemas operativos pueden causar serios problemas de seguridad a las organizaciones, aunque ya se dispone de un importante número de soluciones para luchar contra todo tipo de ataques, (Caballero,1998).

V.13 Desarrollo de Internet

Originalmente, Internet fue desarrollado para direccionar los recursos de los ordenadores. La aplicación que rápidamente se generalizó fue el correo electrónico. Hasta el arribo del servicio de www en 1993, el tráfico de información en Internet era relativamente bajo y los requerimientos de ancho de banda eran limitados. Pero, con la llegada de www los requerimientos de ancho de banda se incrementaron drásticamente. Imágenes, páginas web avanzadas, grandes archivos adjuntos y una gran cantidad de nuevos usuarios han dado como resultado una mayor expansión de Internet.

Las nuevas comunicaciones requieren servicios de convergencia, y éstos son:

- Extenderse a la población de escasos recursos.
- Comunicar nuevas comunidades.
- Impactar el estilo y calidad de vida.
- Etcétera.

V.13.1 Limitaciones del modelo de direcciones IP

Internet a crecido sumamente rápido en años recientes, en 1994 tenía más de 32,000 redes conectadas, con más de 3.8 millones de computadoras en más de 90 países. IPv4 con un campo de direcciones de 32 bits provee más de 4 mil millones de direcciones posibles, parecería que el esquema de direcciones IP es más que adecuado para la tarea de direccionar todos los datagramas de los “hosts” en Internet, desafortunadamente este no es el caso, por varias razones, incluyendo las siguientes:

El direccionamiento IP está dividido en dos partes, número de red y número de “host”, el cual es administrado separadamente. Aunque el espacio de direcciones dentro de una red puede ser ocupada esparcidamente, tan lejano como el espacio de direcciones IP le permita, si un número de red es usado entonces todas las direcciones dentro de esa red son ocupadas. El espacio de direcciones para las redes esta estructurado en clase de redes A, B, C de diferente tamaño, el espacio dentro de cada una de estas clases requiere ser considerado separadamente. El esquema de direccionamiento IP requiere que a todas las redes IP les sea asignado un número de red único, aunque actualmente estén o no conectadas al Internet.

El crecimiento de TCP/IP (usado en nuevas áreas), podría resultar en una explosión rápida del número requerido de direcciones IP. Por ejemplo, el uso extendido de TCP/IP para conectar terminales electrónicas, puntos de venta o para recibir cable por televisión podría incrementar enormemente el número de “hosts” IP. El esquema de direccionamiento IPv4 con una única dirección IP por cada “host” (no ruteador) podría cambiar en un futuro (RFC 1681).

Estos factores significan que el espacio de direcciones es mucho más restringido de lo que el análisis anterior puede indicar. Este problema es conocido como: agotamiento de las direcciones IP.

V.13.2 IP: La Siguiete Generación (IPnG)

Métodos para resolver el problema de agotamiento de direcciones IP ya se están empleando, pero eventualmente, el espacio de direcciones IP será agotado. El IETF tiene un grupo trabajando sobre las expectativas del tiempo de vida del esquema de direcciones IP (ALE) con el propósito de proporcionar una fecha estimada cuando las direcciones IP se agoten, las expectativas son (como lo informo ALE en diciembre de 1994) que el espacio de direcciones IP estará agotado en algún momento entre el 2005 y el 2011. Antes que esto pase, un reemplazo a la versión de IP (IPv4), fue necesario, este reemplazo es conocido como IP: la Nueva Generación (IPnG). Existen varios grupos de trabajo relacionados con el funcionamiento de IPnG:

- IPnG Requirements (IPNGREQ),
- Transition And Co-Existence Including Testing (TACIT),
- Y un grupo propuesto para IPnG,

Todos estos grupos son temporales y se espera que sean unidos a otros grupos de trabajo en otras áreas cuando el proceso de definición de IPnG concluya. En Julio de 1994 en la reunión del IETF en Toronto, el IPnG "Area Directors" del IETF presento el RFC 1752 (la recomendación para el IP "Next Generation Protocol"). Esta recomendación fue aprobada por el IETF en Noviembre de 1994 y se hizo una norma (estándar). Estos eventos fueron la culminación de mucho trabajo y discusión, el cual involucro a muchas partes interesadas. El consejo de administración publicó el RFC 1550-IP, donde se establecen los requerimientos para IPnG. Algunos de los requerimientos más importantes son:

- IPnG debe permitir el encapsulamiento de su propio paquete o de otros protocolos.
- IPnG debe permitir agregar clases de servicios para distinguir tipos de datos que están siendo transmitidos, como por ejemplo, tráfico isócrono como audio y vídeo en tiempo real.
- IPnG debe proporcionar direccionamiento "multicast", de forma que este completamente más integrado con el resto del conjunto ("suite") de protocolos que la implementación actual.
- IPnG debe proporcionar autenticación ("authentication") y encriptación ("encryption").
- IPnG debe preservar las virtudes de IPv4: robustez, independencia de las características físicas de la red, alto desempeño, topología flexible, extensibilidad, servicio de datagramas, direccionamiento globalmente único, un protocolo de control internamente construido, estándares libremente disponibles.
- La implementación de IPnG debe comprender un plan de transición sencillo.
- IPnG debe coexistir con IPv4.

Existieron tres propuestas principales para IPnG:

1. Common Architecture for the Internet (CATNIP).
2. TCP and UDP whit Bigger Address (TUBA).
3. Simple Internet Protocol Plus (SIPP).

V.13.3 IP Versión 6 (IPv6)

El Consejo de Administración determinó que las tres propuestas fueron insuficientes para cumplir con la lista de requerimientos aceptada, pero SIPP, era la propuesta más cercana a la lista de requerimientos.

Después de algunos cambios a la propuesta original, por la instancia de usar 128 bits en lugar de 64 bits de direccionamiento, el Consejo de Administración de IPnG dictaminó que SIPP era la base para IPnG y que características de las otras propuestas podrían ser agregadas para cubrir el resto de los requerimientos. La solución propuesta fue llamada IP Versión 6 (IPv6).

La definición de IPv6 esta aún en progreso, IPv6 usa el término paquete en lugar de datagrama, pero el significado es el mismo, aunque los formatos son diferentes. IPv6 introduce un nuevo término: nodo, que puede ser un “host” o un ruteador.

Para un sistema corriendo IPv6, un “host” es un nodo que no reenvía paquetes IPv6, los cuales no están direccionados hacia él. Un ruteador es un nodo el cual reenvía paquetes IP no direccionados hacia él.

V.14 Limitaciones de la Internet actual

La evolución de las tecnologías de información ha puesto los ojos en la Internet como la gran plataforma de comunicación globalizada. Si bien es cierto, la Internet ha jugado un papel muy importante en lo económico, político y educativo sin mencionar otras áreas sociales, sus aspectos de comercialización dejan mucho que desear, sobre todo en el servicio prestado al usuario de la última milla, donde los problemas de conectividad, congestión en los nodos del proveedor de servicio y la falta de opciones con quien contratar el servicio son ejemplos de esta situación.

El desarrollo de la Internet continua en aumento, tal es la creación de nuevas aplicaciones multimedia como Televisión de Alta Definición (HDTV), Voz sobre IP (VoIP), videoconferencia y sistemas de teleinmersión para medicina, mecánica y juegos.

Estas nuevas aplicaciones generan una gran cantidad de tráfico o ancho de banda, que va desde 1.5 Mbps para el estándar H.323 de videoconferencia hasta los 20 Mbps o más para aplicaciones de videoconferencia en tercera dimensión e IP-HDTV.

Este tipo de aplicaciones definitivamente no podrían ser utilizadas en el esquema general de la Internet actual, por limitantes no solo del ancho de banda sino por otros aspectos como el de seguridad, esquemas calidad de servicio (QoS), IP “multicast”, etcétera.

V.14.1 Internet 2 como solución

En los últimos años se ha creado una iniciativa por proveer una Internet con características especiales para el soporte de nuevas aplicaciones avanzadas. A esta nueva Internet le denominan Internet 2 el cual es un proyecto de Norteamérica, está formada por instituciones de investigación y educación de México, EUA y Canadá. En México, Internet 2 es un proyecto nacional el cual dio inicio en Abril de 1999. En esta corporación se planean y diseñan los mecanismos que regirán a la Internet 2 mexicana, de acuerdo a las necesidades y situación económica del país. Actualmente, cuenta con una red ATM de alta velocidad operando a los 155 Mbps, conectando las principales ciudades de México, Monterrey, Tijuana, Guadalajara y el D.F. (Rivera,2002).

V.14.1.1 Ventajas que ofrece Internet 2

Gran ancho de banda: Una de las características fundamentales de Internet 2 es el manejo de un gran ancho de banda. En la actualidad, dependiendo de los recursos disponibles, se tienen velocidades del orden de los cientos de Megabits por segundo, pero la tendencia es alcanzar rangos de Gigabits por segundo según la demanda.

Calidad de los servicios (“Quality of Service”): En la Internet, todos los paquetes de información tienen la misma prioridad, de tal forma que si se envía video por la red, a la vez que se transfiere un archivo de datos, ambas operaciones compiten por el mismo canal, por lo que probablemente los cuadros de video no lleguen a su destino en forma continua, es decir, se tendrá un congelamiento o al menos un deterioro en la calidad de la imagen. En cambio, en Internet 2, se le puede dar prioridad al video, de tal forma que se garantice que todos los cuadros lleguen a tiempo y, sólo en los espacios que el video deje libre, se irán transmitiendo los paquetes del archivo de datos. Esta característica permite también mantener en un nivel adecuado el retardo de la información. Siendo importante sobre todo para sistemas de control de dispositivos a distancia.

Transmisión multipunto (“multicast”): Otra solución que ofrece Internet 2 es que en Internet normal, cuando se desea transmitir información a un conjunto de usuarios (por ejemplo: en la transmisión de un evento en vivo), se envían los mismos paquetes de la señal de video a cada uno de los usuarios, multiplicando el tráfico en la red; en Internet 2 se está experimentando una tecnología conocida como “multicasting”, mediante la cual se envía, una sola vez, cada paquete con la información necesaria para que llegue a todos los usuarios que deben recibirlo.

Retardo reducido y uniforme (“low latency/low jitter”): En aplicaciones sensibles al retardo de la información es vital reducir éste al mínimo posible; en Internet 2 con la combinación de un gran ancho de banda, la priorización de los servicios y técnicas avanzadas de enrutamiento se logran retardos realmente muy pequeños en el orden de los milisegundos extremo a extremo. Esto permite desarrollar sistemas de control a distancia de equipos muy complejos, en los cuales demasiado retardo de la información de control podría resultar fatal.

Mayor seguridad, privacidad y confiabilidad. Otro aspecto importante que se está experimentando en Internet 2 consiste en la mejora de la seguridad y privacidad de la red, utilizando protocolos que permitan autenticar plenamente el origen de los datos y que asegure la integridad y confidencialidad de los mismos, (Rivera, 2002).

V.15 Carencias de Internet y MPLS como solución

Uno de los factores de éxito de la Internet actual está en la aceptación de los protocolos TCP/IP como estándar para todo tipo de servicios y aplicaciones. La Internet ha desplazado a las tradicionales redes de datos y ha llegado a ser el modelo de red pública del siglo XXI.

Si bien es cierto que la Internet puede llegar a consolidarse como el modelo de red pública de datos a gran escala, pero puede no llegar a satisfacer todos los requisitos de los usuarios, principalmente los de aquellos de entornos corporativos, que necesitan la red para el soporte de aplicaciones críticas. Una carencia fundamental de la Internet es la imposibilidad de seleccionar diferentes niveles de servicio para los distintos tipos de aplicaciones de usuario.

La Internet se valora más por el servicio de acceso y distribución de contenidos que por el servicio de transporte de datos, conocido como de "best-effort". Si el modelo Internet ha de consolidarse como la red de datos del siglo XXI, se necesita introducir cambios tecnológicos fundamentales, que permitan ir más allá del nivel "best-effort" y puedan proporcionar una respuesta más determinística y menos aleatoria.

La arquitectura de Conmutación por Etiquetas Multiprotocolo (MPLS), es la base para la inclusión en la red de nuevas aplicaciones y para poder ofrecer diferentes niveles de servicio, en un entorno de mayor fiabilidad y con las garantías necesarias.

MPLS es un estándar emergente de la Fuerza de Trabajo de Ingeniería de Internet (IETF) que surgió para aprobar diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes a mitad de los años 90.

Según el énfasis (o interés) que se ponga a la hora de explicar sus características y utilidad, MPLS se puede presentar como un sustituto de la arquitectura IP sobre ATM. También como un protocolo para hacer túneles (sustituyendo a las técnicas habituales de "tunneling"). O bien, como una técnica para acelerar el encaminamiento de paquetes. En realidad, MPLS es una tecnología de encaminamiento intermedio entre la capa de enlace (nivel 2) y la capa IP (nivel 3) capaz de asociar la potencia de la conmutación de una con la flexibilidad del encaminamiento de la otra.

Pero, ante todo, se debe considerar MPLS como el avance más reciente en la evolución de las tecnologías de "routing" (el control de la información sobre la topología y tráfico en la red) y "forwarding" (el envío en sí de datos entre elementos de la red) en las redes IP, lo que implica una evolución en la manera de construir y administrar estas redes.

Los problemas que presentan las soluciones actuales de IP sobre ATM, tales como la expansión sobre una topología virtual superpuesta, así como la complejidad de administración de dos redes separadas y tecnológicamente diferentes [Figura 5.15], quedan resueltos con MPLS. Al combinar en uno solo lo mejor de cada nivel (la inteligencia del “routing” con la rapidez del “switching”), MPLS ofrece nuevas posibilidades en la administración de “backbones”, así como en la provisión de nuevos servicios de valor añadido, (Barberá, 2001).

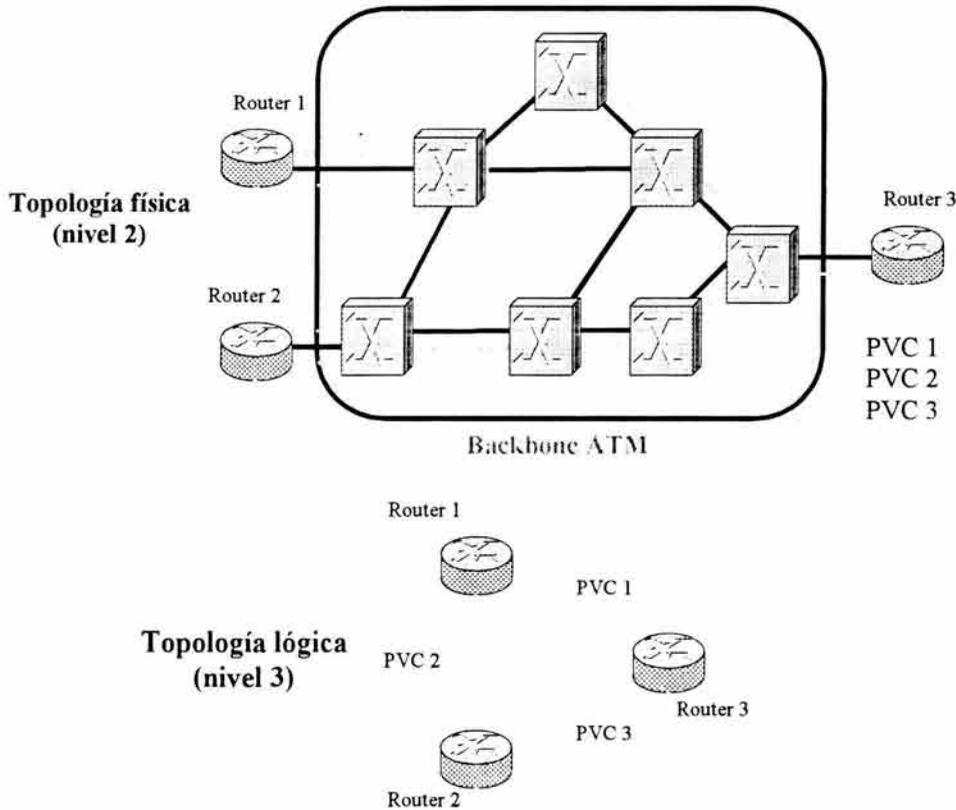


Figura 5.15 Diferencia entre la topología física de una red ATM con la de la topología lógica IP superpuesta sobre la anterior.

El crecimiento imparable de la Internet, así como la demanda sostenida de nuevos y servicios más complejos, supone cambios tecnológicos fundamentales respecto a las prácticas habituales desarrolladas a mitad de los años 90. Nuevas tecnologías de transmisión sobre fibra óptica, proporcionan una eficaz alternativa al ATM para multiplexar múltiples servicios sobre circuitos individuales. Además, los tradicionales conmutadores ATM están siendo desplazados por una nueva generación de ruteadores con funciones especializadas en el transporte de paquetes en el núcleo de las redes. Esta situación se complementa con MPLS y se considera fundamental en la construcción de los nuevos cimientos para la Internet de los próximos años. La tecnología MPLS integra IP y ATM y además proporciona soluciones para incrementar la velocidad y la prioridad de tráfico en el cable de la red. Esto requiere inversión en nuevos ruteadores capaces de leer la información que tiene los encabezados de cada paquete y asignar rutas específicas para distribuir los datagramas, (RISQ, 2003).

V.16 Servicios Diferenciados

Diffserv (DS; “Differentiated Services”) y MPLS son dos estándares separados los cuales pretenden ayudar a resolver el problema de calidad de IP. Cuando se discute sobre los niveles de calidad es importante diferenciar entre Calidad de Servicio (QoS) y Clase de Servicio (CoS). El concepto de QoS es absoluto y define niveles de calidad. El concepto CoS proporciona niveles relativos de calidad dependiendo de la red utilizada.

DS (“Differentiated Services”) es un protocolo para especificar y controlar el tráfico de la red por “clase” tomando en cuenta de que existe cierto tipo de tráfico, por ejemplo; el tráfico de voz. El DS acerca dos parámetros: cualitativo y cuantitativo. El cualitativo especifica por ejemplo; prioridad relativa, mientras que el aspecto cuantitativo especifica por ejemplo, el ancho de banda. DS es el más avanzado método para manejar tráfico llamado Clase de Servicio.

DiffServ 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 mucho más dependientes del retardo y de la variación del mismo, como son las de video y voz interactiva, (González, 2002).

* * *

En éste capítulo se puede deducir que la industria de las comunicaciones se está desplazando hacia las redes que soportan cualquier tipo de aplicaciones, esta tendencia mejorará los servicios que recibe el usuario final y redundará en importantes aumentos en la productividad y una reducción en el costo de los negocios, además proporcionará más y mejores herramientas de administración de redes.

Un factor clave en el uso de estas tecnologías emergentes es un concepto llamado ancho de banda por demanda. El término significa que un usuario pueda solicitar y recibir ancho de banda dinámicamente.

Ahora, se requiere una unión entre redes de datos y voz, combinarlas de manera eficiente para aliviar y/o resolver los problemas en las redes actuales. Estas aplicaciones, incrementarán el desempeño de los usuarios y lo más importante es llevar al negocio a una eficiencia en relación a sus costos.

Los sistemas de administración son un aspecto clave para aprovechar plenamente las ventajas de las redes actuales, por otra parte cada vez más grandes y complejas. El ideal de la administración de sistemas es la administración integrada, es decir, controlar todos los recursos con independencia de su origen o tipo, lo cual permitiría un acceso completo a entornos multifabricante y con una administración flexible.

En el siguiente capítulo se presenta el proyecto de aplicación como parte de una posible solución a algunos de los problemas que presentan las redes en la actualidad.

CAPÍTULO 6:

ANÁLISIS E IMPLEMENTACIÓN DE UNA RED ACTUAL

VI.1 Introducción

Día a día, se hace mas evidente el crecimiento de las redes. En el caso de Internet el numero de usuarios que se conecta se incrementa de una manera asombrosa, ahora este no es el mayor reto que tiene que enfrentar la Internet actual. Además de los usuarios que a ella se conectan, existen también las distintas aplicaciones que en ella se ejecutan, por ejemplo, las aplicaciones que se corren en entornos corporativos (videoconferencia, VoIP, etcétera) que requieren de un tratamiento más especial que las aplicaciones que corre un usuario común desde su casa. La Internet no llega a satisfacer todos los requisitos de los usuarios, principalmente los que necesitan la red para el soporte de aplicaciones criticas.

Una carencia fundamental de la Internet es la imposibilidad de seleccionar diferentes niveles de servicio para los distintos tipos de aplicaciones de usuario. La arquitectura de Conmutación por Etiquetas Multiprotocolo (MPLS), es la base para la inclusión en la red de nuevas aplicaciones y para poder ofrecer diferentes niveles de servicio, en un entorno de mayor fiabilidad y con las garantías necesarias.

MPLS se puede presentar como un sustituto de la arquitectura IP sobre ATM. Los problemas que presentan las soluciones actuales de IP sobre ATM, tales como la complejidad de administración de dos redes separadas y tecnológicamente diferentes, quedan resueltos con MPLS. La tecnología MPLS integra IP y ATM y además proporciona soluciones para incrementar la velocidad y la prioridad de tráfico en el cable de la red.

VI.2 Descripción de la red

La red que sustenta el presente trabajo de tesis es una red de telecomunicaciones capaz de transmitir voz, datos y video entre dependencias universitarias, con el fin de recibir y transmitir datos prioritarios entre las diferentes sedes ubicadas en diferentes estados de la república mexicana.

Es un sistema de comunicación, que da servicio a investigadores, profesores, alumnos y empleados universitarios, a través de los equipos con los que cuenta cada institución. En esta red se planeó unificar las redes de voz, datos y video en una sola, utilizando la tecnología ATM como enlace principal.

Esta infraestructura permite brindar múltiples servicios de comunicación local y administración de información a todas las dependencias, además de permitir su presencia en Internet.

VI.2.1 Topología de la red

Es una red de transporte de banda ancha de topología variable [Figura 6.1] en función de las necesidades y enlaces disponibles tomando en cuenta los servicios que debe soportar (voz, datos y video).

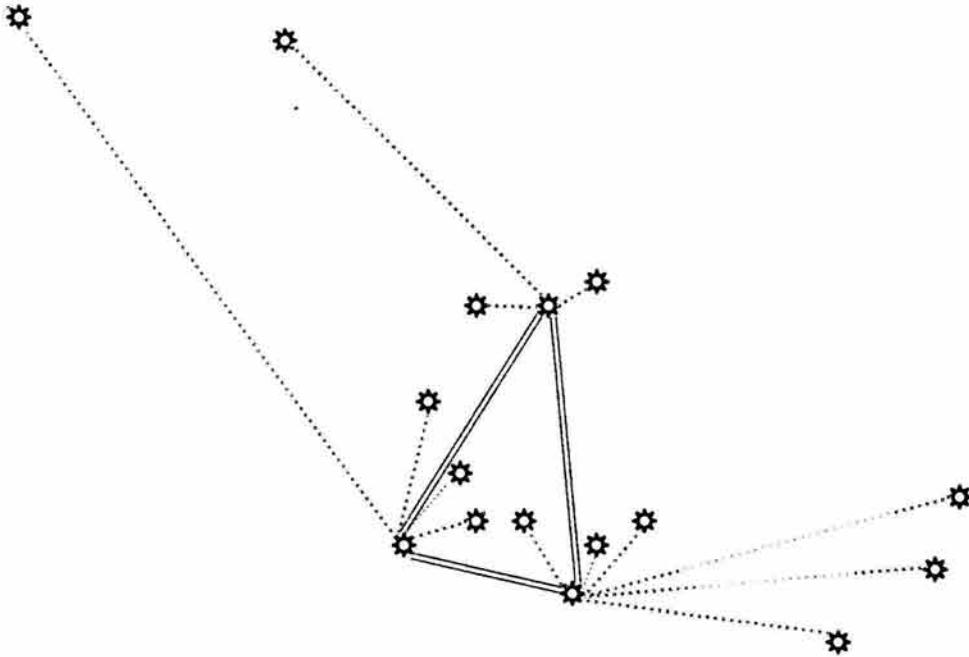


Figura 6.1 Topología física de la red.

La red tiene la siguiente estructura:

La red está integrada por 16 sedes de las que tres envuelven la mayor carga de tráfico de voz, datos y video, por lo que se han englobado en una red dorsal “backbone”.

Mientras que las 13 sedes restantes que se encuentran dispersas por la República Mexicana, se han agrupado en tres zonas por motivos de proximidad geográfica, volumen de tráfico y necesidad de intercambio de información, para unirse a los tres nodos principales, tal y como se observa en la [Figura 6.2], donde se muestra el diseño lógico de la red.

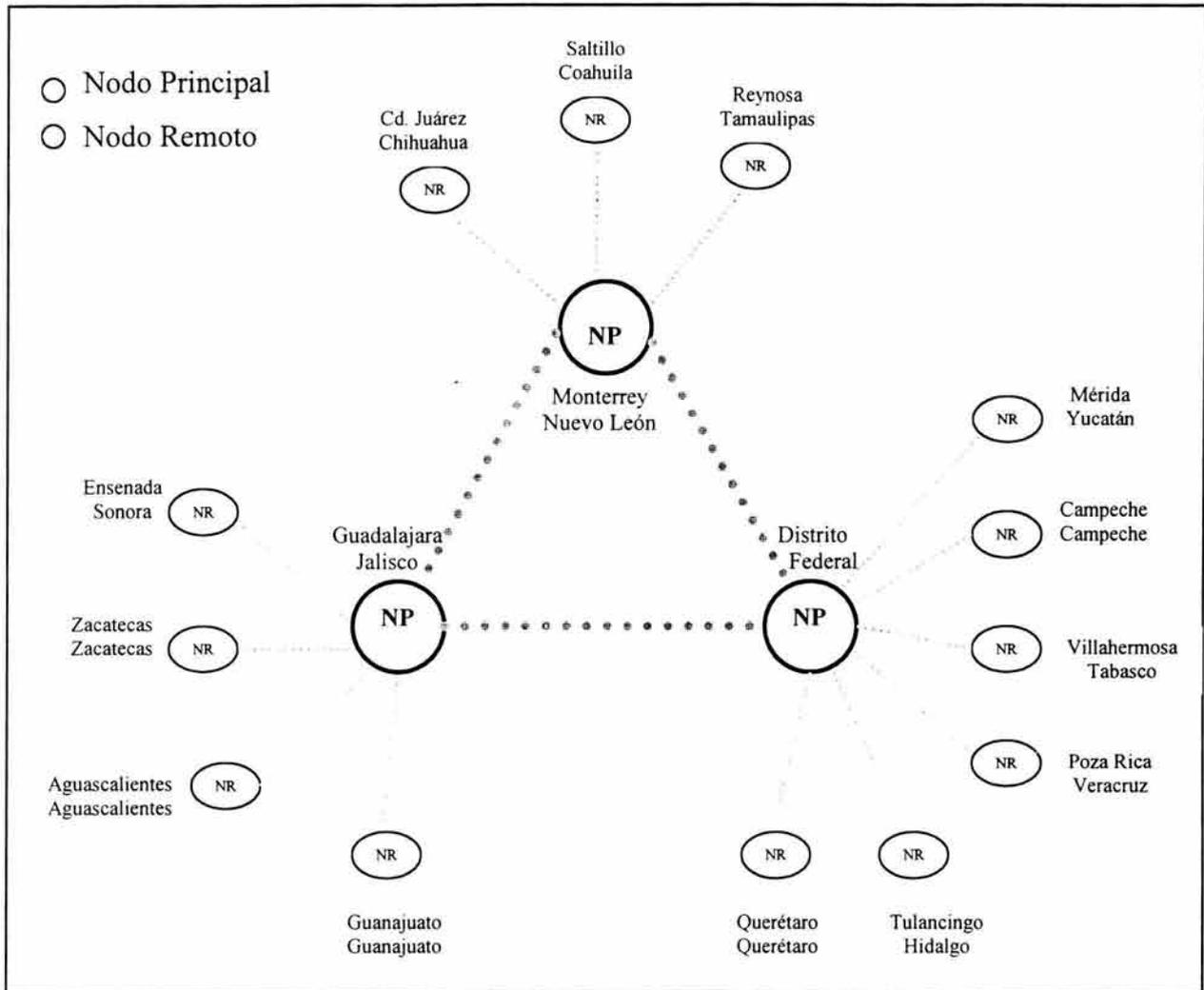


Figura 6.2 Diseño lógico de la red.

VI.2.2 Servicios que proporciona la red

Los servicios de la red están basados en necesidades académicas y laborales, permite la incorporación de servicios de banda ancha orientados a mejorar el desempeño académico, y la investigación con el fin de modernizar los actuales métodos de enseñanza, dentro de los servicios que se proporcionan se tiene lo siguiente:

- **Video:** Se utiliza para la videoconferencia en la educación a distancia, tanto para reuniones de grupo, como para clases de teoría, permitiendo el rápido acceso a cursos en línea y bases de datos multimedia.
- **Voz:** Se utiliza en la comunicación telefónica y en el envío de fax, el principal objetivo del área de telefonía es implantar un sistema de comunicación eficiente entre todas las unidades académicas y dependencias que conforman cada institución.

- **Datos:** Se utiliza para el acceso e intercambio de información pública generada por cada sede, se ofrece la consulta de bases de datos remotas, la transferencia de documentos, además de los servicios tradicionales de Internet como el correo electrónico.

VI.3 Análisis y diseño de la red

La red en general se divide en campus universitarios ubicados en diferentes regiones geográficas, y cada campus se divide en varios edificios que están integrados en la red. Se busca una solución de red interna de cada edificio para interconectarlo con los edificios restantes que integran el campus. Además del cableado interno de cada edificio, es necesario el diseño de una red troncal, que ofrezca una solución para interconectar los campus entre sí y con los nodos principales integrando una Red de Área Amplia (WAN).

Para simplificar el entendimiento de la red, se ha propuesto el análisis y diseño comenzando con el esquema típico que se tiene en cada uno de los edificios que integran cada Red de Área Local. Posteriormente, se integrarán las diferentes redes LAN para conformar la Red de Área Amplia mostrada en la [Figura 6.1].

VI.3.1 Red de Área Local

El siguiente diseño tiene como objetivo ejemplificar el esquema general de la red que se tiene en cada uno de los edificios que integran cada sede universitaria. Sin embargo, no todas las sedes tienen las mismas necesidades de comunicación y/o uso de aplicaciones, ni las mismas condiciones de acceso.

Se ha tomado como referencia un campus universitario que está integrado por las siguientes Facultades: Ingeniería, Medicina, Ciencias y Derecho, el siguiente diseño está basado en la Facultad de Ingeniería [Figura 6.3] por ser el nodo central de la red en el campus:

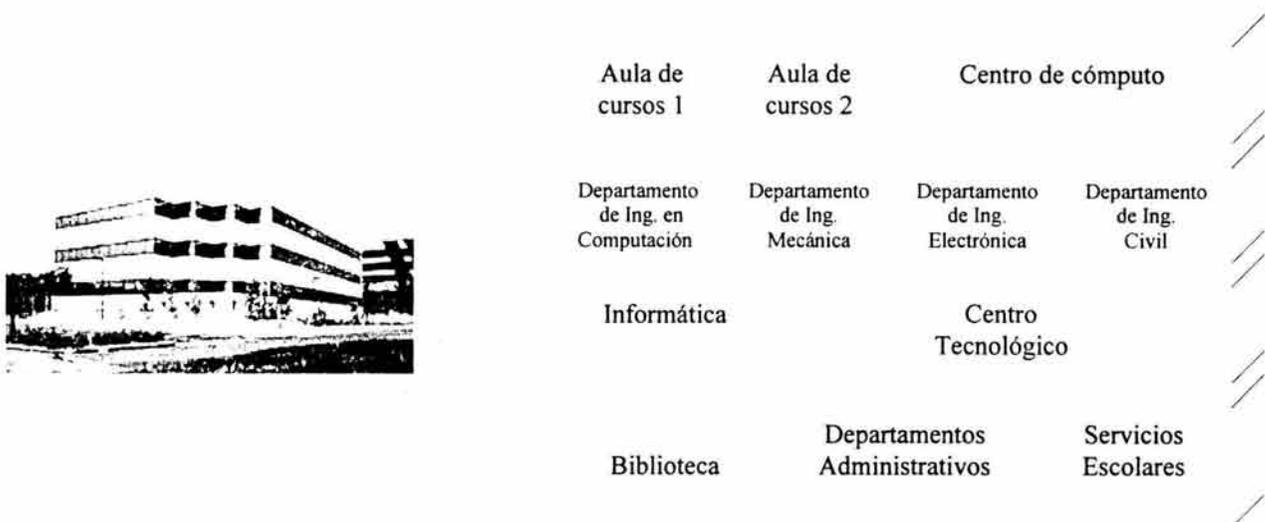


Figura 6.3 Diseño físico de la Facultad de Ingeniería.

VI.3.1.1 Análisis de la red

La red está subdividida lógicamente en tres grupos de terminales conformando subredes [Figura 6.4]. A cada departamento o área se le asigna una subred, los equipos para interconectividad destinados a las subredes correspondientes a cada departamento, están concentrados en tres sitios (gabinetes de telecomunicaciones o “racks”), distribuidos según la ubicación física de los grupos de terminales y cantidad de usuarios por cada sector, como se muestra a continuación:

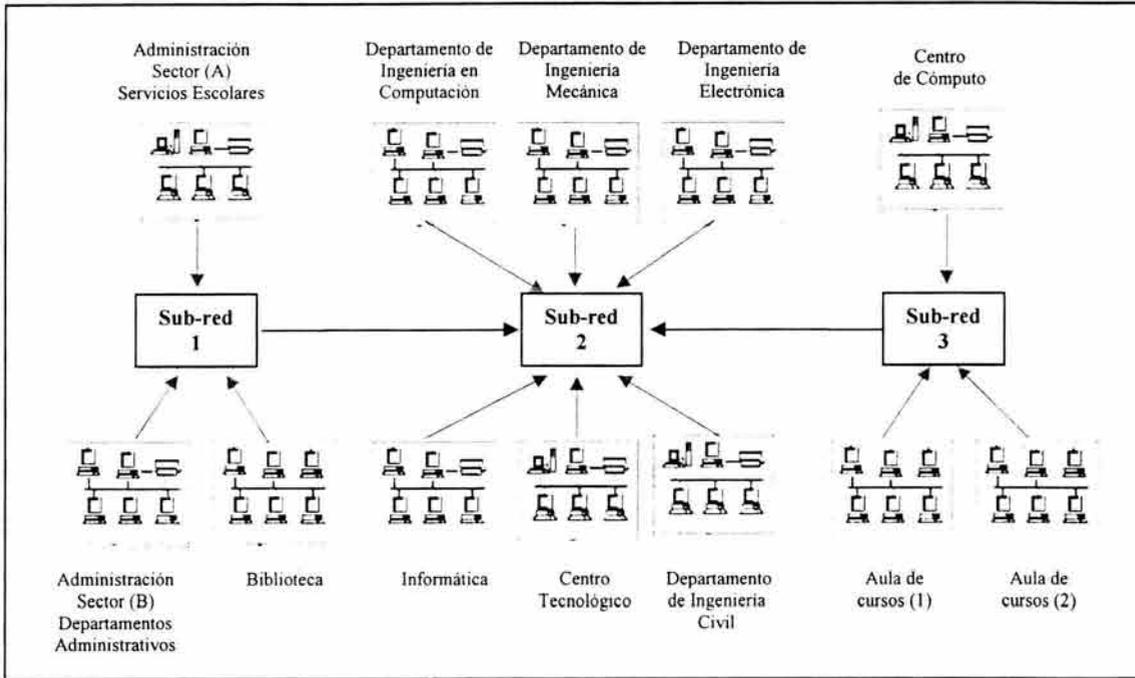


Figura 6.4 Distribución de la red.

Para esta asignación, se tomó en consideración el porcentaje de terminales que se concentrarían en cada segmento de red:

Número de usuarios por áreas		
1	Informática	6
2	Administración Servicios Escolares (Sector A)	30
3	Administración Departamentos Administrativos (Sector B)	30
4	Departamento de Ingeniería Mecánica	23
5	Departamento de Ingeniería Electrónica	23
6	Departamento de Ingeniería en Computación	27
7	Departamento de Ingeniería Civil	23
8	Centro de Cómputo	35
9	Biblioteca	16
10	Aula de cursos 1	16
11	Aula de cursos 2	16
12	Centro Tecnológico	16
Total de usuarios		261

Tabla 1: Usuarios por áreas.

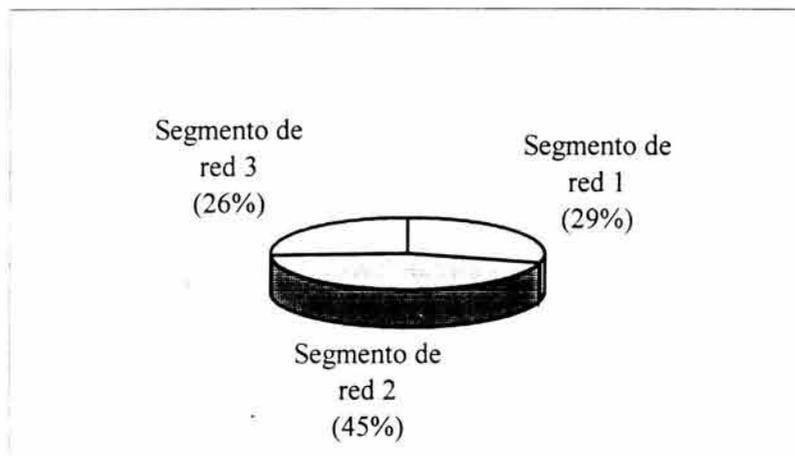


Figura 6.5 Distribución de usuarios.

VI.3.1.2 Descripción de las funciones de la red

Segmento de red 1	
Administración Sector (A) Servicios Escolares	Se instalaron 2 Impresoras, 28 ordenadores y un servidor en el cual reside información como: expedientes de alumnos, guía telefónica, catálogo de la biblioteca, etcétera. Se realizan consultas al servidor principal y accesos esporádicos a Internet. Cada puesto de trabajo dispone de comunicación telefónica.
Administración Sector (B) Departamentos Administrativos	Se instalaron 28 ordenadores y dos impresoras, se realizan consultas al servidor principal y al servidor de servicios escolares para obtener información de interés general relativa a la universidad, alumnos, académicos, empleados, etcétera. Cada puesto de trabajo dispone de comunicación telefónica.
Biblioteca	Se instalaron 16 ordenadores donde se realizan consultas al servidor principal y al servidor de servicios escolares. Se cuenta con cuatro extensiones telefónicas.
Segmento de red 2	
Ingeniería en Computación, Mecánica, Electrónica y Civil	Se instalaron 4 impresoras, 1 en cada departamento, 92 ordenadores, 22 en los departamentos de ingeniería mecánica, electrónica y civil; en el departamento de ingeniería en computación se instalaron 26 ordenadores, con acceso a Internet para consultas de correo electrónico, paquetes de "software" en el servidor del centro de cómputo, acceso y consulta a bases de datos científicas, acervo de tesis, audio, video y transferencias de archivos. Se cuenta con 16 extensiones telefónicas, (cuatro en cada departamento).
Informática	Se instalaron 6 ordenadores y el servidor principal que recibe consultas desde diversos departamentos así como desde sucursales remotas, reside información de toda la universidad. Cada puesto de trabajo cuenta con comunicación telefónica.

Centro tecnológico	Se instalaron 15 ordenadores y una impresora para apoyo informático a la investigación como: Acceso a los servicios de Internet, “software”, videoconferencia, cursos en línea y bases de datos multimedia. Tiene acceso al servidor principal. Cada puesto de trabajo cuenta con comunicación telefónica.
Segmento de red 3	
Centro de Cómputo	Se instalaron una impresora, 34 ordenadores, más un servidor local en donde residen distintos paquetes de “software” además de tener accesos frecuentes a Internet. Se cuenta con dos extensiones telefónicas.
Aula de cursos (1 y 2)	Se instalaron 32 ordenadores, 16 en cada aula donde se realizan trabajos que requieren de la ejecución de paquetes que residen en el servidor del centro de cómputo. Se cuenta con dos extensiones telefónicas (una extensión en cada aula).

Tabla 2: Funciones de la red por segmento.

VI.3.1.3 Diseño físico de la red

La red está basada en la tecnología para Redes de Área Local (LAN) conocida como Ethernet. Esta tecnología se basa en la técnica de Acceso Múltiple por Detección de Portadora con Detección de Colisiones (CSMA/CD). Básicamente, una estación de trabajo envía paquetes de datos cuando no hay otros circulando por la red. Si muchas estaciones transmiten al mismo tiempo ocurren colisiones. En este caso, cuando las estaciones que transmitieron y detectaron que hubo una colisión, cada una espera un tiempo aleatorio para repetir la transmisión; si vuelve a colisionar, nuevamente espera y transmite y así sucesivamente hasta que logre transmitir satisfactoriamente. A medida que el número de ordenadores aumenta, también lo hacen las colisiones.

Siguiendo las recomendaciones del cableado estructurado 10BaseT que estipula que el cable usado se llama UTP, utiliza una topología en estrella consistente en que cada nodo va de un cable a un concentrador (“hub”) que es el encargado de interconectarlos. Cada uno de estos cables no puede tener una longitud superior a 90 metros. El conector usado es similar al utilizado habitualmente en los teléfonos pero con 8 conectores (“pines”) y se le conoce con el nombre de RJ-45. Para las redes Ethernet se pueden utilizar cables de categoría 3 o 5. No obstante, si se utiliza el cable de la categoría 5, se podrá aumentar la red de Ethernet a Fast Ethernet en el futuro (ya que el cable de la categoría 3 no se puede utilizar para las redes Fast Ethernet). La red utiliza el protocolo TCP/IP, es el protocolo que predomina en las redes. Al tratarse del protocolo de Internet, los datos se pueden enviar a cualquier lugar del mundo. La red utiliza la tecnología Ethernet como medio de transporte.

Sin embargo, cuando el tráfico en la red se hace pesado y empiezan a ocurrir colisiones, se produce una disminución del tiempo de respuesta de la red.

Para solventar este problema se utiliza la tecnología LAN “switch”, la cual divide una red LAN en varios segmentos. Éstos limitan el tráfico a un segmento o segmentos a los cuales pertenece. A diferencia de muchos usuarios que comparten el ancho de banda en una LAN tradicional, cada usuario o grupo de usuarios tiene su propio segmento dedicado. LAN “switch” es una tecnología de segmentación que se utiliza en el manejo de un gran tráfico de información. La topología de LAN “switch” ofrece una conexión que proporciona anchos de banda dedicados con 10 Mbps ó 10BaseT usando CSMA/CD como método de acceso. Los LANs “switches” proporcionan anchos de banda dedicados para soportar múltiples conexiones simultáneas sin afectar el ancho de banda de cada usuario. El núcleo de la red lo constituyen “switches” 10/100. Estos elementos aseguran la capacidad de segmentación de las subredes, la optimización del ancho de banda disponible a 10 Mbps y un cableado troncal en Fast Ethernet a 100 Mbps. Estos elementos se unen físicamente por medio de un cable de fibra multimodo, (este tipo de fibra es usado típicamente para distancias cortas menores de un kilómetro). [Figura 6.6].

VI.3.1.4 Topología física de la red LAN

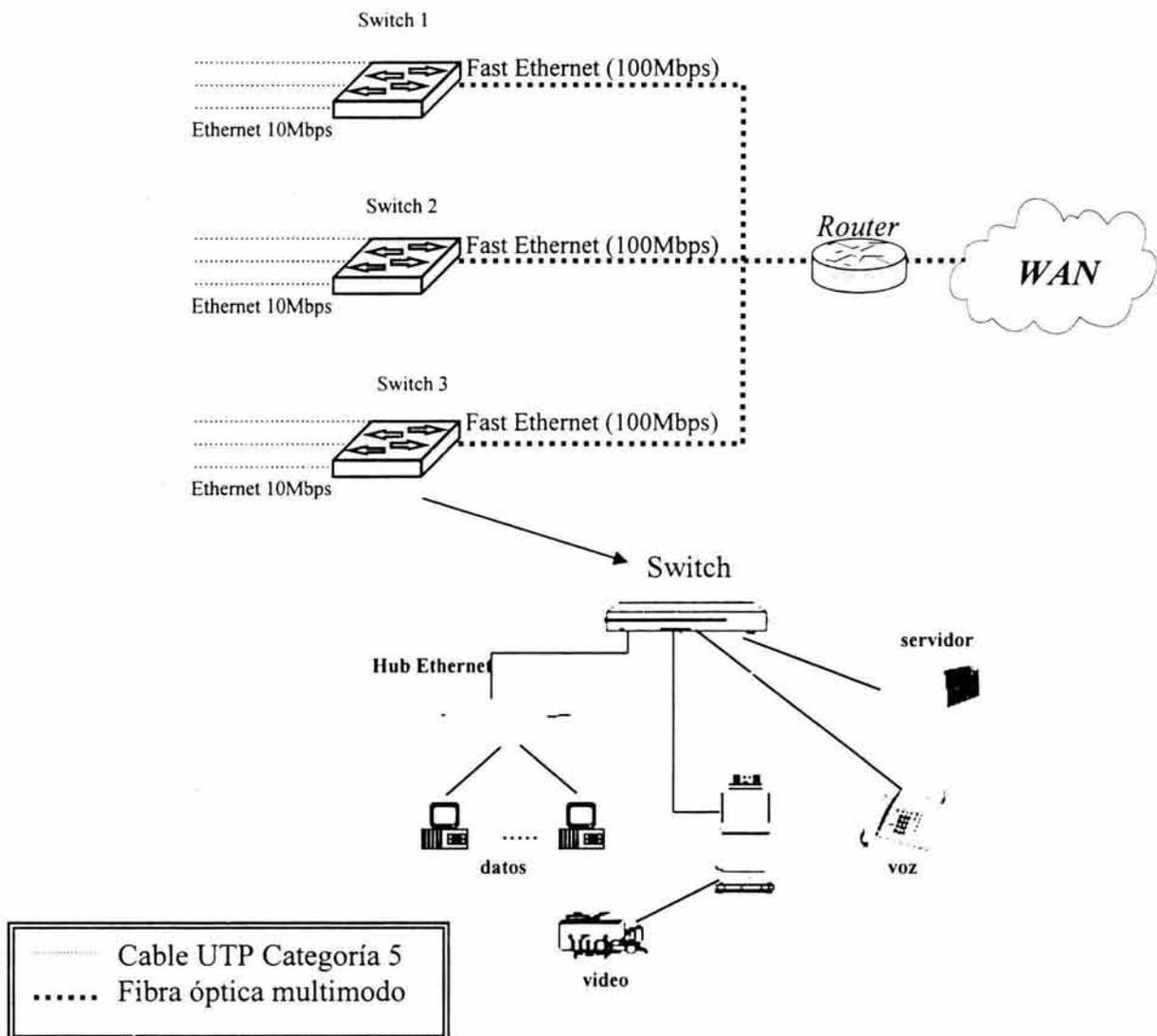


Figura 6.6 Topología de la red LAN.

La elección del medio de transmisión se realiza en función de la frecuencia de uso prevista y cantidad de tráfico generado (por ejemplo, una conexión para la que se prevé un uso esporádico con poca carga de tráfico, se conecta al puerto de menor categoría en el armario correspondiente). La conectividad Fast Ethernet se realiza en los enlaces principales para cada Red de Área Local porque se requiere un ancho de banda más grande para la transmisión de información entre subredes.

Estimación del tráfico en la Facultad de Ingeniería:

Nodo	Tecnología de Transporte	Velocidad Máxima	Tráfico promedio de entrada	Tráfico promedio de salida
Sudred 1	Fast Ethernet	100 Mbps	29.5 Mbps	32.5 Mbps
Subred 2	Fast Ethernet	100 Mbps	38.1 Mbps	47.2 Mbps
Subred 3	Fast Ethernet	100 Mbps	25.3 Mbps	31.0 Mbps

Tabla 3: Tráfico estimado en el nodo central.

La estimación del tráfico para esta red está basada en los tres “switches” que integran la red dorsal de la red LAN. Se debe tomar en cuenta que no todo el tráfico generado en cada uno de los segmentos de red sale por el “switch” correspondiente, debido a que parte del tráfico que se produce dentro del segmento de red es tráfico interno, propio de cada uno de los segmentos. De igual forma, no todo el tráfico generado en los tres “switches” llega al ruteador que comunica a la Facultad con las otras Facultades.

Como se puede apreciar el segmento de red número dos, es el que produce mayor tráfico de entrada, como de salida debido a que en este segmento se encuentran los servidores principales del campus, los cuales reciben consultas frecuentes generando la mayor carga de tráfico.

VI.3.1.5 Equipos de interconectividad en la red

Se utilizan concentradores (“hubs”) para el borde de la red en las áreas de trabajo y “switches” como elementos destinados al enlace con el cableado principal y la segmentación de las diferentes subredes y para la comunicación telefónica se utilizan teléfonos convencionales

El “backbone” de la red consiste en tres “switches”, a los que se conectan los “hubs” para grupos de usuarios, mientras que algunos puertos de los “switches” pueden ser utilizados directamente en estaciones que requieran un mayor ancho de banda como servidores de red.

La razón por la cual se utilizan estos equipos es la siguiente:

“Hubs”: Son simples dispositivos repetidores destinados a interconectar grupos de usuarios. Este dispositivo reenvía los paquetes de datos que recibe desde una estación de trabajo (documentos de texto, “e-mail”, gráficos, peticiones para impresión, etcétera) a los restantes puertos del dispositivo. Por lo tanto, todos los usuarios conectados al “hub” están en el mismo segmento de colisión compartiendo el ancho de banda disponible. Es por eso que conectar más estaciones de trabajo al mismo segmento provoca una disminución del rendimiento de la red e inclusive, se puede colapsar en los horarios de mayor demanda (uso).

“Switch”: Reenvía los paquetes de datos solamente al puerto o receptor destino basado en la información de la cabecera de cada paquete. Para realizar esta operación, el “switch” establece conexiones temporales entre la fuente y el destino, aislando las transmisiones de los restantes puertos y finaliza cuando concluye este proceso de “conversación”. Estos dispositivos soportan “conversaciones” múltiples y poseen la capacidad de mover mayor tráfico a través de la red. Literalmente, cada puerto de un “switch” puede ser asociado a un segmento de colisión independiente. El “switch” separa segmentos (o dominios) de colisión.

“Router”: El objetivo de colocar “routers” es subdividir las redes en grupos más pequeños (subredes) o bien vincular redes con topologías diferentes.

Las funciones primarias de un ruteador son: Segmentar la red, suministrar un envío inteligente de paquetes y soportar rutas redundantes en la red. Aislar el tráfico de la red ayuda a diagnosticar problemas, puesto que cada puerto del ruteador es una subred separada.

La inteligencia de un ruteador permite seleccionar la mejor ruta, basándose sobre diversos factores. Estos factores pueden incluir la cuenta de saltos, velocidad de la línea, costo de transmisión, retraso y condiciones de tráfico.

VI.3.2 Red del Campus

El siguiente diseño tiene como objetivo ejemplificar el esquema típico de la red que se tiene en cada uno de los campus que integran la red. Sin embargo, no todos los campus tienen las mismas necesidades de comunicación, uso de aplicaciones, ni las mismas condiciones de acceso.

VI.3.2.1 Descripción de la red

Los servicios se encuentran distribuidos en cuatro sedes (Facultades) dentro del campus, la red debe soportar todas las comunicaciones entre los edificios del campus, dando servicios tanto a las necesidades actuales como a las que puedan surgir en el futuro.

Los servicios de acceso se centralizan en la Facultad de Ingeniería, desde este edificio se da acceso a Internet y al servicio telefónico a los tres edificios restantes utilizando la tecnología Frame Relay.

Cuatro edificios (Facultades) constituyen el “backbone” de la red del campus, cada edificio universitario dispone de una red, se trata de una estructura en la que las estaciones de trabajo se conectan, mediante Ethernet a 10 Mbps a “switches” que a su vez, están conectados por Fast Ethernet a 100 Mbps a un “router”, los “routers” (uno en cada edificio) se enlazan entre sí con el servidor de ruteo principal el cual entre otras cosas es el “router” de salida del campus a la red.

Como las redes locales generan flujos esporádicos, el consumo de ancho de banda debe adaptarse a sus necesidades particulares. Frame Relay ajusta el ancho de banda a las aplicaciones con pequeños tiempos de tránsito al adaptarse a las necesidades de transmisión, se adecua al tráfico intermitente o en ráfagas de las LAN, que requiere la disponibilidad de un gran ancho de banda en un instante dado, además permite al usuario pagar sólo por la velocidad media contratada y no sobre el tráfico cursado.

Uno de los componentes clave del transporte de Voz sobre Frame Relay (VoFR) es el Dispositivo de Acceso a Frame Relay (FRAD) [Figura 6.7], el cual soporta múltiples canales de voz y datos sobre una conexión Frame Relay, este dispositivo amplía servicios del conmutador (PBX) a las sucursales y elimina la utilización de líneas arrendadas costosas (por ejemplo, DS0, E1, etcétera).

El FRAD envuelve (encapsula) todo el tráfico en tramas Frame Relay para hacer posible su transmisión a través de la red. Voz y datos se mantienen en tramas distintas. En el caso de la voz, previamente se digitaliza si el dispositivo conectado es analógico, y a continuación se comprime.

Además, dispone de la facilidad de supresión de silencios, que consiste en transmitir sólo cuando el usuario habla. Mientras un usuario permanece en silencio escuchando a su interlocutor no se transmite nada a través de la red, pero si se genera un ruido confortable en el extremo distante para evitar que el interlocutor remoto tenga la sensación de que se ha cortado la comunicación.

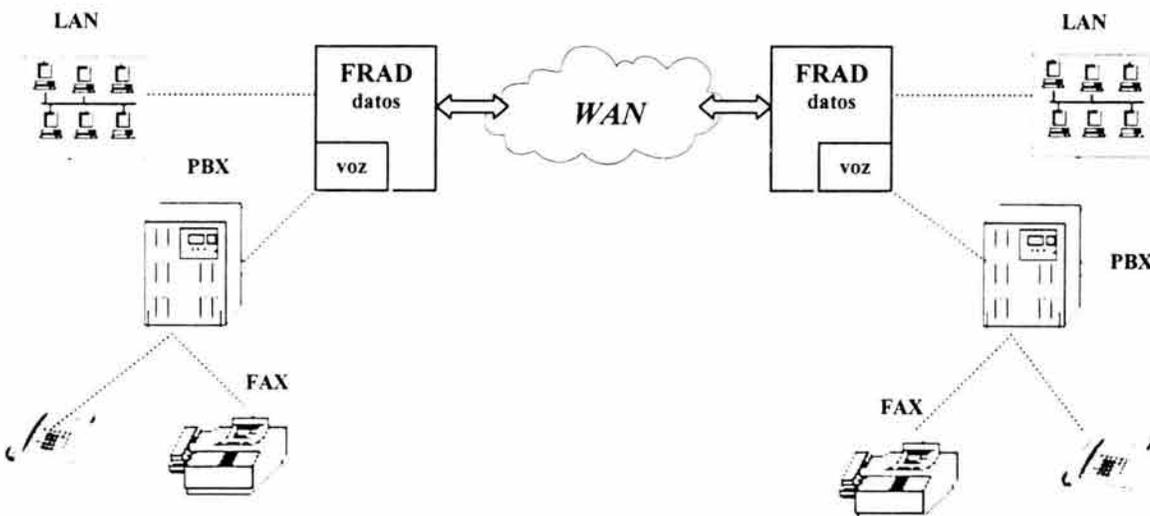


Figura 6.7 Funcionamiento del FRAD.

Por la línea de acceso a la red, viajan las tramas Frame Relay de voz y datos. La calidad de la voz depende de varios factores, como: algoritmos de compresión, tecnología utilizada, ancho de banda, etcétera.

Todo el ancho de banda está a disposición de quién lo necesite. Por ejemplo, durante las horas de oficina en que normalmente son frecuentes las comunicaciones de telefonía, los datos dispondrán de la pequeña capacidad no usada por la voz. Sin embargo, durante la noche, período que es previsible que no hay llamadas telefónicas, todo el ancho de banda podrá ser usado por los datos.

VI.3.2.2 Diseño de la red

La red está basada en Frame Relay sobre la tecnología de transporte PDH con un enlace digital E1 con múltiples ramificaciones de tipo Ethernet que se conectan al mismo. La topología concreta de la red se muestra en la [Figura 6.8].

El nodo central (Facultad de Ingeniería) cuenta con servidores principales de datos, éstos reciben consultas desde todos los departamentos, así como también desde las sedes remotas. Debido a que estos servidores poseen datos compartidos que son utilizados por todo el campus, se planteó la ubicación de los mismos en el “backbone”. El acceso a los datos se protege mediante un “firewall”.

En el ruteador que se utiliza para la conexión al exterior del campus, se implementan los filtros que se consideran convenientes para restringir o controlar los accesos hacia o desde el exterior por razones de seguridad; para esto se utiliza un muro de fuego (“firewall”) que permite definir reglas para el descarte de información que cumpla o que no cumpla con determinadas condiciones, ya que realiza un análisis de la información que entra a la red.

La red de voz que conecta al campus a la red pública de teléfonos (RTPC o PSTN por sus siglas en Inglés) es través de líneas de tipo E1 (2.048 Mbps). Para este diseño se ha adquirido una central telefónica (PBX) situada en el nodo central y se conecta con las otras facultades mediante interfases FXO¹ provenientes del PBX.

El FRAD es un equipo capaz de combinar tráfico de voz y de datos y enviarlo por un mismo enlace. En este caso, el FRAD dispone de interfases FXS² para la conexión de teléfonos convencionales en cada uno de los puestos de trabajo que requieran de comunicación telefónica.

¹ Foreign Exchange Office: Interfase (líneas) de salida del PBX.

² Foreign Exchange Station: Esta interfase “simula” una línea telefónica, a la que se puede conectar un teléfono analógico.

VI.3.2.3 Topología física de la red

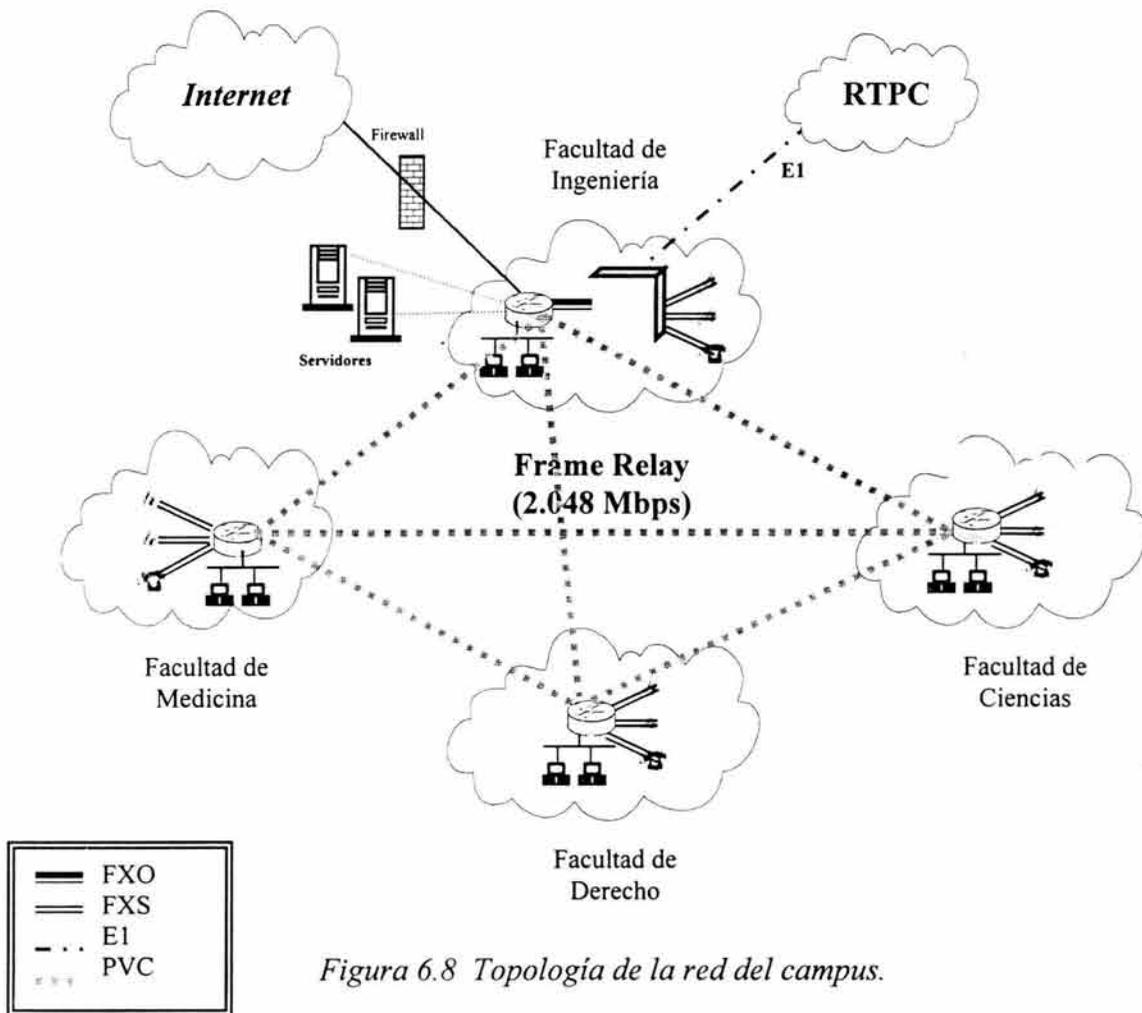


Figura 6.8 Topología de la red del campus.

Estimación del tráfico en el Campus:

Nodo	Tecnología de transporte	Velocidad Máxima	Tráfico promedio de entrada	Tráfico promedio de salida
Facultad de Ingeniería	PDH	2,048 Mbps	0.9 Mbps	1.3 Mbps
Facultad de Medicina	PDH	2,048 Mbps	0.7 Mbps	0.5 Mbps
Facultad de Derecho	PDH	2,048 Mbps	0.6 Mbps	0.7 Mbps
Facultad de Ciencias	PDH	2,048 Mbps	0.8 Mbps	0.5 Mbps

Tabla 4: Tráfico estimado en el campus.

La estimación del tráfico para esta red está basada en cada uno de los ruteadores que se encuentran en cada Facultad, los cuales son los responsables de establecer la comunicación entre Facultades, sin embargo no todo el tráfico generado por cada facultad está dirigido hacia el ruteador de salida del campus, el cual es el encargado de establecer la comunicación con el exterior.

Por ser el nodo principal, el que recibe más consultas y el que produce más información dirigida hacia el exterior del campus, la Facultad de Ingeniería es el nodo en el que se presenta mayor carga de tráfico en comparación con los nodos restantes.

VI.3.2.4 Especificaciones de Frame Relay

Un circuito virtual permanente (PVC): Consiste en un trayecto predefinido a través de la red Frame Relay que conecta dos puntos finales. El servicio Frame Relay proporciona PVC situados donde hayan especificado los clientes. Dicho circuito se mantiene establecido todo el tiempo, sin importar si existe o no, un flujo de datos. Un PVC es requerido para cada localidad del cliente conectada a un “puerto” de la red.

El tráfico de voz es muy sensible a los retardos, por lo que los circuitos virtuales de voz se configuran como prioritarios y sensibles al retardo. Por contra, el tráfico de datos no es tan sensible al retardo pero es mucho más impulsivo, es decir, requiere altas velocidades durante cortos intervalos de tiempo. Por esta razón, los circuitos virtuales de datos se configuran como no prioritarios y con maximización del caudal.

Puerto: Se refiere al dispositivo físico (tarjeta instalada en el “router” o “switch” Frame Relay) que forma parte de la infraestructura de la red Frame Relay y que se conecta a la línea de acceso y que funge como interfase entre el equipo de datos del usuario y la red.

Tasa de Información Comprometida (CIR): Es un parámetro de dimensión de red específico de Frame Relay que permite a cada usuario elegir una velocidad media garantizada en los dos sentidos de la comunicación para cada circuito virtual (PVC). Como no todos los PVC utilizan en un mismo momento dado su ancho de banda reservado, un determinado PVC puede emitir parte de su carga hacia los otros. En resumen, Frame Relay permite dividir estadísticamente el ancho de banda entre diferentes circuitos virtuales. Por ejemplo, gracias al CIR se puede optar por instalar una red basada en Frame Relay con velocidades de 32 ó 64 Kbps desde el nodo central hacia las sedes remotas y de 16 Kbps en el sentido inverso.

El CIR, que fija una velocidad se mide en bits por segundo y es independiente del transporte físico. La velocidad de envío y recepción de los datos puede ser mayor que la CIR, siempre que exista capacidad disponible en el puerto y en la troncal.

VI.3.3 Red WAN

Una WAN (Red de Área Amplia) interconecta las Redes de Área Local que se encuentran separadas por grandes distancias físicas. Las WAN llevan a cabo el intercambio de paquetes y tramas de datos entre los ruteadores y las LAN. Utilizan los servicios de proveedores de servicios de telecomunicaciones tales como Telmex o Avantel.

VI.3.3.1 Descripción de la red

En este caso la red WAN está integrada por 16 sedes, tres (Campus Distrito Federal, Campus Guadalajara y Campus Monterrey) engloban la red dorsal, se ha alquilado un enlace de transporte* SDH enlazando las sedes principales. La utilización de SDH permite la transmisión de cualquier tipo de información (voz, datos y vídeo) a la vez que facilita una alta velocidad en función de las necesidades que vayan surgiendo.

La Jerarquía Digital Síncrona (SDH) proporciona una solución a largo plazo por estandarizar los accesos a redes entre diferentes fabricantes. En lo que respecta a la disponibilidad, los enlaces de las redes basadas en SDH son altamente seguros. Debido a que su topología es de anillo, existen enlaces redundantes que en caso de que una fibra se corte, la ruta de transmisión seguirá funcionando con el enlace de respaldo y la comunicación será restaurada nuevamente.

Las trece sedes restantes se enlazan a los nodos principales correspondientes mediante la tecnología de transmisión PDH que permite el intercambio de información entre diferentes localidades.

VI.3.3.2 Diseño de la red

La red permite brindar servicios de banda ancha a las universidades (campus), es una red ATM que se puede dividir en el "backbone" y "los accesos". La red dorsal dispone de tres campus que cuentan con "switches" ATM que están interconectados entre sí mediante tres enlaces STM-1 (155 Mbps).

ATM con STM-1 soporta una interfase de fibra óptica multimodo, esta interfase es un estándar y la soportan la mayor parte de los "switches" ATM del mercado; sin embargo, existe un convertidor a interfase de fibra monomodo si la red lo requiere. Una interfase WAN puede conectarse en un "switch" ATM, proporcionando la conectividad a los otros sitios de la corporación y a Internet. Los "switches" ATM aseguran que el tráfico de grandes volúmenes sea flexiblemente conmutado al destino correcto.

* Tecnología de "transporte" se refiere al uso de técnicas de conmutación y multiplexación en la capa de enlace (Capa 2 del Modelo OSI) para el traslado del tráfico del usuario final de la fuente al destino, dentro de una red.

Los accesos (ubicaciones más pequeñas, 13 en total) consisten en “routers”, interconectados con un enlace digital E3 (34,368 Mbps) vía fibra óptica al equipo de “backbone” correspondiente [Figura 6.9] para aplicaciones multimedia que necesitan un elevado caudal, estos “routers” deben contar con capacidades de configuración de parámetros ATM, este equipo reúne los datos emitidos por la aplicación del cliente y les da el formato de paquetes adecuados para la transmisión de la información sobre la red ATM.

Toda la red comparte el mismo esquema de funcionamiento, si bien cada campus dispone de sus propios servidores, los servidores de los campus actúan de forma conjunta manteniéndose coherentes, de manera que ante un fallo de uno de ellos el otro adopta las funciones del primero.

VI.3.3.3 Topología física de la red

La siguiente figura muestra la topología física de la red:

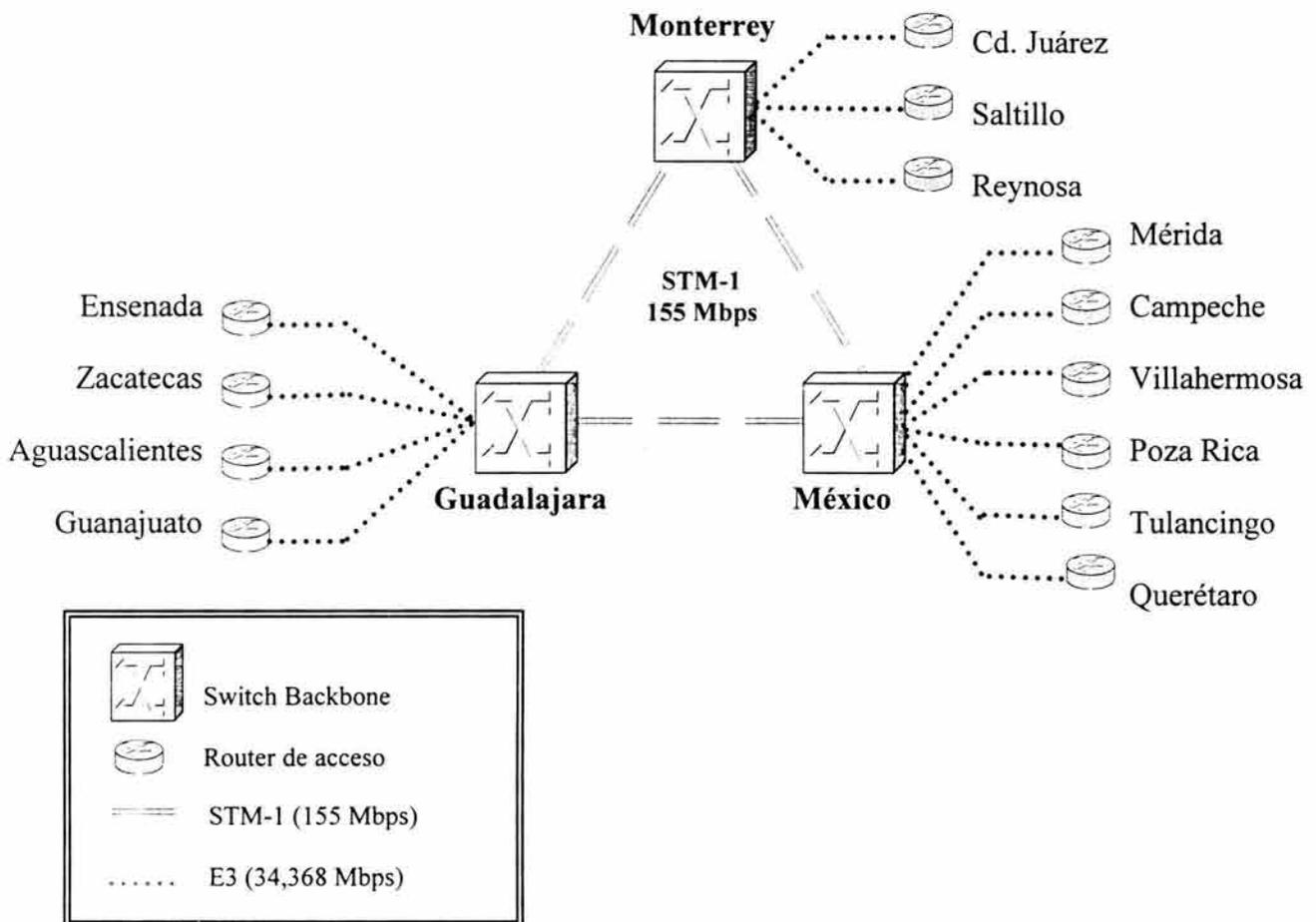


Figura 6.9 Topología física de la red WAN.

Para el intercambio de datos a través de la red ATM, en cada campus existe un ruteador conectado al “switch” ATM correspondiente, el cual permite la comunicación entre las diferentes subredes de cada campus y con el resto de los campus.

Estimación del tráfico en la red WAN:

Para estimar el tráfico, se considera el caso de las puertas de entrada de cada campus, es decir el ruteador que conecta la red del campus con el resto de Internet. Todo el tráfico que sale y entra a la red debe pasar por dicho ruteador.

Nodo	Tecnología de Transporte	Velocidad Máxima	Tráfico promedio de entrada	Tráfico promedio de salida
México D.F.	SDH	155.5 Mbps	84.9 Mbps	29.5 Mbps
Guadalajara	SDH	155.5 Mbps	97.3 Mbps	37.4 Mbps
Monterrey	SDH	155.5 Mbps	61.3 Mbps	59.3 Mbps
Cd. Juárez	PDH	34.368 Mbps	17.2 Mbps	5.8 Mbps
Saltillo	PDH	34.368 Mbps	22.5 Mbps	4.3 Mbps
Reynosa	PDH	34.368 Mbps	16.4 Mbps	1.6 Mbps
Ensenada	PDH	34.368 Mbps	21.7 Mbps	4.1 Mbps
Zacatecas	PDH	34.368 Mbps	19.6 Mbps	2.3 Mbps
Aguascalientes	PDH	34.368 Mbps	24.6 Mbps	5.2 Mbps
Guanajuato	PDH	34.368 Mbps	29.7 Mbps	3.7 Mbps
Mérida	PDH	34.368 Mbps	18.9 Mbps	5.4 Mbps
Campeche	PDH	34.368 Mbps	15.3 Mbps	9.7 Mbps
Villahermosa	PDH	34.368 Mbps	22.9 Mbps	2.7 Mbps
Poza Rica	PDH	34.368 Mbps	12.1 Mbps	3.4 Mbps
Tulancingo	PDH	34.368 Mbps	21.5 Mbps	4.2 Mbps
Querétaro	PDH	34.368 Mbps	27.0 Mbps	4.5 Mbps

Tabla 5: Tráfico estimado en la red.

Los nodos que integran el “backbone “ de la red WAN son los que presentan mayor carga de tráfico por ser los que reciben y transfieren información de y a todos los nodos restantes.

VI.3.3.4 Especificaciones de ATM

Una red ATM consiste en una serie de nodos interconectados punto a punto mediante enlaces ATM. Las redes ATM son fundamentalmente orientadas a conexión, en los que se designa la Conexión de un Circuito Virtual (VCC). ATM se caracteriza por el transporte de celdas de tamaño fijo de 53 bytes, de los cuales 5 son la cabecera y los otros 48 bytes son de datos.

Se diferencian dos tipos de circuitos virtuales:

1. Caminos Virtuales (VP, "Virtual Path").
2. Canales Virtuales (VC, "Virtual Channel").

Un camino virtual está compuesto por varios canales virtuales. Cada uno de ellos tiene asociado un identificador (VPI, "Virtual Path Identifier" y VCI, "Virtual Channel Identifier"), los cuales se usan para el transporte de cada celda a través de la conexión. Para transmitir de forma integrada voz y datos se usa un camino virtual, para el transporte de datos se usa un canal virtual y para transmitir voz se usa otro canal virtual.

Capa de adaptación ATM (AAL): Debido a que las celdas tienen un tamaño fijo, los datos deben ser fragmentados en bloques de 48 bytes, y una vez recibidos deben ser reensamblados. A este proceso se le denomina SAR y lo realizan los extremos del circuito ATM y no los elementos intermedios. Para realizar el SAR se necesitan capas de adaptación ATM (AAL, "ATM Adaptation Layer"). Algunas capas de adaptación bastante usadas son: AAL1 para transporte de telefonía, ó AAL5 para el transporte de paquetes de longitud variable, como puede ser el tráfico de una LAN.

Transporte de voz y datos en ATM: Una de las ventajas de usar ATM en el "backbone" es la habilidad de especificar qué cantidad de ancho de banda y qué Calidad de Servicio (QoS) se requiere a través de un enlace WAN. En vez de usar separadamente líneas alquiladas (por ejemplo, E1 y E3) para conectar múltiples destinos, un servicio ATM WAN a través una única interfase puede soportar requerimientos variables de ancho de banda para transportar datos y voz a múltiples destinos. Una única interfase ATM puede soportar múltiples circuitos virtuales, cada uno de ellos con diferentes anchos de banda y QoS.

STM-1 permite múltiples caminos virtuales a través de una única interfase, cada terminación puede incluir hasta 256 circuitos virtuales, cada uno usando diferentes anchos de banda o parámetros de QoS para transportar datos y voz.

ATM permite solucionar la integración de voz y datos, ya que permite la separación los circuitos virtuales dedicados al transporte de voz [Figura 6.10], es decir, se puede transportar servicios de voz y vídeo por un lado y datos por otro de manera eficiente.

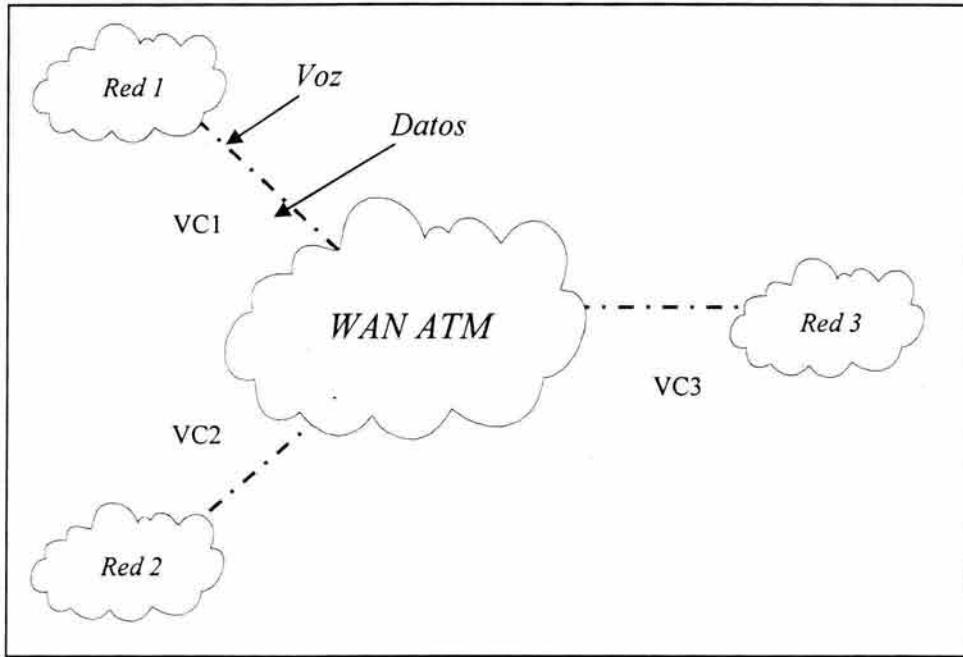


Figura 6.10 Separación de Circuitos Virtuales (VC).

ATM típicamente trabaja a velocidades de transmisión desde $N \times E1$ ($N=1$ como mínimo), E3 (34.368 Mbps), DS3 (44.736 Mbps), STM-1/OC-3 (155.52 Mbps), y eventualmente a nivel STM-4/OC-12 (662.08 Mbps) y STM-16/OC-48 (2,488.32 Mbps). También las celdas ATM pueden ser transportadas en módems de 9,600 bps.

La velocidad del puerto del "switch" ATM define la velocidad máxima a la cual el cliente puede transmitir y recibir datos hacia y desde la red ATM. El acceso a un puerto ATM es siempre, a través de una línea de acceso digital. El servicio ATM requiere que el cliente cuente con su CPE, el cual puede ser un "router" o "switch", en este caso en los nodos que integran el "backbone" es un "switch" y en las sedes remotas es un "router".

VI.3.3.5 Modo de operación de ATM

Una red ATM consiste en un conjunto de "switches" ATM interconectados punto a punto por enlaces o interfaces ATM. Los conmutadores ATM soportan 2 tipos principales de Interfaces: UNI y NNI.

Los nodos finales se comunican con un dispositivo ATM por medio de una interfase usuario a red (UNI) y los "switches" ATM se comunican entre sí con una interfase red a red (NNI), [Figura 6.11].

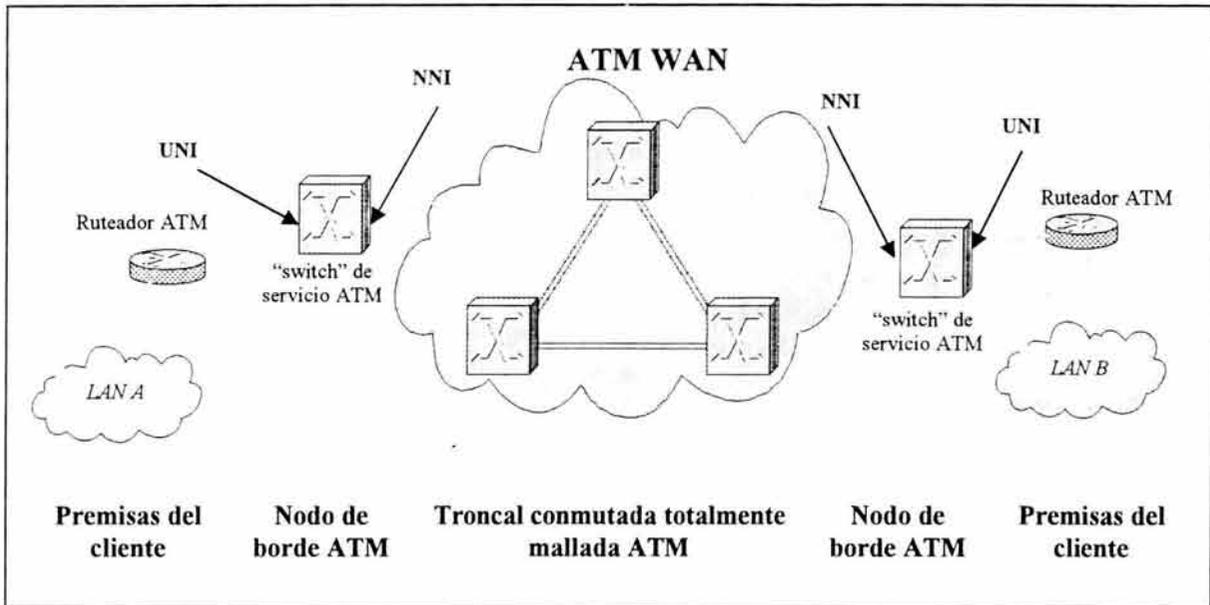


Figura 6.11 Operación de ATM.

Como cualquier otro tipo de red, ATM usa direcciones para cada punto de conexión. Para conectar un dispositivo a una red ATM, éste debe primero tener instalada una tarjeta de interfase de red ATM (NIC). Esas NIC son dispositivos de capa 2 y contienen circuitería ATM. La conexión física puede ser cobre UTP de categoría 5 (corriendo a 25 Mbps ó 155 Mbps), fibra óptica (con rangos de velocidad entre 155 Mbps y Terabits), o inalámbrico (10 Mbps o mayores). UNI especifica el establecimiento de conexión y la calidad de los requisitos de servicio para el tráfico entre la NIC y el "switch". Los "switches" ATM son los responsables de transmitir datos en una red ATM.

Las celdas ATM [Figura 6.12] son la unidad básica de datos que cruzan las UNI, y son fijas en longitud. El encabezado de la celda lleva la información necesaria para transportar una celda a través de una red ATM.

Celda ATM³

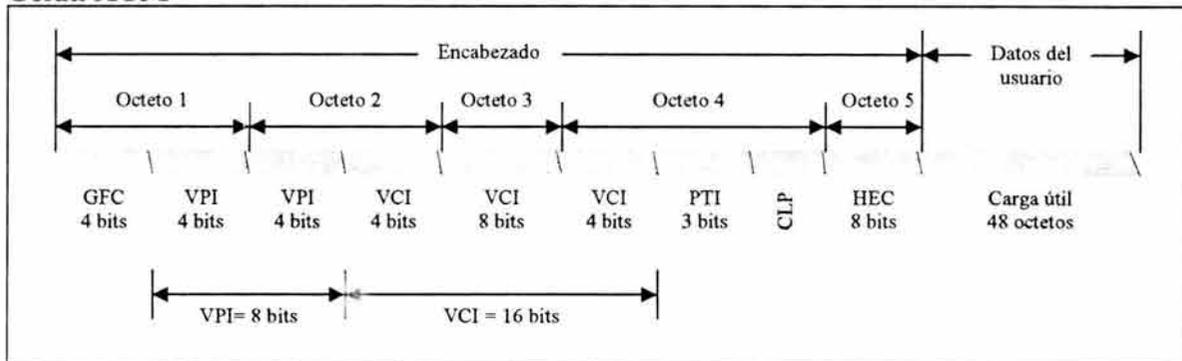


Figura 6.12 Estructura de una celda ATM.

³ Estructura y contenido de una celda ATM UNI. Una celda NNI es casi idéntica a la celda UNI. La única diferencia es que no hay necesidad del campo GFC. En la celda NNI, el GFC es incluido en el VPI, que consta en total de 12 bits en lugar de 8.

Control genérico de flujo (GFC): Controla el flujo de datos a través de la interfase usuario a red (UNI) permitiendo que múltiples dispositivos ATM sean unidos a la misma interfase de red. Los bits GFC son reasignados y se vuelven bits VPI en la interfase red a red (NNI), proporcionando así soporte adicional para más trayectorias virtuales.

Identificador de Trayecto Virtual (VPI): Parte de la dirección de red usada para identificar un agrupamiento de canales entre entidades de la red. Los primeros cuatro bits del VPI están en el primer octeto; los bits restantes están en el segundo octeto.

Identificador de Canal Virtual (VCI): Apuntador que identifica el canal virtual que el sistema está usando sobre una trayectoria particular. La combinación VPI/VCI forma el enlace de datos que corre entre dos nodos de red. El VCI tiene 16 bits de longitud y usa los segundos 4 bits del octeto 2, todos los 8 bits del octeto 3, y los primeros 4 bits del octeto 4.

Identificador Tipo de carga Útil (PTI): Indica el tipo de información contenida en la celda. Como las celdas son usadas para transportar diferentes tipos de información, varios tipos de indicadores del tipo de carga útil han sido definidos.

* Un 0 en el bit más significativo (000, 001, 010 y 011) denota que la celda llena información del usuario. Celdas con información del usuario con un bit intermedio de 1 (010 y 011) indica que la celda ha experimentado una congestión.

* Un 1 en el bit más significativo (100, 101, 110 y 11) denota que la celda lleva información de control o de administración de recursos.

100 y 101 representan mantenimiento y control de la red.

100 es para administración de recursos.

111 es reservado para definición futura.

Celda de Pérdida de Carga Útil (CPL): Especifica si debe descartarse o no la celda en presencia de congestión. Si se fija igual a 1, la red puede descartar la celda. Si se fija igual a 0, la celda podría no ser descartada.

Control de Error del encabezado (HEC): Proporciona corrección de error para errores de simples bits únicos y detección de error para errores de bits múltiples en la celda del encabezado.

Conexiones virtuales

Una conexión de canal virtual proporciona una conexión lógica entre una fuente y un destino. Un identificador de canal virtual (VCI), que está contenido dentro del encabezado de una celda se usa para identificar el canal.

Una conexión de trayectoria virtual (VPC) es semipermanente y proporciona una conexión lógica de enlaces virtuales que tienen los mismos puntos extremos. En otras palabras, un VPC lleva un grupo de canales virtuales, todos con los mismos puntos terminales.

Sobre cada enlace físico, una VPI especifica una trayectoria virtual y un VCI especifica un canal virtual particular. Pueden usarse trayectorias virtuales para establecer una topología de red lógica que sea independiente de la topología física.

Direccionamiento

Dos “switches” pueden ser interconectados mediante una VPC sin un enlace físico directo entre ellos. Un “switch” ATM recibe una llamada en un puerto de llegada. El “switch” examina el encabezado de la celda para identificar los valores contenidos en los campos VPI/VCI y luego consulta su tabla de traslación para determinar el puerto apropiado de salida con base a los valores VPI/VCI. Una vez identificado el puerto correcto, el “switch” trasmite la celda fuera del puerto.

Así en vez de llevar direcciones de fuente y destino como la hacen los paquetes TCP/IP, ATM se basa en los VPI/VCI contenidos dentro de un encabezado de la celda. Pueden agregarse trayectorias virtuales adicionales incrementado el tamaño del “switch”.

VI.3.3.6 Dispositivos ATM

Una red ATM se construye con conmutadores (“switches”) ATM y dispositivos (o puntos) finales ATM, [Figura 6.13]. Un conmutador ATM es responsable del tránsito de las celdas a través de la red: recibe la celda de un punto-final ATM o de otro conmutador ATM, entonces lee y actualiza la información del encabezado y rápidamente conmuta la celda de una interfase de salida hacia su destino.

Un punto final (o sistema final) ATM contiene una interfase de red. Ejemplos de estos dispositivos son: estaciones de trabajo (“workstations”), ruteadores (“ruters”), conmutadores (“switches”) LAN, entre otros.

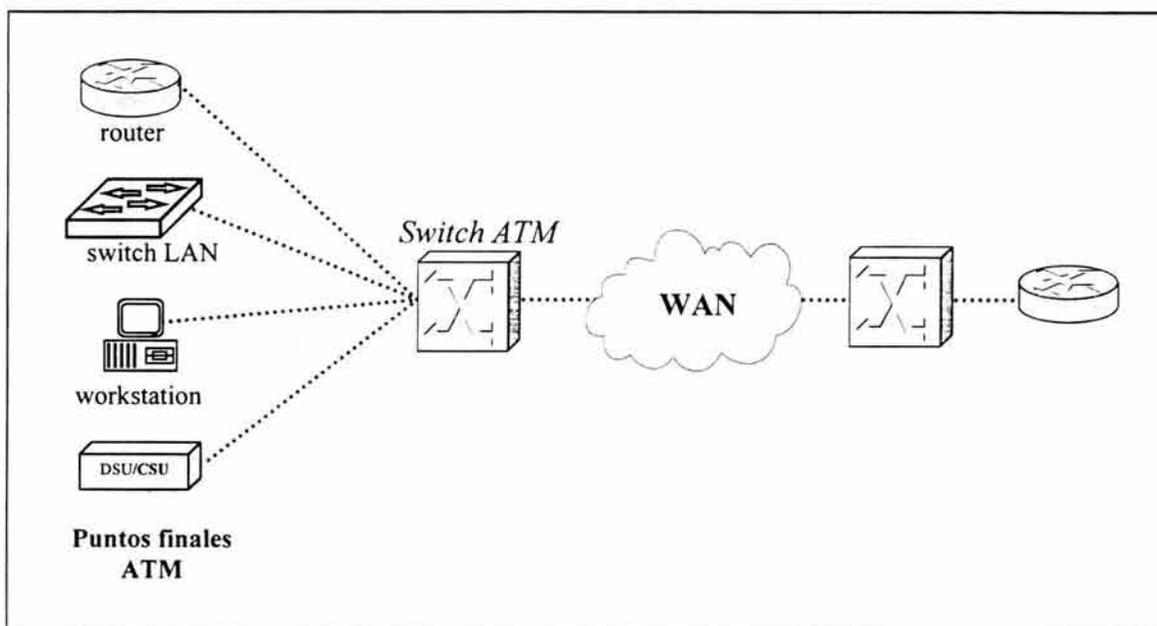


Figura 6.13 Dispositivos ATM.

VI.4 Implementación de MPLS

Actualmente, hay muchas opciones para ahorrar costos en el núcleo de una red ATM. Puede hacerse reduciendo el número de conexiones de larga distancia, o mediante una operación más eficiente que incorpore la tecnología óptica directamente usando técnicas como la Multiplexación en Longitud de Onda (DWDM). Sin embargo, MPLS es una solución con grandes posibilidades de éxito debido a la facilidad a la hora de implementar MPLS en una red actual (Fame Relay, ATM, Ethernet, etcétera).

En una red tradicional (por ejemplo, una red IP), un “router” conmuta los paquetes de una interfase de entrada a una interfase de salida; además, actualiza la información de enrutamiento. Para enviar los paquetes, debe examinar la cabecera del paquete IP para cada paquete. Estas dos funciones, envío y enrutamiento, tienen lugar en cada salto que realiza un paquete para atravesar la red.

Lo que se busca con MPLS es llevar las funciones de enrutamiento únicamente a los equipos exteriores del dominio MPLS, de tal forma que en el interior de dicho dominio no sea necesario realizar labores de enrutamiento, sino sólo de conmutación mediante la consulta de unas etiquetas añadidas a cada paquete en el momento de entrada al dominio, (González, 2002).

MPLS es un protocolo que soporta Clases de Servicio (CoS), cualidad que permite clasificar las aplicaciones y dar prioridad a aquellas que son de misión crítica y sensibles al tiempo (tales como vídeo o voz), sobre el tráfico que no es crítico en cuanto al tiempo, (correo electrónico o datos no prioritarios).

Así mismo, asigna a cada uno el ancho de banda que requiere, la forma de hacerlo es por su sistema de conmutación de etiquetas, lo que hace es poner un número, un “código postal”, que facilita la inmediatez en la administración de los paquetes de información. Esta característica permite, controlar los costos mediante la unificación de redes, sin necesidad de tener excedentes de ancho de banda.

Por otro lado, MPLS no requiere conexiones, sólo necesita un circuito de acceso en cada sede, en vez de enlaces preconfigurados o Circuitos Virtuales Permanentes (PVC), en este caso, la configuración la hace automáticamente la red.

Todo esto incrementa la flexibilidad del servicio porque se pueden añadir nuevas sedes rápida y fácilmente. Además, al suministrarlo como un servicio administrado, se reduce el costo y el tiempo empleado en la implementación y el mantenimiento.

VI.4.1 Conceptos fundamentales de MPLS

Ruteador de Conmutación de Etiquetas (LSR, "Label Switching Router"): Es un ruteador de alta velocidad especializado en el envío de paquetes etiquetados por MPLS. Participa en el establecimiento de los Trayectos Conmutados por Etiquetas (LSP). Los LSR, pueden ser internos o extremos (frontera), los primeros añaden o eliminan etiquetas, mientras que los segundos sustituyen unas etiquetas por otras.

Ruteador de Etiquetas Frontera (LER, "Label Edge Router"): Es un dispositivo que opera en la periferia de la red de acceso y la red MPLS, el cual se encarga de insertar las etiquetas en base a información de enrutamiento. Un LER soporta múltiples puertos conectados a redes distintas (como pueden ser ATM, Frame Relay y Ethernet) y envía este tráfico a través de la red MPLS después de haber establecido un LSP (camino) utilizando un protocolo de distribución de etiquetas. También, se encarga de retirar las etiquetas y distribuir el tráfico a las redes de salida.

Etiqueta: Es un identificador corto (de longitud fija) y con significado local, empleado para identificar una Clase Equivalente de Envío (FEC). Un paquete puede tener una o más etiquetas apiladas (jerarquía). Cuando un paquete atraviesa dominios interiores a otros dominios, es cuando se produce el apilamiento de etiquetas.

Clase Equivalente de Envío (FEC, "Forwarding Equivalent Class"): Es una agrupación de paquetes que comparten los mismos atributos (dirección destino, VPN, etcétera) y/o requieren el mismo servicio ("multicast", QoS, etcétera). Se asigna en el momento en que el paquete entra a la red. Todos los paquetes que forman parte de la clase, siguen un mismo LSP.

Uno de los motivos por los que se utiliza la FEC es porque permite agrupar paquetes en clases. Gracias a esta agrupación, el valor de la FEC en el paquete se puede utilizar para establecer prioridades, de tal forma que se da más prioridad a unos FEC sobre otros. Para establecer la relación entre una FEC y un paquete, MPLS usa la etiqueta. Dicha etiqueta identifica una FEC específica. Para diferentes clases de servicio se utilizan diferentes FEC.

Trayecto Conmutado por Etiquetas (LSP, "Label Switched Path"): Es una ruta a través de uno o más LSR que sigue un paquete de un FEC en particular. Este camino puede establecerse mediante protocolos de enrutamiento, así como manualmente.

Reenvío ("Forwarding"): Esta operación la realizan tanto conmutadores como ruteadores y consiste básicamente en encaminar un paquete recibido por la línea de entrada en base a unos campos que contiene el paquete.

Intercambio de etiquetas ("Label Swapping"): Cuando un LSR recibe un paquete extrae el valor de la etiqueta y accede con él a la tabla de encaminamiento. En dicha tabla de encaminamiento, [Tabla 6] encontrará el nuevo valor de la etiqueta que ha de ponerle al paquete antes de reenviarlo, así como la interfase de salida por donde ha de mandarlo.

Etiqueta de entrada	Puerto de entrada	Etiqueta de salida	Puerto de Salida
---------------------	-------------------	--------------------	------------------

Tabla 6: Tabla de encaminamiento.

El algoritmo de reenvío se suele implementar en “hardware” por su sencillez. Esto repercute favorablemente en el rendimiento del LSR.

La siguiente figura [Figura 6.14] muestra de forma gráfica algunos de estos términos:

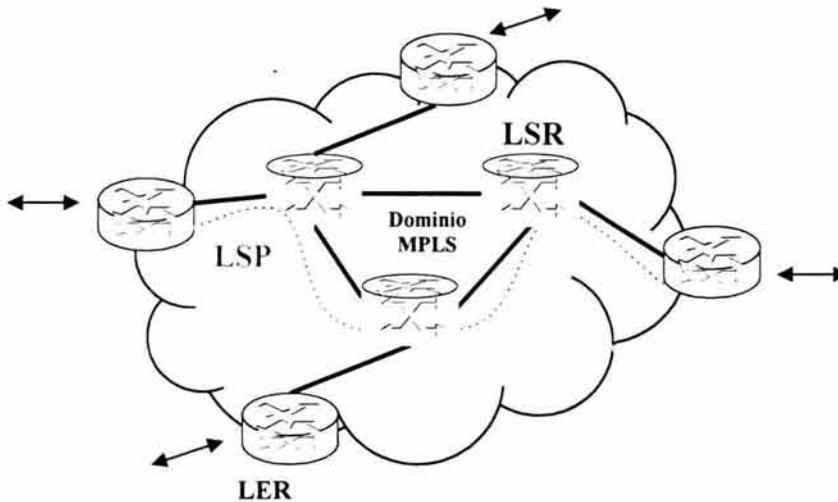


Figura 6.14 Componentes de MPLS.

VI.4.2 Beneficios de MPLS

MPLS utiliza eficazmente la separación de las funciones de control y reenvío en los ruteadores: Debido al crecimiento continuo de Internet, cada vez se exigen mayores prestaciones a los ruteadores, por lo que es necesario separar las funciones de control y reenvío de estos. Éste es uno de los aspectos más importantes de la conmutación de etiquetas (“Label Switching”). La ventaja fundamental de separar ambas funciones es la posibilidad de modificar una de ellas sin modificar la otra.

Precio/Rendimiento: MPLS permite conseguir la simplicidad del reenvío de las tecnologías de conmutación de la capa 2 (enlace de datos) manteniendo la flexibilidad y escalabilidad del encaminamiento de la capa 3 (capa de red). En general, un ruteador es un dispositivo de nivel 3 mientras que un conmutador es un dispositivo de nivel 2. Un conmutador es más simple que un ruteador y soporta un número más limitado de protocolos y características. El algoritmo de reenvío de un conmutador es mucho más simple que el de un ruteador.

El precio de un ruteador es mayor que el de un conmutador, pero éste suele ser más rápido. Esto es debido a que básicamente, lo único que hace un conmutador es reenviar

paquetes. Gracias a la conmutación de etiquetas se tienen dispositivos con características de precio/rendimiento de un conmutador, pero con la funcionalidad de un ruteador.

Un concepto básico de MPLS es convertir el equipo de capa 2 en la red (los “switches” ATM) en ATM-LSR, el cual puede ser visto como una combinación de un sistema de conmutación ATM y un “router” tradicional, compuesto por la unidad de control y la unidad de envío como se muestra en la figura siguiente [Figura 6.15]:

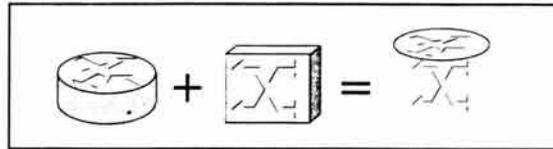


Figura 6.15 “Switch” con funcionalidad de “router”.

Integración de IP sobre ATM: La arquitectura ATM difiere significativamente de la arquitectura IP. La primera es una arquitectura orientada a conexión mientras que la segunda no lo es, es decir, es no orientada a conexión. Sin embargo, muchas partes de Internet de hoy día están construidas sobre conmutadores ATM rodeados de ruteadores relativamente lentos. Este tipo de redes se dice que usan el modelo superpuesto, esto es, una red IP superpuesta en una red ATM. La red ATM permite una conectividad de alta velocidad mientras que la red IP tendrá la inteligencia para reenviar datagramas IP. Aunque se tenga sólo una infraestructura física, se tienen dos redes separadas que funcionan de distinta forma y de distinta tecnología. Todos los esquemas que usan la conmutación de etiquetas no tienen en cuenta el modelo superpuesto, permitiendo que los protocolos de control IP corran directamente en “hardware” ATM. Por lo tanto, los conmutadores ATM se vuelven ruteadores IP.

Escalabilidad: Otro de los problemas del modelo superpuesto consiste en que se tiene una red completamente mallada: todos los ruteadores están conectados entre sí. Cada conmutador tendrá $N-1$ vecinos (siendo “N” el número total de conmutadores). Aumentando el número de ruteadores, llegará un momento en que la cantidad de información transmitida será tal que el rendimiento caerá exponencialmente. La solución al problema anterior se encuentra en la conmutación de etiquetas, los ruteadores están acoplados a los conmutadores por lo que se tienen menos vecinos y por tanto, una alta escalabilidad.

Velocidad y retardo: El reenvío (“forwarding”) tradicional basado en “software” es demasiado lento para manejar las grandes cantidades de tráfico de Internet o de las redes interconectadas. El tiempo de la búsqueda en las tablas de encaminamiento o ruteo, es demasiado elevado aún teniendo en cuenta métodos de aceleración de la búsqueda. Esto se traduce en pérdida de paquetes y conexiones, y por tanto en un bajo rendimiento. La conmutación de etiquetas es más rápida. El motivo es que el valor de la etiqueta que se pone en la cabecera de los paquetes es el que se usa para acceder a la tabla de encaminamiento del ruteador (es el índice para acceder a la tabla).

Esto requiere un solo acceso a la tabla (cómo se tiene el índice, se accede directamente). Por tanto, el tiempo para transmitir un paquete es menor que con el encaminamiento tradicional IP. Se reduce el retardo y el tiempo de respuesta.

Control de la ruta: En la mayoría de las redes interconectadas, el encaminamiento se realiza basándose en la dirección de destino IP. El encaminamiento basado en el destino no siempre es eficiente. La conmutación de etiquetas permite controlar las rutas llevando los paquetes a su destino encaminándolos por rutas distintas. Por lo tanto, la conmutación de etiquetas permite emplear nuevas funcionalidades de encaminamiento. Esto permite dar a distintas clases de tráfico distintos niveles de servicio. De esta forma, se usa MPLS para conseguir que la red se adapte a las necesidades de las clases de tráfico.

Otros beneficios de MPLS

En MPLS, la asignación de un paquete a una FEC se realiza cuando el paquete entra en la red asignándole a dicho paquete una etiqueta. En los siguientes saltos sólo se usará la etiqueta para determinar la interfase por donde reenviar el paquete, por lo que no será necesario analizar la cabecera del nivel de red. La etiqueta se usa como índice en la tabla de encaminamiento donde se obtiene el siguiente salto y la nueva etiqueta con la que sustituir la anterior. En MPLS, los conmutadores pueden realizar el reenvío, pero éstos no tienen necesidad de analizar las cabeceras del nivel de red. Las ventajas de basar el reenvío en las etiquetas en vez de en la cabecera del nivel de red son:

* Dado que un paquete se asigna a una FEC cuando entra en la red, el ruteador frontera que encapsula el paquete podrá usar toda la información que tenga sobre el paquete. Incluso información que no esté en la cabecera del nivel de red, por ejemplo podrá usar información del nivel de transporte, para asignar paquetes a la FEC. Por lo tanto, gran parte del trabajo se realiza antes de que el tráfico entre en la red. Con el encaminamiento convencional sólo se puede examinar la cabecera del nivel de red.

* Un paquete que entra en la red por un determinado ruteador puede etiquetarse de distinta forma que si hubiera entrado por otro. Por lo tanto, se pueden tomar decisiones dependientes del ruteador frontera que encapsula el paquete. Esto no se puede hacer en el encaminamiento convencional porque la identidad del ruteador frontera que introdujo el paquete en la red no viaja con el paquete.

* Se podría forzar a un paquete a seguir una ruta elegida antes o en el momento que el paquete entre en la red, en vez de elegirse por el algoritmo dinámico de encaminamiento a medida que el paquete fluye por la red. Esto podría hacerse para permitir la ingeniería de tráfico. En el encaminamiento convencional el paquete tendría que llevar la información de la ruta (encaminamiento fuente). En MPLS, se puede usar una etiqueta para representar la ruta, de tal forma que el paquete no tiene por qué llevar la información de la ruta.

Algunos ruteadores analizan la cabecera del nivel de red para determinar la clase de servicio a la que pertenece el paquete así como para determinar el siguiente salto.

MPLS permite, pero no impone, que la clase de servicio se derive total o parcialmente de la etiqueta. Así se puede decir que una etiqueta representa la combinación de una FEC y una clase de servicio. MPLS se llama así porque soporta cualquier protocolo de nivel de red así como cualquiera de nivel de enlace. Por lo tanto, MPLS puede o no, usar tecnologías subyacentes de “backbone” como ATM, Frame Relay, SDH y DWDM.

VI.4.3 Arquitectura de MPLS

VI.4.3.1 Tipos de nodos MPLS

Los LSR frontera son los encargados de etiquetar los paquetes que entran en la red. Para poder realizar este trabajo, estos LSR deben implementar el componente de control y el componente de reenvío tanto del encaminamiento convencional como de la conmutación de etiquetas. Si un paquete entra en la red, el ruteador frontera utilizará el componente de reenvío de la conmutación de etiquetas para determinar la etiqueta que se le pondrá al paquete. Si el siguiente salto no es un LSR y el paquete no tiene etiqueta, entonces el ruteador deberá reenviar el paquete usando el componente de reenvío del encaminamiento convencional. Cuando el paquete va a salir de la red MPLS, el LSR que recibe el paquete le quitará la etiqueta y lo reenviará al siguiente salto usando el componente de reenvío del encaminamiento convencional. Dicho LSR sabrá que el paquete quiere abandonar la red simplemente porque el siguiente salto no es un LSR.

Los tipos de nodos MPLS son, [Figura 6.16]:

LSR de entrada (“Ingress LSR”): LSR que recibe tráfico de usuario (por ejemplo datagramas IP) y lo clasifica en su correspondiente FEC. Genera una cabecera MPLS asignándole una etiqueta y encapsula el paquete junto a la cabecera MPLS obteniendo una Unidad de Datos del Protocolo MPLS (PDU, “Protocol Data Unit”).

LSR de salida (“Egress LSR”): LSR que realiza la operación inversa al de entrada, es decir, desencapsula el paquete removiendo la cabecera MPLS.

LSR intermedio o interior: LSR que realiza el intercambio de etiquetas examinando exclusivamente la cabecera MPLS (obteniendo la etiqueta para poder realizar la búsqueda en la tabla de encaminamiento).

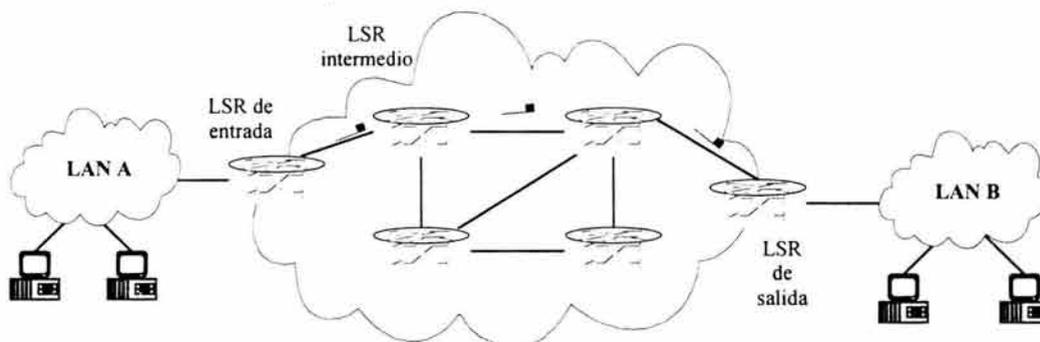


Figura 6.16 Nodos MPLS.

VI.4.3.2 Transporte de la etiqueta

ATM y Frame Relay (tecnologías del nivel de enlace) llevan la etiqueta en la cabecera del paquete. ATM puede llevar la etiqueta en el campo VCI o en el VPI de la cabecera [Figura 6.17], mientras que en Frame Relay estará en el campo del Identificador de la Conexión del Enlace de Datos (DLCI).

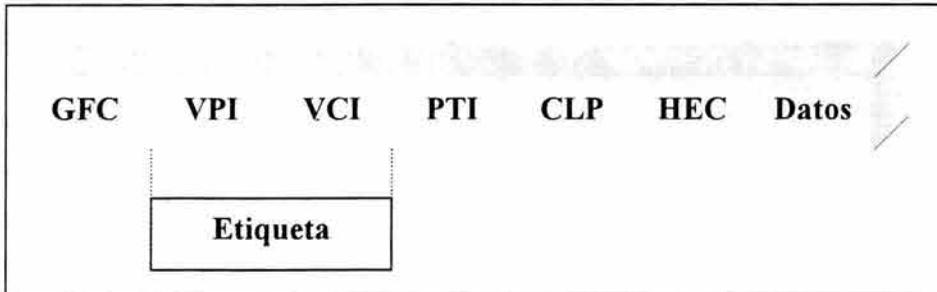


Figura 6.17 Celda ATM.

El hecho de llevar la etiqueta en el campo VCI de las células ATM permite que un conmutador ATM funcione como un LSR siempre que tenga el “software” de control apropiado. La cabecera de relleno está situada en una posición donde la mayoría de los ruteadores pueden procesarla por “software”, por lo que los ruteadores convencionales pueden convertirse en LSR siempre que tengan el “software” apropiado.

En tecnologías como Ethernet que no disponen de un campo para poder llevar la etiqueta en la cabecera del nivel de enlace, la etiqueta se transporta en un campo específico para la etiqueta, que se inserta entre la cabecera del nivel de enlace y la cabecera del nivel de red, [Figura 6.18]. Esta cabecera se denomina "cabecera shim" (cabecera de relleno). De este modo, se permite cualquier tecnología o combinación de tecnologías del nivel de enlace. Por ejemplo; conmutación de etiquetas en redes Ethernet, [Figura 6.19].

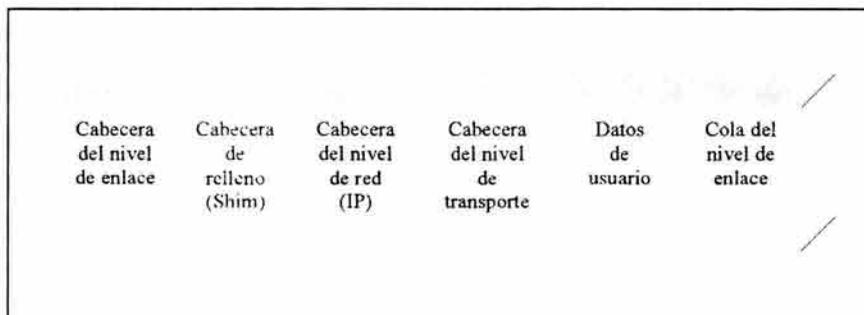


Figura 6.18 Encapsulado genérico MPLS.

Formato de las etiquetas: Una etiqueta MPLS tiene 32 bits.

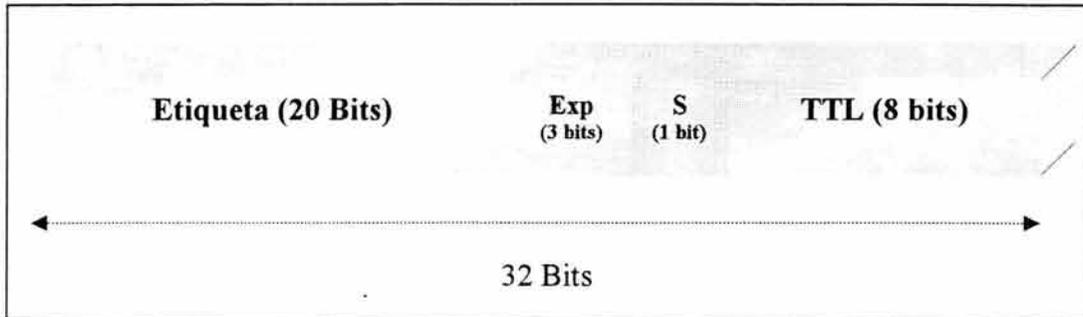


Figura 6.19 Etiqueta para redes sin campo de etiquetas.

- Etiqueta: Valor de la etiqueta.
- Exp: Uso experimental. No está definido totalmente.
- S: Bit de apilamiento (“Stacking bit”), se usa para apilar etiquetas.
- TTL: Tiempo de vida (“Time To Live”), número de nodos (saltos) que puede atravesar el paquete MPLS. Se necesita porque los LSR intermedios no analizan el campo IP TTL.

VI.4.3.3 Pila de etiquetas

En MPLS un paquete puede tener más de una etiqueta, organizadas éstas a modo de pila el primero que entra es el primero que sale (FIFO, “First Input, First Output”). A esto se le conoce como pila de etiquetas. Siempre que se procese una etiqueta, ésta será la de la cima, sin importar cuántas etiquetas pueda haber debajo. Se puede considerar un paquete no etiquetado como un paquete con una pila de etiquetas vacía.

Si la profundidad de la pila de etiquetas de un paquete es m , a la etiqueta que está al fondo de la pila se le llama etiqueta de nivel 1, a la que está encima etiqueta de nivel 2, y así sucesivamente.

VI.4.3.4 Protocolos de distribución de etiquetas

Un protocolo de distribución de etiquetas es un conjunto de procedimientos por los que un LSR le informa a otro de las asociaciones de etiquetas a FEC que ha hecho. A dos LSR que utilizan un protocolo de distribución de etiquetas para intercambiar información de asociaciones de etiquetas a FEC se les conoce como un par de distribución de etiquetas (“label distribution peers”) respecto a la información de las asociaciones que intercambian.

MPLS no asume que haya sólo un protocolo de distribución de etiquetas. De hecho, se están normalizando distintos protocolos de distribución de etiquetas. También se están definiendo nuevos protocolos como el LDP (“Label Distribution Protocol”).

VI.4.4 Funcionamiento de MPLS

El funcionamiento del protocolo MPLS se puede resumir en los siguientes pasos, [Figura 6.20]:

1. Creación y distribución de etiquetas.
2. Creación de tablas en cada ruteador.
3. Creación de los Trayectos Conmutados por Etiquetas (LSP).
4. Agregar etiquetas a los paquetes con la información de la tabla.
5. Envío del paquete.

La base del MPLS está en la asignación e intercambio de etiquetas, que permiten el establecimiento de los Trayectos Conmutados por Etiquetas (LSP) por la red. Los LSP son unidireccionales (“simplex”) por naturaleza; el tráfico bidireccional (“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 (LSR) a otro, a través del dominio MPLS.

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. Al llegar un paquete al LSR de cola (salida), éste determina que el siguiente salto va fuera de la red MPLS, por lo que al consultar la tabla de conmutación de etiquetas, remueve la etiqueta y envía dicho paquete por enrutamiento convencional. La identidad del paquete original queda enmascarada durante el transporte por la red MPLS.

Las etiquetas se insertan en cabeceras MPLS, según las especificaciones del IETF, MPLS debía funcionar sobre cualquier tipo de transporte: LAN, ATM, Frame Relay, etcétera. Por ello, si el protocolo de transporte de datos contiene ya un campo para etiquetas (por ejemplo: ATM o Frame Relay), se pueden utilizar esos campos nativos para las etiquetas. Sin embargo, si la tecnología empleada no soporta un campo para etiquetas (por ejemplo: LAN), entonces se emplea una cabecera genérica MPLS de 4 octetos, que contiene un campo específico para la etiqueta.

Las tablas de envío se generan con la información que se tiene sobre la red, tales como topología, patrón de tráfico y características de los enlaces, entre otros. Esta información es la que manejan los Protocolos de Intercambio Interior (IGP, “Interior Gateway Protocol”) para construir sus tablas de enrutamiento.

MPLS utiliza la información de estos protocolos para establecer los caminos virtuales o LSP. Para cada ruta en la red se crea un camino de etiquetas, concatenando las de entrada/salida en cada tabla de los LSR; el protocolo interno correspondiente se encarga de pasar la información necesaria.

1(a). Construcción de tablas de encaminamiento mediante protocolos internos.

1(b). Creación de rutas LSPs mediante tablas de intercambio de etiquetas entre LSRs adyacentes. Distribución a los LSR por el LDP.

4. LSR cola (salida): quita la etiqueta entrega el paquete al destino.

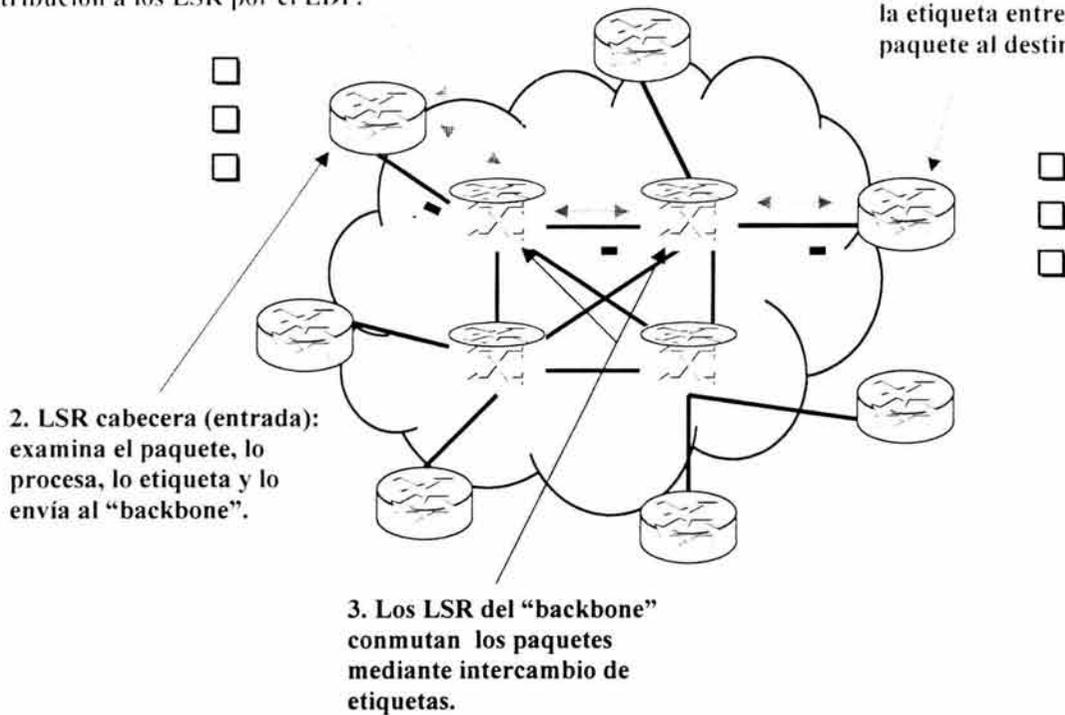


Figura 6.20 Funcionamiento general de MPLS.

MPLS es tecnología que permite a cada usuario clasificar y dar prioridad a los diferentes servicios que utilizan la misma línea.

Conmutadores ATM como LSR: Se pueden utilizar conmutadores ATM como LSR si se les dota del "software" adecuado. Los conmutadores ATM utilizan el puerto de entrada y el valor del campo VPI/VCI como índice de la tabla de donde obtienen el puerto de salida y el valor de salida del campo VPI/VCI. Por tanto, si se codifica el valor de la etiqueta en estos campos se podrán utilizar estos conmutadores como LSR.

VI.4.5 Aplicaciones de MPLS

Las aplicaciones principales de MPLS son :

- Ingeniería de tráfico.
- Soporte a las CoS.
- Servicio de Redes Privadas Virtuales (VPN, "Virtual Private Network").

VI.4.5.1 Ingeniería 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, a manera de evitar que un subconjunto (enlaces, equipos, etcétera) de la red se sature mientras otro subconjunto de la misma se encuentra infrautilizado, mejorando el rendimiento de la red global.

Los flujos de tráfico siguen el camino más corto calculado por el algoritmo de Protocolo de Intercambio Interior (IGP) correspondiente. En casos de congestión de algunos enlaces, el problema se resolvería añadiendo más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos).

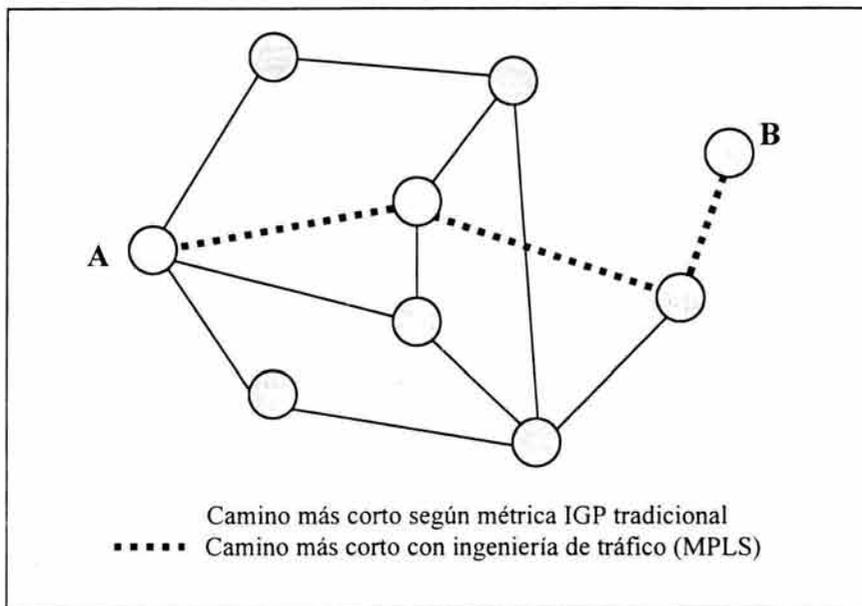


Figura 6.21 Ingeniería de tráfico.

En la figura anterior [Figura 6.21], 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 hagan aconsejable la utilización del camino alternativo indicado con un salto más. MPLS es una herramienta efectiva para esta aplicación en grandes “backbones”, ya que:

- Permite al administrador de la red el establecimiento de rutas, 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 "enrutamiento restringido", de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad).

La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre una 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.

VI.4.5.2 Clases de Servicio

MPLS está 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 mucho más dependientes del retardo y de la variación del mismo, como son las de video y voz interactiva.

MPLS se adapta a ese modelo, ya que las etiquetas MPLS tienen 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 suministrar múltiples LSP, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda (por ejemplo, un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico "best-effort").

VI.4.5.3 Redes Privadas Virtuales (VPN)

La construcción de una red privada virtual (VPN) está basada en conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPN es el soporte de aplicaciones intranet/extranet, integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces.

En la siguiente figura [Figura 6.22] se presenta una comparación entre el modelo de túneles del Protocolo de Internet Seguro (IPSec) con Circuitos Virtuales Permanentes (PVC) y el modelo de LSP de MPLS.

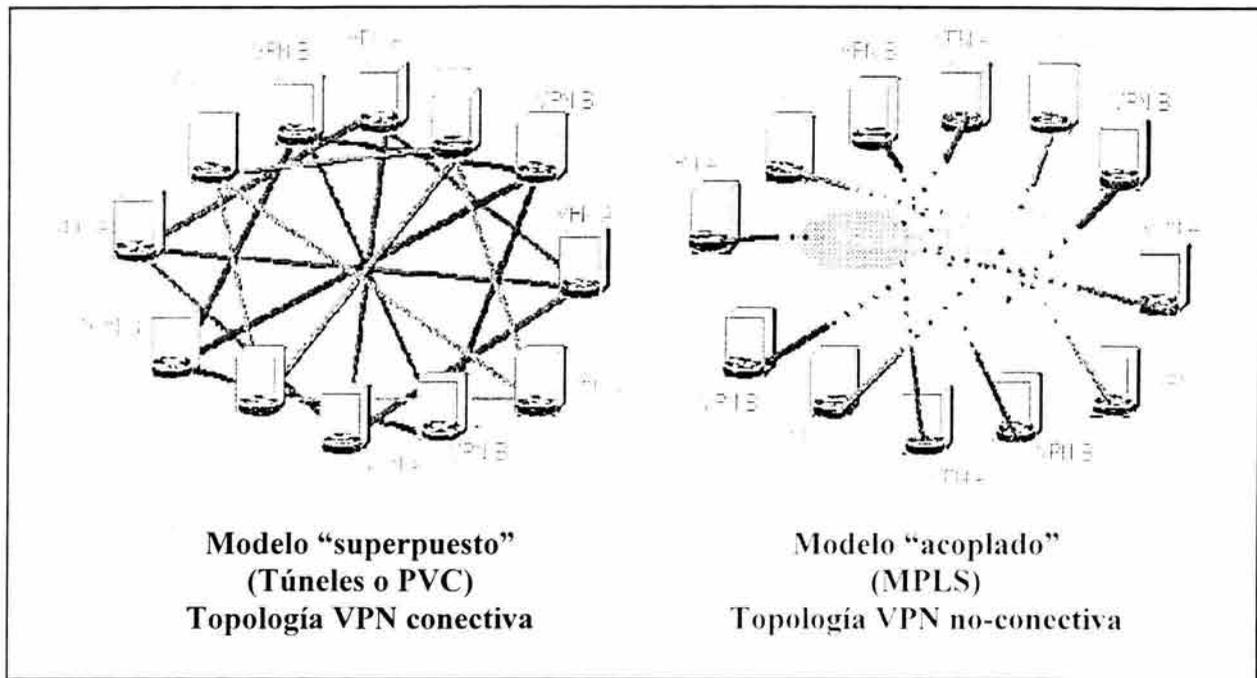


Figura 6.22 Comparación entre el modelo IPsec y el modelo MPLS para VPN.

La diferencia entre los túneles IP convencionales (o los circuitos virtuales) y los "túneles MPLS" (LSP) está en que éstos se crean dentro de la red, basados en LSP, y no de extremo a extremo a través de la red.

Resumiendo, las ventajas que MPLS ofrece para VPN son:

- Proporcionar un modelo "acoplado" o "inteligente", ya que la red MPLS conoce de la existencia de las VPN (lo que no ocurre con túneles ni PVC).
- Evita la complejidad de los túneles y PVC.
- Provee de un servicio sencillo: una nueva conexión afecta a un solo ruteador y tiene mayores opciones de crecimiento.
- Permite mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada.
- Permite aprovechar las posibilidades de ingeniería de tráfico para las poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda, retardo, etcétera), lo que es necesario para un servicio completo VPN.

VI.5 Propuesta de implementación de MPLS

VI.5.1 Estructura de una red con MPLS

Una red implementada con MPLS consiste en routers de conmutación de etiquetas frontera (LER) alrededor de un núcleo de routers de conmutación de etiquetas (LSR), [Figura 6.23]. Los clientes de la red se conectan a ella por medio del proveedor de servicio de red.

Los equipos de usuario (CPE) corren IP convencional, es decir, normalmente no corren MPLS. Es importante resaltar que los LER son parte del proveedor de servicio de la red y son controlados por éste mismo.

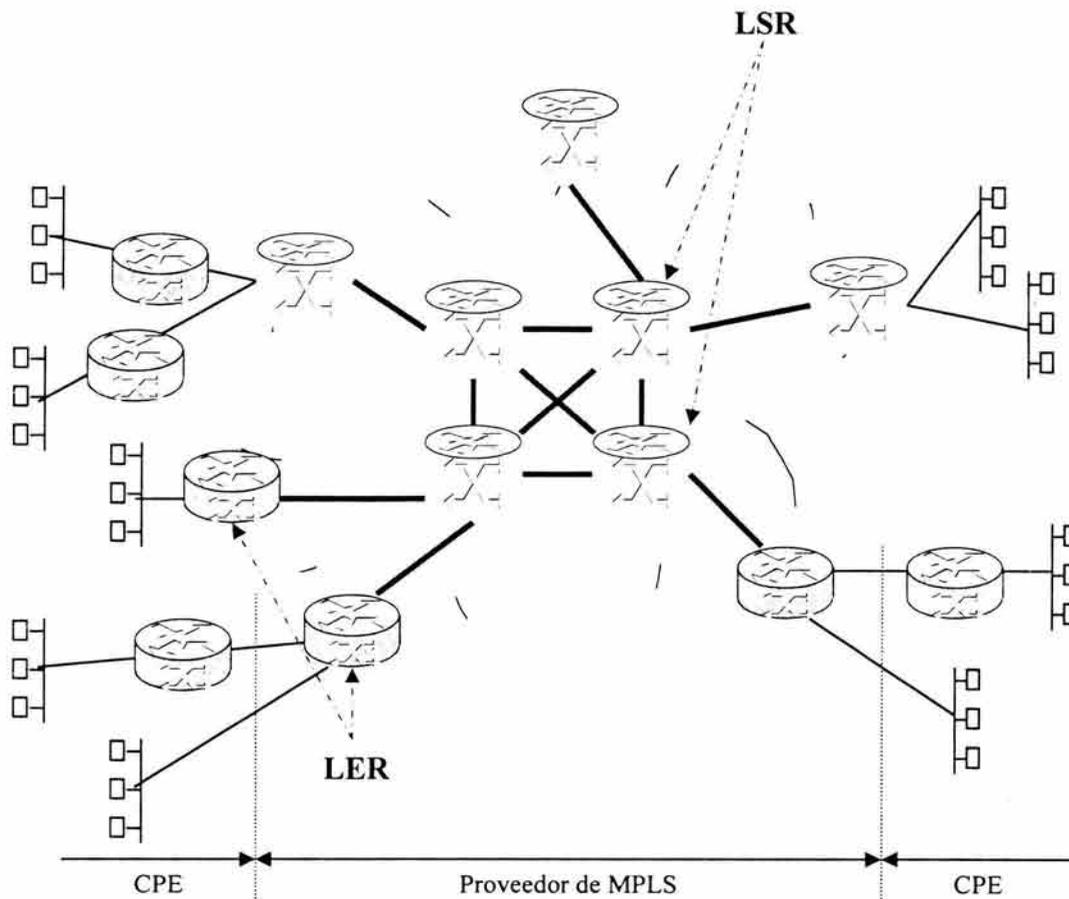


Figura 6.23 Estructura de una red con MPLS.

VI.5.2 Elementos MPLS en una red ATM WAN

A continuación se hace una descripción de los elementos MPLS en una red ATM:

Ruteador de conmutación de etiquetas (LSR, "Label Switching Router"): Es un dispositivo que implementa los componentes de control y reenvío MPLS.

Interfase de un conmutador de etiquetas controlado por ATM (LC-ATM, "Label-Controlled ATM interface"): Es una interfase ATM controlada por el componente de control MPLS; el componente de control puede estar integrado en un "switch" o en un controlador externo.

ATM-LSR: Es un ruteador de conmutación de etiquetas (LSR) basado en un "switch" ATM el cual tiene interfaces LC-ATM.

LSR basado en paquetes ("Packed based LSR"): Es un LSR que envía paquetes completos entre interfaces. Puede o no tener interfaces LC-ATM. Los LSR basados en paquetes típicamente consisten en "software" MPLS corriendo en plataformas de ruteadores ordinarios, algunas veces hay "hardware" con características específicas para la implementación de MPLS.

LSR ATM frontera ("ATM Edge LSR"): Es un ruteador de conmutación de etiquetas basado en paquetes conectado a la nube ATM-LSR por medio de interfaces LC-ATM. Tiene la función de agregar y quitar etiquetas de los paquetes.

En ATM/MPLS los componentes de control y reenvío consisten en:

Componente de control: Utiliza los protocolos estándares de encaminamiento, como OSPF y BGP. Utilizando estos protocolos los ruteadores intercambian información de encaminamiento para construir y mantener las tablas de encaminamiento. Además el componente de control debe crear las asociaciones entre etiquetas y FEC y distribuir esta información.

Componente de Reenvío: Envía los paquetes desde la entrada hacia la salida. Para reenviar los paquetes, el componente de reenvío examina la información de la cabecera del paquete, busca en la tabla de encaminamiento la entrada correspondiente y reenvía el paquete. Por tanto, el componente de reenvío consiste en el conjunto de procedimientos que usa el ruteador para tomar la decisión sobre el reenvío de un paquete.

Cada ruteador de la red implementa ambos componentes. Se podría ver el encaminamiento del nivel de red como una composición de ambos componentes (control y reenvío) implementado de una manera distribuida por el conjunto de ruteadores que conforman la red. La ventaja fundamental de separar ambos componentes es la posibilidad de modificar uno de ellos sin modificar el otro.

VI.5.3 Estructuras de red para la implementación de MPLS en una red ATM

MPLS basado en paquetes

Es la estructura más simple para implementar MPLS, el sitio del usuario es conectado directamente a un LER y el LER es conectado con un LSR que usualmente se basa en plataformas de ruteadores, [Figura 6.24]. Esta estructura se utiliza únicamente para redes que usarán MPLS para poder soportar servicios de redes privadas virtuales (VPN) o ingeniería de tráfico. Esta opción puede ser utilizada durante la fase inicial de la implementación de MPLS en una red ATM.

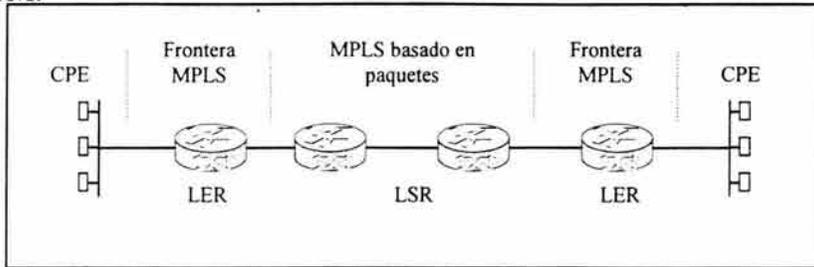


Figura 6.24 MPLS basado en paquetes.

ATM/MPLS con LER

Como en el caso anterior, los sitios son conectados directamente a un LER y este mismo es conectado al núcleo de LSR ATM, [Figura 6.25].

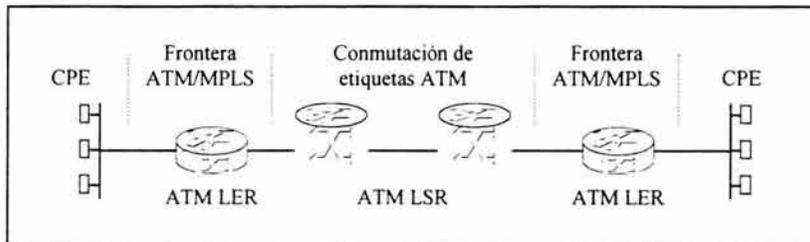


Figura 6.25 ATM/MPLS con LER.

Mezcla de los anteriores

Es posible mezclar ATM/MPLS con LER y MPLS basado en paquetes en una sola red. Algunos enlaces ejecutan MPLS de una forma y otros enlaces lo ejecutan de la otra forma, [Figura 6.26]. Los dispositivos que se conectan entre MPLS de paquetes y ATM/MPLS son los mismos ruteadores que actúan como ATM-LER.

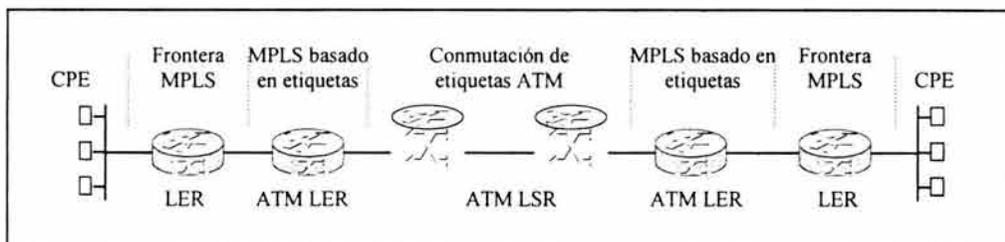


Figura 6.26 Mezcla de ATM y MPLS basado en paquetes.

ATM/MPLS con dispositivos de acceso separados

Las redes ATM/MPLS con LER también suelen usar dispositivos de acceso separados, esto ocurre cuando el acceso es requerido a través de un dispositivo que no soporta los servicios de MPLS. Hay casos en donde esta estructura es requerida, por ejemplo, en donde el acceso es requerido para ambos servicios: IP y ATM o cuando el dispositivo de acceso aún no dispone de “software” que soporte MPLS.

El tráfico del usuario es transportado a través del dispositivo de acceso hacia el LER. Entre el dispositivo de acceso y el LER, hay un enlace diferente para cada cliente, [Figura 6.27]. Éste puede ser Frame Relay, un PVC ATM, etcétera.

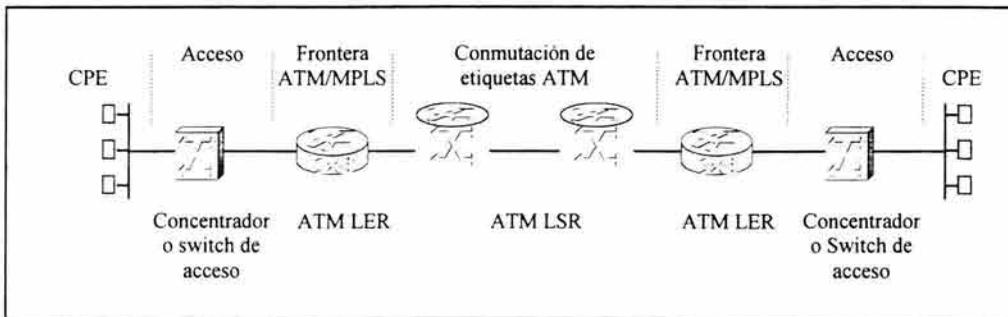


Figura 6.27 ATM/MPLS con dispositivos de acceso separados.

ATM/MPLS con dispositivos de acceso IP+ATM

El caso anterior puede ser simplificado si el dispositivo de acceso soporta LER con funciones de Frame Relay, ATM u otra clase de servicios. En este caso un solo dispositivo proporciona acceso a los servicios IP y ATM, [Figura 6.28].

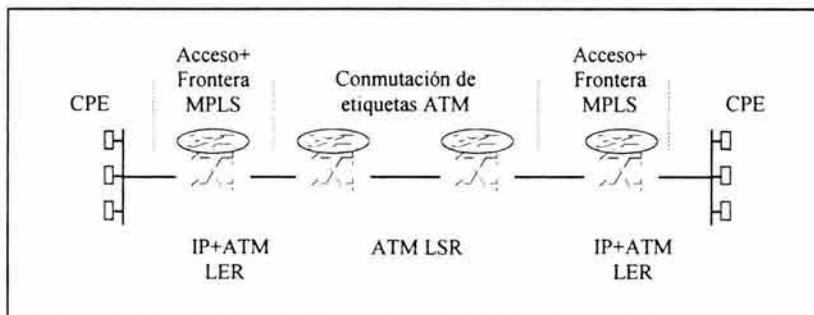


Figura 6.28 ATM/MPLS con dispositivos de acceso IP+ATM.

VI.5.4 Formas de implementación de MPLS

MPLS puede ser introducido en una red ATM gradualmente, comenzando con un solo par de ATM-LER en una red puramente ATM. MPLS puede ser desplegado a través de “switches” tradicionales, utilizando caminos o rutas virtuales (VP); estas conexiones son llamadas túneles VP ya que permiten a MPLS “hacer un túnel” a través de los conmutadores ATM tradicionales.

La [Figura 6.29(a)] muestra la posición inicial con ruteadores conectados por medio de VP a través de una nube ATM, pero tiene las desventajas de mal escalamiento y mala eficiencia de ancho de banda, sin embargo puede proporcionar los servicios VPN MPLS. Desplegando algunos ATM-LSRs en la red como se muestra en las [Figuras 6.29(b) y 6.29(c)] mejora la escalabilidad: el número de VP a cada LER puede reducirse a uno (dos si hay conexión de respaldo). Debido a que un ATM-LSR puede soportar servicios ATM, los conmutadores ATM ordinarios pueden ser retirados, permitiendo el despliegue completo de la red ATM/MPLS como se muestra en la [Figura 6.29(d)], la utilización de VP ya no es requerida. La siguiente figura muestra una estrategia posible para introducir MPLS en una red existente ATM.

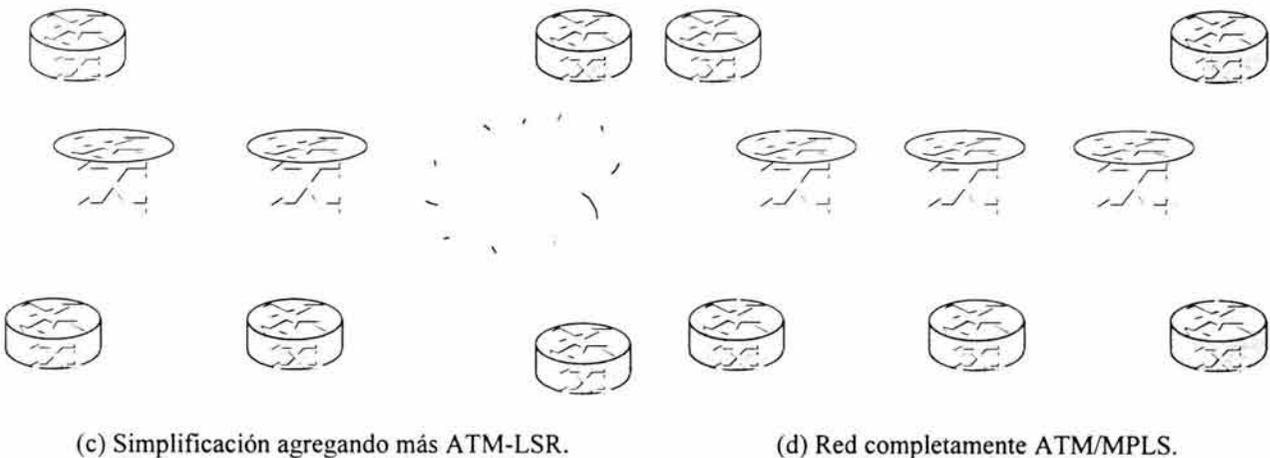
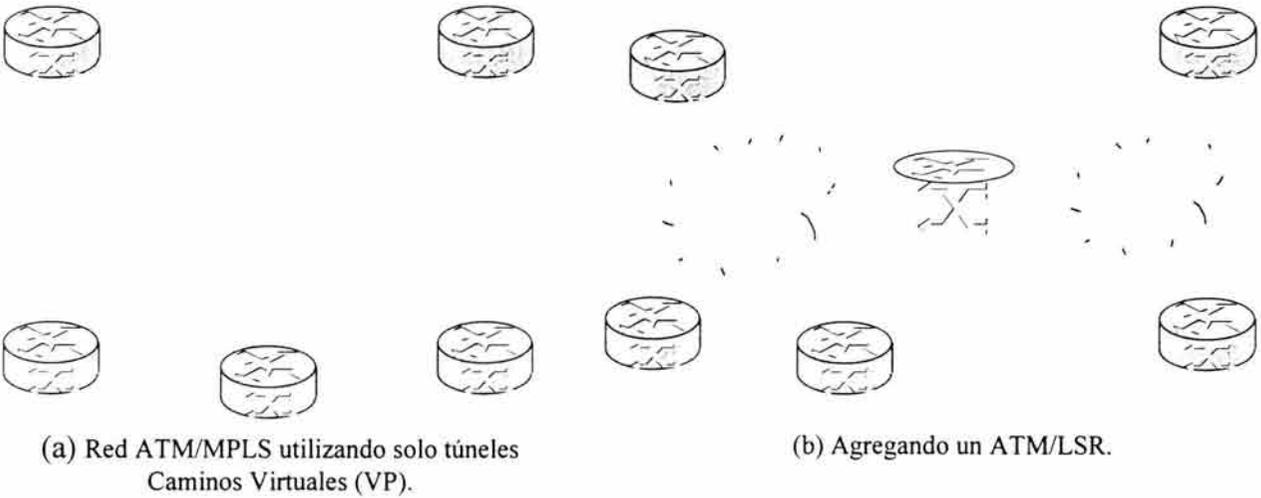




Figura 6.29 Implementación de MPLS en una red ATM.

VI.5.5 Propuesta para implementar MPLS en la red

Primero es necesario hacer el análisis de la tecnología MPLS y los recursos con los que se cuenta en la red para que este protocolo pueda ser implementado.

La estructura de la red para este trabajo de tesis es la siguiente: Enlaces de “backbone” a capacidades de STM-1 (155 Mbps) por medio de equipos de alta capacidad de conmutación con tecnología IP/ATM en cada uno de ellos. Se cuenta con un acceso E3 (34 Mbps) para conectar a cada uno de los nodos remotos hacia el “backbone”, [Figura 6.30]. Los nodos del “backbone” cuentan con equipos con interfaces STM-1 y E3 para poder asegurar la operación como conmutadores ATM + IP.

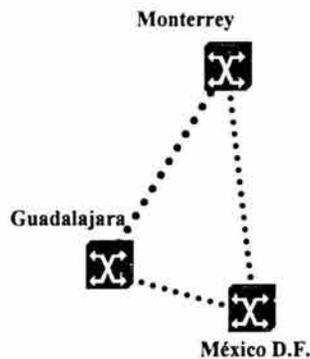


Figura 6.30 Nodos del “backbone”.

Se requiere de una tecnología para realizar un enrutamiento eficiente, el cual permita la aplicación de ingeniería de tráfico, soporte de calidad de servicio (Qos) y otras estrategias que permitan una utilización óptima de la red, la cual esta basada en el protocolo IP sobre una red de conmutación de celdas ATM.

Lo anterior justifica la aplicación de la tecnología MPLS, obteniendo una gran variedad de beneficios pudiendo implementarlo de una manera flexible en lo que respecta a costos, ya que los equipos con los que se cuenta en los nodos del “backbone” son de características muy semejantes (del mismo distribuidor), lo que permite la aplicación de MPLS de una manera totalmente interoperable, sin tener que adquirir una gran variedad de equipo costoso. En lugar de esto, los conmutadores ATM con los que se cuenta en cada nodo “backbone” se convertirán en conmutadores ATM/MPLS, permitiendo la utilización de enlaces ATM y MPLS al mismo tiempo.

La configuración de la red con la propuesta de implementación se muestra en la [Figura 6.31]. Los nodos de acceso hacia el “backbone” de la red realizarán la clasificación del tráfico de datos y aplicarán las etiquetas a los paquetes, permitiendo que sean transportados a su destino por medio de caminos preestablecidos (de forma manual u automática), en base a la conmutación de etiquetas.

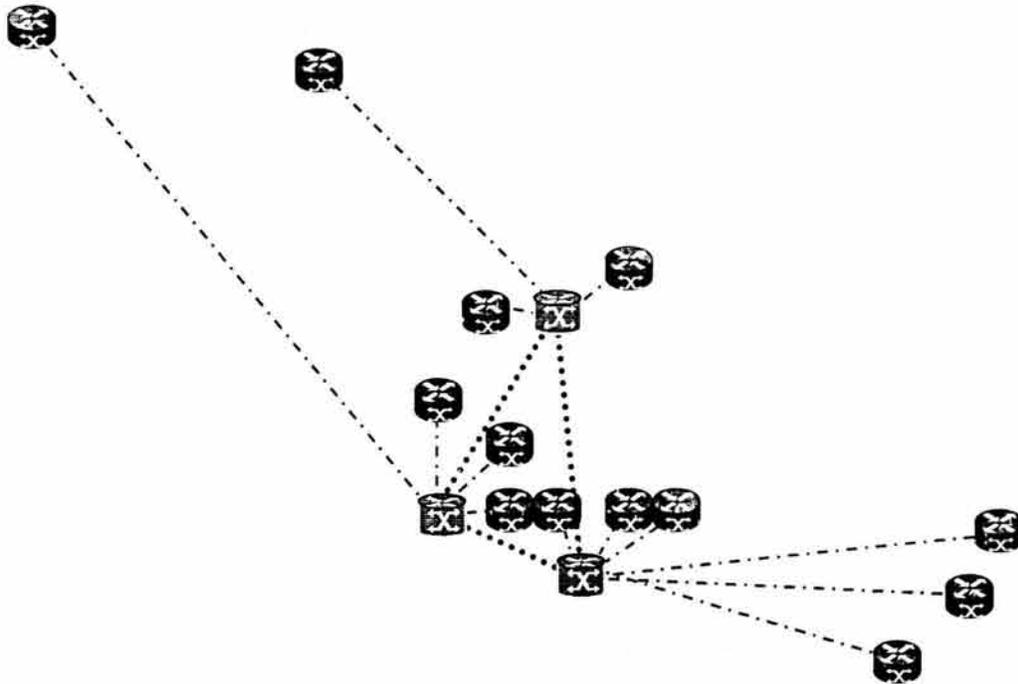


Figura 6.31 Configuración propuesta para la red ATM/MPLS.

Se propone implementar MPLS desde el ruteador central de cada campus [Figura 6.32], teniendo un mayor grado de control sobre el tráfico que es enviado hacia el exterior, clasificando los paquetes en un punto más cercano a la aplicación, satisfaciendo de una mejor manera los requerimientos para proporcionar calidad del servicio.

La propuesta se basa en la implementación de MPLS a partir del ruteador de salida hacia el exterior, ya que sería muy complicado implementarlo desde un inicio dentro de cada red de área local, porque MPLS no es completamente interoperable, lo que trae una serie de dificultades. En un futuro, ya que MPLS sea una tecnología completamente madura y probada, se espera poder llevar su implementación cada vez mas hacia los usuarios finales.

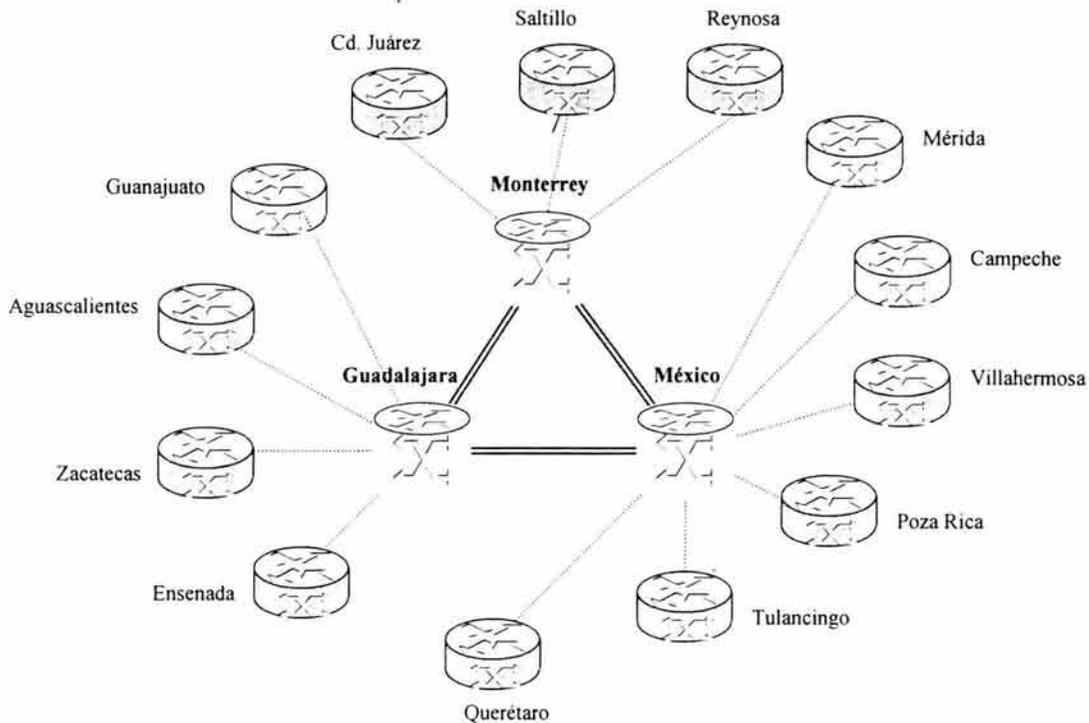


Figura 6.32 Arquitectura propuesta para implementar MPLS.

En la estructura de red ATM/MPLS cada sitio se conecta directamente a un LER, los cuales se conectan con el núcleo de la red. Los conmutadores ATM transportan paquetes con etiquetas ATM/MPLS.

Como parte de la configuración inicial de la red el operador asigna recursos de la red ATM a la Interfase Privada Red a Red (PNNI) [protocolo de encaminamiento dinámico que apoya a la fase de señalización (establecimiento) de los Circuitos Virtuales Conmutados (SVC)] y a MPLS (por ejemplo, ancho de banda en enlaces, espacios VPI/VCI en los enlaces, espacios de tabla de conexión de los circuitos virtuales).

Conclusiones

Como se puede observar en el presente trabajo, MPLS provee ventajas significativas para el óptimo aprovechamiento en una infraestructura de telecomunicaciones, utiliza equipo existente y direccionamiento IP (en conjunto con los mecanismos de señalización adecuados con una actualización de “software” y sin importar la tecnología actual que se esté usando), por lo que no se tienen que hacer grandes cambios para utilizarlo, lo que permite implantaciones a muy bajo costo.

La incorporación de MPLS en una red, permite ofrecer un aumento de eficiencia y ahorro en costos de administración, se pretende que la simplificación de la administración genere mejoras en los servicios, permitiendo la disminución de conexiones lógicas entre equipos, la reducción de la complejidad de la red con la consecuente disminución de costos y riesgos en la operación de la red.

Entre los beneficios más importantes de MPLS, está la capacidad de clasificar y priorizar el tráfico, con un mayor ancho de banda, menor tiempo de envío y con calidad de servicio en las diversas tareas que se llevan a cabo en la red. En consecuencia, la red permite incrementar la productividad en diversas áreas, por ejemplo; los departamentos que administran grandes volúmenes de información pueden mejorar sus tiempos de respuesta e incrementar los servicios disponibles a un mayor número de usuarios. La red permite estar en condiciones de integrar el tráfico de información de diferente naturaleza y optimizar el ancho de banda, suficiente para atender mayores requerimientos de usuarios y aprovechar mejor la infraestructura de transmisión lo cual representa importantes ahorros.

Diferentes tipos de tráfico requieren diferentes características de servicio, las cuales deben de ser garantizadas a lo largo de todo el camino a través de la red. MPLS es una tecnología que permite que la información prioritaria viaje primero que la que tiene menos importancia en la red. Por ejemplo, que las aplicaciones de misión crítica lo hagan antes que una simple transferencia de archivos o la comunicación de una conversación (“chat”). También MPLS permite crear redes privadas virtuales, lo que brindará la facilidad de escalar la red simplificando su administración y abastecimiento de servicios; con las VPN, se puede compartir la infraestructura de la Red de Área Amplia con diferentes sedes remotas en un ambiente mucho más controlado.

La tecnología MPLS lo que hace es poner etiquetas para diferenciar la información, con lo que el control del tráfico de información lo tiene el usuario. Otra de las aplicaciones de MPLS es la Integración de IP con todo tipo de redes subyacentes: Frame Relay, ATM, DWDM, etcétera. Proporciona una mejor integración de ATM con IP (ATM + IP).

Una red en donde las aplicaciones se manejan por separado, crean deficiencias en la administración de la red, porque se administran incorrectamente los medios de comunicación (anchos de banda) ocasionando desperdicio de recursos, cuando otras aplicaciones con más prioridad o de tipo crítico, podrían estar aprovechando este recurso, y además se tienen costos altos por no lograr una convergencia de las diferentes aplicaciones que se tienen implantadas.

MPLS permite, aquellas empresas u organizaciones que implantan el protocolo, controlar los costos mediante la unificación de sus redes, sin necesidad de tener excedentes de ancho de banda.

Actualmente, todos los proveedores de servicios de red, tienen ante sí el enorme reto de administrar redes cada vez más complejas y extensas, con una mayor gama de servicios y con creciente demanda de ancho de banda, calidad y garantías. Esto junto con la tendencia mundial de las redes hacia la convergencia tecnológica de voz, datos, video e imagen, lo cual es consistente con MPLS ya que se puede implementar en cualquier red actual como Fame Relay, ATM, Ethernet, están teniendo un adelanto al unificar estos servicios.

El hecho de integrar en una sola red servicios que antes eran proporcionados por redes diferentes, posibilita la administración de una única red en lugar de varias y ésta reducción del número de redes, reduce los costos de administración y en el aspecto a nivel del usuario, presenta las ventajas más relevantes debido a que se produce una mejoría en las aplicaciones. Mientras servicios distintos se transmiten por redes distintas el ancho de banda contratado en una red, aunque no se use, no está disponible a los servicios de otras redes. Con la integración de servicios, el ancho de banda contratado se pone en cada momento a disposición de quien lo necesite

Hablando de ATM, que es el modo de transporte en una red, la conmutación de celdas es altamente flexible y permite el manejo sencillo de tráfico a velocidad constante (audio y video), como variable (datos); ATM es igualmente adecuada, para aplicaciones de voz, datos, imagen y video, para redes públicas y privadas y se puede usar en LAN, MAN y WAN. ATM combina los beneficios de la conmutación de paquetes y la conmutación de circuitos, reservando ancho de banda bajo demanda de una manera eficaz y de costo efectivo, a la vez que garantiza ancho de banda y calidad de servicio para aquellas aplicaciones sensibles a retardos.

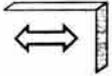
De este modo, ATM está diseñado para ser independiente del medio de transmisión, usa celdas de tamaño fijo, lo que garantiza una velocidad de entrega constante. Puede crear y dar servicio simultáneamente a múltiples aplicaciones independientes con prioridades diferentes (clase de servicio). Además, esas transmisiones simultáneas y múltiples son efectuadas con una velocidad constante de entrega. Como todas las celdas ATM son exactamente del mismo tamaño, son mucho más fácil (y por lo tanto más rápido) de procesar, simplificando la operación de conmutación capaz de trabajar a muy altas velocidades.

Por último, quiero comentar que el presente trabajo me permitió reforzar los conceptos adquiridos durante mi formación profesional y adquirir nuevos conocimientos en el área de telecomunicaciones, descubriendo los múltiples aspectos que se involucran en las redes de voz y datos, al mismo tiempo pude analizar parte de la problemática actual en las redes y con esta tesis aportar una posible solución y una perspectiva general de la tendencia tecnológica de las redes.

Simbología de equipos de interconexión



REPETIDOR (“REPEATER”)



CONCENTRADOR (“HUB”)



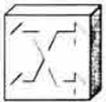
PUENTE (“BRIDGE”)



RUTEADOR (“ROUTER”)



CONMUTADOR (“SWITCH”)



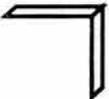
CONMUTADOR ATM (“SWITCH ATM”)



RUTEADOR ATM (FRONTERA) DE CONMUTACIÓN DE ETIQUETAS (“ATM EDGE LSR”)



RUTEADOR ATM DE CONMUTACIÓN DE ETIQUETAS (“ATM LSR”)



CENTRAL TELEFÓNICA (PBX)

Equipos de interconexión

Dos o más redes separadas están conectadas para intercambiar datos o recursos, forman una interred (“internetwork”). Enlazar Redes de Área Local en una interred requiere de equipos que realicen ese propósito. Estos dispositivos están diseñados para sobrellevar los obstáculos para la interconexión sin interrumpir el funcionamiento de las redes. A estos dispositivos que realizan esa tarea se les llama equipos de interconexión, (Martinez, 1999).

Existen equipos de Interconexión a nivel de:

- *Redes de Área Local (LAN)*: Concentrador, conmutador, repetidor, puerta de enlace, puente.
- *Redes de Área Amplia (MAN)*: Repetidor, conmutador capa 3, ruteador, puente inalámbrico, modem analógico, DSU/CSU.
- *Redes de Área Amplia (WAN)*: Ruteador, modem analógico, DSU/CSU, modem satelital.

REPETIDOR

Un repetidor (o generador) es un dispositivo electrónico que opera sólo en la Capa 1 del Modelo OSI (capa física). Un repetidor permite sólo extender la cobertura física de una red, pero no cambia la funcionalidad de la misma. Un repetidor regenera una señal a niveles más óptimos. Es decir, cuando un repetidor recibe una señal muy débil o corrompida, crea una copia “bit” por “bit” de la señal original. La posición de un repetidor es vital, éste se debe poner antes de que la señal se debilite. En el caso de una red local (LAN) la cobertura máxima del cable UTP es 100 metros; el repetidor debe ponerse unos metros antes de esta distancia para poder extender la distancia a otros 100 metros o más. Existen también generadores ópticos conocidos como Amplificadores de Fibra Dopada con Iones de Erblio (EDFA) los cuales permiten extender la distancia de un haz de luz sobre una fibra óptica hasta 125 millas.

Aplicación
Presentación
Sesión
Transporte
Red
Enlace de
Datos
Física

Repetidor
→



*Repetidor fibra óptica
Omnitron Systems Technology, Inc.
2 Puertos GIGABIT SM SC.*

PUENTE (“BRIDGE”)

Los puentes operan tanto en la Capa Física como en la de Enlace de Datos del Modelo de referencia OSI. Los puentes pueden dividir una red muy grande en pequeños segmentos. Pero también pueden unir dos redes separadas. Los puentes pueden hacer filtraje para controlar el tráfico en una red.

Como un puente opera en la capa de enlace de datos, da acceso a todas las direcciones físicas a todas las estaciones conectadas a él. Cuando una trama entra a un puente, el puente no sólo regenera la señal, sino también verifica la dirección del nodo destino y reenvía la nueva copia sólo al segmento al cual pertenece la dirección. En cuanto un puente encuentra un paquete, lee las direcciones contenidas en la trama y compara esa dirección con una tabla de todas las direcciones de todas las estaciones en ambos segmentos. Cuando encuentra una correspondencia, descubre a que segmento pertenece la estación y envía el paquete sólo a ese segmento.

Un puente también es capaz de conectar dos Redes de Área Local que usan diferente protocolo (por ejemplo: Ethernet y Token Ring). Esto es posible haciendo una conversión de protocolos de un formato a otro.

Aplicación
Presentación
Sesión
Transporte
Red
Puente
→ **Enlace de Datos**
Física



*Puente entre TCP/IP, AppleTalk, DecNet, NetBeui y Ethernet.
Interfases 10/100BaseT Ethernet y RS-232/422/485.*

CONMUTADOR DE PAQUETES (“SWITCH”)

El “switch” es otro dispositivo de interconexión de capa 2 que puede ser usado para preservar el ancho de banda en la red al utilizar la segmentación. Los “switches” son usados para reenviar paquetes a un segmento particular utilizando el direccionamiento de hardware MAC (como los puentes). Debido a que los “switches” son basados en “hardware”, estos pueden conmutar paquetes más rápido que un puente.

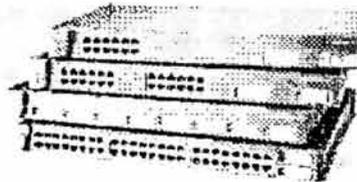
Aplicación
Presentación
Sesión
Transporte
Red
Enlace de
Datos
Física

Switch
→

Los “switches” pueden ser clasificados en como reenvían los paquetes al segmento apropiado. Están los “store-and-forward” y los “cut-through”.

Los conmutadores que emplean la técnica “store-and-forward” completamente procesan el paquete y la determinación del direccionamiento del paquete. Esto requiere que el paquete sea almacenado temporalmente antes de que sea enviado al segmento apropiado. Este tipo de técnica elimina el número de paquetes dañados que son enviados a la red.

Los conmutadores que usan la técnica “cut-through” son más rápidos debido a que estos envían los paquetes tan pronto la dirección MAC es leída. Por otra parte, también existe en el mercado conmutadores de paquetes de capa 3 y 4. Es decir hacen las funciones que los de capa 2, pero además realizan funciones de enrutamiento (capa 3) y conmutación de voz (capa 4).



Switch marca Cisco modelo Catalyst 3500 XL.

RUTEADOR (“ROUTER”)

Los ruteadores operan en la capa de red (así como enlace de datos y capa física) del Modelo OSI. Los Ruteadores organizan una red grande en términos de segmentos lógicos. Cada segmento de red es asignado a una dirección así que cada paquete tiene tanto dirección destino como dirección fuente.

Aplicación
Presentación
Sesión
Transporte
Red
Enlace de
Datos
Física

Ruteador
→

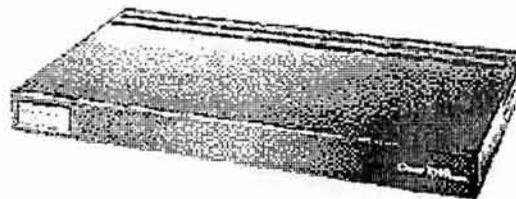
Los ruteadores son más inteligentes que los puentes, no sólo construyen tablas de enrutamiento, sino que además utilizan algoritmos para determinar la mejor ruta posible para una transmisión en particular.

Los protocolos usados para enviar datos a través de un ruteador deben ser específicamente diseñados para soportar funciones de enrutamiento.

Los ruteadores pueden ser de dos tipos:

Ruteadores estáticos: Estos ruteadores no determinan rutas. En lugar de eso, se debe de configurar la tabla de enrutamiento, especificando las rutas potenciales para los paquetes.

Ruteadores dinámicos: Estos ruteadores tienen la capacidad de determinar rutas (y encontrar la ruta más óptima) basados en la información de los paquetes y en la información obtenida de los otros ruteadores.



Ruteador marca Cisco 2500 series.

PUERTA DE ENLACE (“GATEWAY o PROXY SERVERS”)

Gateway →	Aplicación	<p>Los “gateways” o “proxy servers” son computadoras que están corriendo una aplicación o “software”. Los “gateways” trabajan en las capas superiores del Modelo OSI (transporte, sesión, presentación y aplicación).</p> <p>Este “software” es capaz de realizar una infinidad de tareas: conversión de protocolos para proveer la comunicación de dos plataformas distintas. También los “gateways” suelen ser servidores que corren “software” de seguridad como “firewall”, correo electrónico; servidores de web, Servidores de Dominios de Nombres (DNS), etcétera.</p>
	Presentación	
	Sesión	
	Transporte	
	Red	
	Enlace de Datos	
	Física	

CONCENTRADOR (“HUB”)

Hub →	Aplicación	<p>El concentrador o “hub” es un dispositivo de capa física que interconecta físicamente otros dispositivos (por ejemplo: computadoras, impresoras, servidores, “switches”, etcétera) en topología estrella o ducto.</p> <p>Existen concentradores pasivos y concentradores activos. Los pasivos sólo interconectan dispositivos, mientras que los concentradores activos además regeneran las señales recibidas, como si fuera un repetidor. Un concentrador activo puede ser llamado como un repetidor multiuertos.</p>
	Presentación	
	Sesión	
	Transporte	
	Red	
	Enlace de Datos	
	Física	



Hub marca 3Com modelo Superstack II 24 puertos.

DSU/CSU (modem digital)

El DSU/CSU (“Data Service Unit/Channel Service Unit”) o mejor conocido como DTU (“Data Terminal Unit”) es un equipo de interconexión que opera en la capa de Enlace de Datos. Un DSU/CSU es básicamente un modem digital que enlaza dos o más redes que tengan servicios digitales tales como E1/T1’s, Frame Relay, etcétera. Para su aplicación a largas distancias, extendiendo la comunicación a través de los pares de cobre.

Un CSU provee acondicionamiento y ecualización de la línea, se utiliza para conectar líneas de conmutación digitales y la regeneración de señal. Es económico y proporciona una terminación para la señal digital. El CSU proporciona varias pruebas del bucle de vuelta en la línea y mantiene la línea conectada si el otro equipo de comunicación falla.

Un DSU es un dispositivo de comunicación, el cual puede contener las características de un CSU, convierte las señales de datos de un Equipo Terminal de Datos DTE (por ejemplo: una computadora, un puente, un ruteador, etcétera) en señales digitales bipolares requeridas en la red digital, realiza la sincronización de relojes y regenera la señal. Un DSU conecta el equipo local de teléfonos de una compañía a las líneas de comunicación digitales, como puede ser una línea T1.

DSU y CSU se combinan a menudo en un dispositivo y se conectan a un grupo de canales, que proporcionan conversión analógico-digital y multiplexación de transmisiones de voz. (LAN TIMES, Enciclopedia de Redes, McGraw-Hill, 1995).

Aplicación
Presentación
Sesión
Transporte
Red
**Enlace de
Datos**
Física

DSU/CSU
→

DSU/CSU marca ADTRAN.

Glosario de términos

10base 2	Red tipo bus con cable coaxial delgado como el RG-58, banda base y que puede transmitir a 10 Mbps a una distancia de 200 metros, a esta se le conoce como chip Ethernet.
10base 5	Describe una red tipo bus con cable coaxial grueso, banda base y que puede transmitir a 10 Mbps a una distancia máxima de 500 metros.
10base T	Este tipo de red es hoy en día una de las más usadas, por su fácil estructuración y control central en esta se utiliza cable UTP y se puede transmitir a 10 Mbps a una distancia máxima de 100 metros.
Analógico	Significa todo aquel proceso entrada/salida cuyos valores son continuos. Algo continuo es todo aquello que puede tomar una infinidad de valores dentro de un cierto límite, superior e inferior.
Ancho de banda	(“Bandwidth”). Diferencia entre las señales de frecuencia senoidal más alta y más baja que pueden transmitirse por una línea de transmisión o a través de una red. El ancho de banda se mide en Hertz (Hz), y también define la capacidad máxima de transporte de información de la línea o red.
Antivirus	Programa que detecta y elimina virus informáticos. Su acción puede ser preventiva o correctiva.
ASCII	Código de 7 bits que sustituye las letras del alfabeto por cifras y otros caracteres informáticos. Los caracteres ASCII permiten la comunicación con ordenadores, que utilizan un lenguaje especial llamado binario formados por ceros y unos. Al escribir en el teclado, el ordenador interpreta cada letra escrita en lenguaje binario ASCII, para que puedan ser leídas, manipuladas, almacenadas o recuperadas.
ASN.1	Sintaxis abstracta empleada para definir la estructura de las unidades de datos asociadas a una entidad de protocolo en particular.
Backbone	Es un enlace de gran caudal o una serie de nodos de conexión que forman un eje de conexión principal. Es la columna vertebral de una red.
Baudio	(“Baud”). Número de variaciones de la señal de la línea por segundo; también indica la velocidad de transmisión de datos por una línea, aunque esto sólo es estrictamente correcto cuando cada bit se representa mediante un solo nivel de señal en la línea de transmisión. En este caso, la tasa de bits y la tasa de señal de la línea son iguales.
BGP	Protocolo de encaminamiento usado entre sistemas autónomos.
Bit	Unidad de medida que se usa para describir la parte más pequeña posible de información en la computadora, representada como un dígito binario.
Bus	Uno o más conductores que sirven como conexión común para un grupo de dispositivos relacionados.
Byte	Unidad de medida usada para describir una cantidad de datos, igual a ocho bits. Un carácter es un byte en tamaño.
CAD/CAM	Este acrónimo es utilizado para referirse a sistemas de computadora generados para la manipulación de la información gráfica relativa al diseño, a la fabricación industrial y a la manufactura de productos.

Cliente/ Servidor	Modelo lógico de una forma de proceso cooperativo, independiente de plataformas “hardware” y sistemas operativos. Generalmente, el modelo se refiere a un puesto de trabajo o cliente que accede mediante una combinación de “hardware” y “software” a los recursos situados en un ordenador denominado servidor.
CMIP	Protocolo de la capa de aplicación del Modelo OSI que sirve para recuperar y enviar información relacionada con la administración a través de una red OSI.
Codec	Aparato utilizado para digitalizar señales analógicas y viceversa, para permitir la comunicación entre computadoras por modem a través de líneas telefónicas.
CORBA	Es una especificación, no es un “software” o aplicación, para establecer interoperatividad entre plataformas.
CPE	Se refiere al equipo del cliente, el cual permite que el servicio contratado (por ejemplo, Frame Relay , ATM, etcétera) sea utilizado por sus aplicaciones.
Cps	Cuadros por segundo.
Cracker	Saboteador. Se define como un individuo cuyas malas intenciones lo llevan a tratar de entrar a una red o sistema burlando su seguridad.
CSMA/CD	Método utilizado para controlar el acceso a un medio de transmisión compartido, como un bus de cable coaxial al cual están conectadas varias estaciones. Lo primero que hace una estación que desea transmitir un mensaje es detectar (escuchar) el medio, y sólo transmitirá el mensaje si el medio está inactivo es decir, si no está presente una portadora. Durante la transmisión del mensaje, la estación vigila la señal del medio de transmisión. Si esta señal es diferente de la que está transmitiendo, se dice que ocurrió una colisión y que fue detectada. La estación dejará de transmitir y repetirá el intento posteriormente. Se usa en Ethernet.
Demodular	Proceso de extracción de datos de una portadora; lo inverso de modulación.
Digital	El término digital involucra valores de entrada/salida discretos, es decir que puede tomar valores fijos, esos valores son el cero (0) o el uno (1).
Dispositivo	Cualquier nodo de la red, desde un gran procesador a una computadora personal, pasando por estaciones de trabajo, impresoras, etcétera.
DLCI	Número de circuito virtual conmutado en una red de retransmisión de tramas. Está situado en la cabecera de la trama e identifica el circuito lógico por el que van los datos.
DNS	Protocolo de aplicación con el que el conjunto TCP/IP se transforman los nombres simbólicos que utilizan las personas en las direcciones plenamente calificadas equivalentes.
DS1	(“Digital Signal level 1”), Señal Digital de Nivel 1: Término usado para referirse a 1.54 Mbps en EUA o 2.048 Mbps en Europa.
Duplex	Describe un canal de comunicación que siempre está abierto en ambas direcciones. En telecomunicaciones, se refiere a la habilidad de ambas partes para transmitir y recibir señales al mismo tiempo. También conocido como “duplex” completo (“full duplex”).
E1	(“European TransMission Service Level 1”), Servicio de Transmisión Europea Nivel 1: Usado para transmitir datos sobre una red telefónica a 2.048 Mbps. Es el equivalente al DS1 en EUA y T1 en Europa .

EGP	Protocolo empleado en interredes grandes que comprenden varias interredes menores conectadas entre sí. Los dispositivos de interconexión implicados se denominan puertas de enlace exteriores y el EGP es el protocolo del que se valen para comunicar las direcciones de IP de las redes presentes en cada una de las interredes menores.
EIA	Grupo que especifica estándares de transmisión eléctrica.
EIA-232	Se utiliza como norma de interfase para conectar un dispositivo periférico, por ejemplo una pantalla o una impresora, a una computadora.
Ethernet	(IEEE 802.3). Las redes Ethernet se basan en una topología de bus donde todas las interfases conectadas al cable "escuchan" lo que otras interfases "escriben". Cuando una interfase desea enviar un dato a través de la red, simplemente comienza a transmitir.
Facsimil	Reproducción (o copia; normalmente de imágenes). Se refiere sobre todo al envío de imágenes sin movimiento a través de una línea de comunicación (Internet, cualquier red, etcétera). Su abreviatura es el FAX.
FDM	División de un medio de transmisión en dos o más canales fraccionando la banda de frecuencia transmitida, en bandas más estrechas, y utilizando cada una de ellas como un canal diferente.
Firewall	Muro de fuego. Mecanismo utilizado para proteger una red, o computadora conectada a Internet de accesos no autorizados. Puede implementarse con "software", "hardware" o una combinación de ambos.
Firmware	Parte del "software" de un ordenador que no puede modificarse por encontrarse en la ROM o memoria de sólo lectura, ("Read Only Memory"). Es una mezcla o híbrido entre el "hardware" y el "software", es decir tiene parte física y una parte de programación consistente en programas internos implementados en memorias no volátiles. Un ejemplo típico de "Firmware" lo constituye la BIOS.
FTP	Protocolo de aplicación IP para transferir archivos entre nodos de red.
HDLC	Protocolo de comunicaciones ISO utilizado en redes de conmutación de paquetes X.25. Proporciona corrección de errores al nivel de enlace de datos.
HTTP	Conjunto de instrucciones que especifica cómo se publicará la información en la Internet.
IEEE	Instituto que define estándares para equipos electrónicos utilizados en ciencias computacionales.
IGP	Es un protocolo para el intercambio de información de enrutamiento entre "gateways" ("routers" o "host") adentro de una red autónoma.
IPSec	Es un panel de trabajo para un conjunto de protocolos para proveer seguridad en la capa de procesamiento de paquetes de la red.
Jitter	Distorsión de línea de comunicaciones análogas causada por la variación de una señal desde sus posiciones de referencia en el tiempo. El "jitter" puede causar pérdida de datos, particularmente a altas velocidades.
Kbps	Kilobits por segundo. Unidad de medición usada para describir la velocidad de transferencia de datos.
LAPB	Protocolo de capa de enlace de datos en la pila del protocolo X.25.

LDP	Es un protocolo para en intercambio y distribución de etiquetas entre los ruteadores de conmutación de etiquetas (LSR) de una red con el protocolo MPLS.
MAC	Protocolo que define las condiciones en las cuales las estaciones de trabajo acceden al medio, su uso está difundido en las LAN tipo IEEE, la capa MAC es la subcapa más baja del protocolo de la capa de enlace de datos.
Mbps	Megabits por segundo.
Mhz	Megahertz.
Micrón	Unidad de longitud, un micrón es igual a una millonésima de un metro, también se conoce como micrómetro, y se exhibe como μm .
Modem	(Modulador/Demodulador): Dispositivo que convierte datos desde un formato digital a un analógico en la computadora de origen, para que se puedan transmitir a través de líneas telefónicas estándares. El modem en la terminal de recibo de la transmisión de inmediato convierte los datos de formato analógico a formato digital, para que la computadora receptora pueda leerlos.
Modulación	Proceso por el cual una señal es modificada para representar una portadora de información.
Monocromática	Estrictamente, luz de una sola longitud de onda, o lo que es lo mismo, color puro. También se aplica a la imagen formada por tonos de un color y a la fotografía en blanco y negro.
Multicast	Paquetes que se copian en un subconjunto específico de direcciones de red. Estas direcciones se especifican en el campo de dirección destino. En contraste, en una propagación, todos los paquetes se envían a todos los dispositivos en una red.
Multiplexar	Dividir una señal en varios canales.
Nodo	("Host"). Cualquier dispositivo que trabaja dentro de una red.
NTSC	Sistema de codificación de la señal televisiva adoptado en varios países como EUA o Japón.
OC-1	("Optical Carrier Level 1"), Portadora Óptica de Nivel 1. Término SONET para una señal transmitida a 51.85 Mbps.
Octeto	Grupo de ocho bits, con el que usualmente se opera como una entidad.
OSPF	Protocolo que especifica cómo los ruteadores intercambian la información de encaminamiento.
PBX	Es un sistema telefónico dentro de una empresa, que maneja llamadas entre usuarios de una empresa en líneas locales mientras permite que entre todos los usuarios compartan un número determinado de líneas telefónicas externas. Su función principal es la de reducir los costos de tener una línea telefónica por cada usuario.
PCM	Proceso en el que se muestrea una señal, y se convierte la magnitud de cada muestra según una referencia prefijada, codificándola en una señal digital.
Pixel	Uno de los puntos individuales que constituyen una imagen gráfica.
PNNI	Protocolo utilizado para intercambiar información de lugar entre ruteadores, esto permite integrar redes sin conexiones, basadas en ruteadores, con redes ATM.

PSTN	Es la red telefónica (analógica).
PVC	Es un camino virtual a través de una red, caracterizado por tener puntos de llegada definidos por el operador de la red. Un camino físico puede soportar varios PVC.
RFC	Serie de documentos usados como los medios primarios para comunicar información a través de Internet. La mayoría de los RFC documentan protocolos tales como Telnet y Ftp, pero algunos son humorísticos o históricos.
RFC 1155	Define la Estructura de Información de Administración (SMI) para redes basadas en TCP/IP. Describe cómo se definen los objetos administrados contenidos en el MIB.
RFC 1157	Define el Sistema de Administración de Redes (NMS) como una estación que ejecuta aplicaciones de administración de red que monitorizan y controlan elementos de red como nodos, puertas de enlace y servidores de terminales. Estos elementos usan un agente de administración para realizar estas funciones.
RG-58	Cable coaxial de 50 ohmios de impedancia. Usado por el IEEE 802.3 10Base2.
RSVP	Protocolo que se utiliza para reservar recursos para una sesión en un entorno de red IP. Pretende proporcionar calidad de servicio estableciendo una reserva de recursos para un flujo determinado. Un "host" hace una petición de una calidad de servicio específica sobre una red para un flujo particular de una aplicación.
Semiduplex	Describe un canal de comunicación que está abierto en los dos sentidos pero en uno solo a la vez, en cualquier momento, en Inglés: "half duplex".
Señal	Cualquier evento que lleve implícita cierta información. Las señales pueden ser: Analógicas (onda electromagnética que varía continuamente y se puede propagar por medios diversos) y Digitales (aquella señal cuya forma de onda es discreta).
Simplex	Modo de transmisión de datos solamente en una dirección preasignada.
SNA	En redes IBM, descripción de la estructura lógica en capas, los formatos protocolos y secuencias operativos que se utilizan para transmitir unidades de información a través de redes, así como para controlar la configuración y la operación de las redes.
T1	("Transmisión Service"), equivalente a DS1. Servicio de comunicaciones en Estados Unidos basado en líneas dedicadas a 1.5 Mbps.
TDM	División de un servicio de transmisión en dos o más canales transmitiendo la información de cada uno de ellos en intervalos de tiempo diferentes.
Telemetría	Datos, normalmente mediciones, transmitidos desde un sensor remoto a un receptor.
Teléx	Servicio final conmutado que permite la transmisión de mensajes codificados en tiempo real entre los terminales de la red mediante la utilización de un código estandarizado.
Telnet	Protocolo de aplicación del conjunto TCP/IP que permite a un usuario en una terminal interactuar con un programa que se ejecuta en otra computadora.
Testigo	("Token"). Paquete (o parte de un paquete) utilizado en Redes de Área Local, la estación que es dueña del paquete es la estación que controla el medio de transmisión.

Token-bus	(IEEE 802.4) Ducto de testigo: Tipo de Red (de datos) de Área Local. El acceso al medio de transmisión compartido (que se implementa en forma de un bus al cual están conectados todos los dispositivos en comunicación) está bajo el control de un solo testigo de control (permiso). Sólo el poseedor actual del testigo puede transmitir un mensaje por el medio. Todos los dispositivos que desean transmitir mensajes están conectados en un anillo lógico. Después de que un dispositivo recibe el testigo y transmite los mensajes que tiene en espera, pasa el siguiente dispositivo del anillo.
Token-ring	(IEEE 802.5) Las redes "token-ring" se basan en una topología de anillo, donde los datos circulan a través del anillo, de interfase en interfase. En esta topología, las interfases no transmiten cuando lo desean, sino que esperan a recibir el "token". Este "token", va circulando por todas las interfases dándole a cada una la posibilidad de transmitir.
Transponder	Equipo de comunicación satelital que recibe señales y las retransmite a tierra.
Troyano	Caballo de troya. Programa que parece inofensivo, pero que, al instalarlo en la computadora, ejecuta funciones dañinas para el sistema. En ocasiones, al ejecutarlo no se notan cambios, pero dejan "puertas de acceso" abiertas, por las que otras personas pueden acceder a la información contenida en la computadora sin nuestra autorización.
V.34	Norma internacional para comunicaciones vía modem que permite alcanzar una velocidad de 28,800 baudios.
VGA	Estándar de presentación de video de IBM, se ha convertido en el estándar mínimo de presentación para computadoras personales. Su modo de resolución más alto es de 640x480 con 16 colores. La mayor parte de los adaptadores VGA proveen resoluciones 640x480, 800x600 y 1024x768 con al menos 256 colores.
Virus	Programa de computadora o porción de código que puede causar daños a la información, datos o programas.
WWW	Base de datos universal que proporciona un medio consistente de acceso a grandes cantidades de información. Los documentos en la "web" facilitan la recuperación rápida de información a través de los enlaces de hipertexto.
X.21	Estándar ITU para la conexión entre DTE y DCE para operación síncrona de redes públicas de datos.

Acrónimos

AAL	ATM Adaptation Layer	Capa de Adaptación de ATM
ACD	Automatic Call Distributor	Distribuidor de Llamadas Automático
ADM	Add/Drop Multiplexer	Multiplexor de Agregar/Liberar
AIX	Advanced Interactive eXecutive	Administrador Interactivo Avanzado
ALE	Address Lifetime Expectations	Expectativas del Tiempo de vida del esquema de direcciones IP
ANSI	American National Standards Institute	Instituto de Estándares Nacionales de América
ARPA	Advanced Research Projects Agency	Agencia de Proyectos Avanzados de Investigación
ARPANET	Advanced Research Projects Agency Network	Red de la Agencia de Proyectos Avanzados de Investigación
ASCII	American Standard Code For Information	Código Estándar Americano para la Información
ASN.1	Abstract Syntax Notation One	Notación Uno de Sintaxis Abstracta
ASR	Automatic Speech Recognition	Reconocimiento de Voz Automático
ATM	Asynchronous Transfer Mode	Modo de Transferencia Asíncrono
ATT	Address Translation Table	Tabla de Traslación de Direcciones
BGP	Border Gateway Protocol	Protocolo de Puerta de Enlace Externa
B-ISDN	Broadband Integrated Services Digital Network	Red Digital de Servicios Integrados de Banda Ancha
BRI	Basic Rate Interface	Interfase de Tasa Básica
CAD	Computer Aided Design	Diseño Asistido por Computadora
CAM	Computer Aided Manufacturing	Fabricación Asistida por Computadora
CBR	Constant Bit Rate	Velocidad de Bit Constante
CCITT	International Consultive Committee on Telegraphy and Telephony	Comité Consultivo Internacional en Telegrafía y Telefonía
CIR	Committed Information Rate	Tasa de Información Comprometida
CLP	Cell Loss Priority	Prioridad de Pérdida de Celda
CMIP	Common Management Information Protocol	Protocolo de Información de Administración Común
Codec	Coder-Decoder	Codificador-Decodificador
CORBA	Common Object Request Broker Architecture	Arquitectura de Agente de Petición de Objeto Común
CoS	Class of Service	Clase de Servicio
CPE	Customer Premises Equipment	Equipos de Usuario
CPU	Central Process Unit	Unidad Central de Proceso
CSMA/CD	Carrier Sense Multiple Access with Collision Detection	Acceso Múltiple por Detección de Portadora, con Detección de Colisiones
CSU	Channel Service Unit	Unidad de Servicio de Canal
CTI	Computer Telephone Integration	Integración Computador-Teléfono
DAS	Dual Attachment Stations	Estaciones de Conexión Doble
DCE	Data Circuit-terminating Equipment	Equipo de Circuito de Datos
DDI	Direct Dialing Inward	Marcación Interior Directa
DFB	Distributed FeedBack	Regeneración Distribuida
DLCI	Data Link Connection Identifier	Identificador de la Conexión del Enlace de Datos
DNS	Domain Name Server	Servidores de Dominios de Nombres
DPAM	Demand Priority Access Method	Acceso de Prioridad de Demanda
DQDB	Distributed Queue Dual Bus	Cola Distribuida en Doble Bus
DSU	Data Service Unit	Unidad de Servicio de Datos
DTE	Data Terminal Equipment	Equipo Terminal de Datos
DWDM	Dense Wavelength Division Multiplexing	Multiplexación en Longitud de Onda
EDFA	Erbium Doped Fiber Amplifier	Amplificador de Fibra Dopada con Iones de Erblio
EGP	Exterior Gateway Protocol	Protocolo de Puerta de Enlace Exterior

EIA	Electronic Industries Association	Asociación de Industrias Electrónicas
ETSI	European Telecommunications Standards Institute	Instituto Europeo de Telecomunicaciones Estándares
FDDI	Fiber Distributed Data Interface	Interfase de Datos Distribuida por Fibra Óptica
FDM	Frecuency Division Multiplexing	Multiplexación por División de Frecuencias
FEC	Forwarding Equivalent Class	Clase Equivalente de Envío
FRAD	Frame Relay Access Device	Dispositivo de Acceso a Frame Relay
FTP	File Transfer Protocol	Protocolo de Transferencia de Archivos
GAN	Global Area Network	Red de Área Global
GFC	Generic Flow Control	Control de Flujo Genérico
HDLC	High-level Data Link Control	Control de Enlace de Datos de Alto Nivel
HDTV	High Definition TV	Televisión de Alta Definición
HEC	Header Cheksum	Suma de Verificación de la Cabecera
HTTP	HyperText Transport Protocol	Protocolo de Transporte de Hipertexto
IDN	Integrated Digital Network	Red Digital Integrada
IEEE	Institute of Electrical and Electronics Engineers	Instituto de Ingenieros Eléctricos y Electrónicos
IETF	Internet Engineering Task Force	Fuerza de Trabajo de Ingeniería en Internet
IGP	Interior Gateway Protocol	Protocolo de Intercambio Interior
IN	Intelligent Network	Red Inteligente
INWG	Internet Working Group	Grupo de Trabajo de Redes
IP	Internet Protocol	Protocolo Internet
IPnG	IP: The Next Generation	IP: La Nueva Generación
IPSec	Internet Protocol Security	Protocolo de Seguridad de Internet
ISDN	Integrated Services Digital Network	Red Digital de Servicios Integrados
ISO	International Standards Organization	Organización Internacional de Estándares
ITU	International Telecommunication Union	Unión Internacional de Telecomunicaciones
IVR	Interactive Voice Response	Sistema Interactivo de Respuesta de Voz
IXC	Interchange Carriers	Portadoras de Intercambio
LAN	Local Area Network	Red de Área Local
LAPB	Link Access Protocol Balanced	Protocolo Equilibrado de Acceso al Enlace
LDP	Label Distribution Protocol	Protocolo de Distribución de Etiquetas
LEC	Local Exchange Carriers	Portadoras de Intercambio Local
LER	Label Edge Router	Ruteador de Etiquetas Frontera
LLC	Link Layer Control	Capa de Control de Enlace
LSP	Label Switched Path	Trayecto Conmutado por Etiquetas
LSR	Label Switching Router	Ruteador de Conmutación de Etiquetas
MAC	Medium Access Control	Control de Acceso al Medio
MAN	Metropolitan Area Network	Red de Área Metropolitana
MIB	Management Information Base	Base de Información de Administración
MII	Media Independent Interface	Interfase Independiente del Medio
MPLS	Multi Protocol Label Switching	Conmutación por Etiquetas Multiprotocolo
NFS	Network File System	Sistema de Archivo de Red
NIC	Network Interface Card	Tarjeta de Interfase de Red
NMS	Network Management Systems	Sistema de Administración de Redes
NNI	Network Network Interface	Interfase Red a Red
NNM	Network Node Management	Administración de Red a nivel Nodo
NOC	Network Operation Center	Centro de Operación de Red
NTSC	National Television Standards Committee	Comité Nacional de Estándares de Televisión
OC	Optical Carrier	Portadora Óptica
OID	Object Identifier	Identificador del Objeto
ORB	Object Request Broker	Agente de Petición de Objeto
OSI	Open System Interconnection	Sistema de Interconexión Abierto
OSPF	Open Shortest Path First	Protocolo Abierto del Primer Camino más Corto
PARC	Palo Alto Research Center	Centro de Investigación de Palo Alto
PBX	Private Branch Exchange	Centralita Privada

PC	Personal Computer	Computadora Personal
PCM	Pulse Codification Modulation	Modulación de Pulsos Codificados
PDH	Plesiochronous Digital Hierarchy	Jerarquía Digital Plesiócrona
PDN	Public Data Network	Red Pública de Datos
PDU	Protocol Data Unit	Unidad de Datos del Protocolo
PIXEL	Picture Element	Elemento de Imagen
PNNI	Private Network to Network Interface	Interfase Privada Red a Red
PSTN	Public Switched Telephone Network	Red Telefónica Pública Conmutada
PTI	Payload Type Identifier	Identificador de Tipo de Carga Útil
PVC	Permanent Virtual Circuit	Circuito Virtual Permanente
QoS	Quality of Service	Calidad de Servicio
QPSX	Queue Package Synchronous Exchange	Intercambio Síncrono de Colas de Paquetes
RFC	Request For Comments	Documento de especificaciones del IETF
RPC	Remote Procedure Call	Llamada a Procedimiento Remoto
RSVP	Resource Reservation Protocol	Protocolo de Reservación de Recursos
SAS	Single Attachment Stations	Estación de Conexión Simple
SDH	Synchronous Digital Hierarchy	Jerarquía Digital Síncrona
SIR	Sustained Information Rate	Tasa de Información Sostenida
SMDS	Switched Multimegabit Data Service	Servicio de Conmutación de Datos Multimegabits
SMI	Structure of Management Information	Estructura de Información Administrable
SNA	Systems Network Architecture	Arquitectura de Sistemas de Redes
SNMP	Simple Network Management Protocol	Protocolo Simple de Administración de Red
SONET	Synchronous Optical NETwork	Red Óptica Síncrona
SR	Speaker Recognition	Reconocimiento del Cliente
SS7	Signaling System Number 7	Sistema de Señalización Número 7
STM-1	Synchronous Transport Module-1	Modulo de Transporte Síncrono de Nivel 1
STP	Shielded Twisted Pair	Par Trenzado Apantallado
STS-1	Synchronous Transport Signal-1	Señal de Transporte Síncrono de Nivel 1
TCP	Transmission Control Protocol	Protocolo de Control de Transmisión
TDM	Frequency Division Multiplexing	Multiplexación por División en el Tiempo
ToS	Type of Service	Tipo de Servicio
TTL	Time To Live	Tiempo de Vida
TTS	Text to Speech	Síntesis de Texto Multilingüe
UDP	User Datagram Protocol	Protocolo de Datagrama de Usuario
UNI	User Network Interface	Interfase Usuario-Red
UTP	Unshielded Twisted Pair	Cable de Par Trenzado no Apantallado
VBR	Variable Bit Rate	Velocidad de Bit Variable
VC	Virtual Container	Contenedor Virtual
VCC	Virtual Channel Connection	Conexión de Canal Virtual
VCI	Virtual Channel Identifier	Identificador de Canal Virtual
VGA	Video Graphics Array	Matriz Gráfica de Video
VMS	Voice Mail System	Sistema de Correo de Voz
VNM	Virtual Network Machine	Máquina Virtual de Red
VoD	Video over Demand	Video sobre Demanda
VoFR	Voice over Frame Relay	Voz sobre Frame Relay
VP	Virtual Path	Camino Virtual
VPI	Virtual Path Identifier	Identificador de Camino Virtual
VPN	Virtual Private Network	Red Privada Virtual
VRU	Voice Response Unit	Unidad de Respuesta de Voz
WAN	Wide Area Network	Red de Área Extensa
WWW	World Wide Web	Telaraña Amplia Mundial

BIBLIOGRAFÍA

- Barba, Antoni (2001)
Gestión de Red
México: Alfaomega.
- Becker, Hal (1997)
Análisis funcional de redes de información. Enfoque estructurado del medio de comunicación de datos
México: Limusa.
- Black, Uyles (1995)
Redes de Computadores (Protocolos, normas e interfaces)
(2ª. Edición)
España: RA-MA.
- Black, Uyles (1999)
Tecnologías emergentes para redes de computadoras
(2ª. Edición)
México: Prentice Hall – Hispanoamericana, S.A.
- Caballero, José M (1998)
Redes de Banda Ancha
España: Alfaomega-marcombo.
- Cisco Systems (2002)
Archivo PDF: Interconexión de dispositivos de red Cisco
CCNA # 640-507.
- Cisco systems, Inc. (1999-2002)
Designing MPLS for ATM
Integrating MPLS with IP and ATM
Cisco MPLS Configuration guide 9.3.0.
- Comer, Douglas & Stevens, David (2000)
Interconectividad de redes con TCP/IP
Volumen II: Diseño e Implementación
(3ª. Edición)
México: Prentice-Hall.
- Gallo, Michael & Hancock, William (2002)
Comunicación entre computadoras y tecnologías de redes
México: Thomsom.
- García, J., Ferrando, S., & Piattini, M. (1997)
Redes para proceso distribuido
España: RA-MA.
- González, N. (1987)
Comunicaciones y redes de procesamiento de datos
(1ª. Edición)
México: McGraw-Hill.
- Guijarro Coloma, Luis (2000)
Redes ATM, Principios de interconexión y su aplicación
España: Alfaomega RA-MA.
- Halsall, Fred (1998)
Comunicación de datos, redes de computadoras y sistemas abiertos
(4ª. Edición)
México: Addison Wesley Longman.
- Joskowicz, José (2003)
Archivo PDF: Redes unificadas
Instituto de Ingeniería Eléctrica, Facultad de Ingeniería
(3ª. Edición)
Universidad de la República.
- Keagy, Scott (2001)
Integración de Redes de Voz y Datos
Madrid: Pearson Educación S.A.
Cisco Systems, Cisco Press.

- Ortega, Beatriz, Flores, Santiago & Almenar, Vicec (1999)
Fundamentos de la Telecomunicación
España: Universidad Politécnica de Valencia.
- Palmer, Michael J. (2001)
Redes de computadoras, una guía práctica
México: Thomson Learning.
- Pezoa, Jorge (2001)
Archivo PDF: Apuntes de redes de datos 533483
Universidad de Concepción: Facultad de Ingeniería.
- Salvucci, G & Virues, L (2003)
Archivo PDF: Voz sobre Frame Relay
Catedra: Arquitectura de redes.
- Stallings, William (2000)
Comunicaciones y redes de computadores
(6ª. Edición)
España: Prentice-Hall.
- Stallings, William (1996)
SNMP, SNMPv2 and RMON: Practical Network Management
(2ª. Edición)
Massachusetts: Addison-Wesley.
- Tanenbaum, Andrew S. (1991)
Redes de Ordenadores
(2ª. Edición)
México: Prentice-Hall Hispanoamericana, S.A.
- Tanenbaum, Andrew S. (1997)
Redes de Computadoras
(3ª. Edición)
México: Prentice-Hall Hispanoamericana, S.A.

Sitios de Internet utilizados:

- Artículos de telecomunicaciones
<http://www.consulintel.es>
- Artículos de telecomunicaciones
<http://www.rediris.com>
- Artículos de telecomunicaciones
<http://www.teleddes.org>
- Administración de redes HP
<http://www.hp.com>
- CiscoWorks
<http://www.cisco.com>
- Curso de telecomunicaciones y redes
<http://www.eveliux.com>
- Información sobre telecomunicaciones
<http://www.cft.gob.mx>
- Información sobre telecomunicaciones
<http://www.iies.es>
- Centro de Operación de Red
<http://www.noc.unam.mx>
- Tutorial y descripción técnica de TCP/IP
<http://www.ditec.um.es>