

112
31



Universidad Nacional Autónoma de México

FACULTAD DE INGENIERIA

INTEGRACION DE TECNOLOGIA ATM
EN UNA RED CORPORATIVA.

T E S I S
que para obtener el Título de
INGENIERO EN COMPUTACION
p r e s e n t a n
Luis Miguel Salcido Sánchez
José Daniel Jiménez Ventura
Elvira Beatriz Solano Palacios
Enrique Uribe Puga
Claudia Torres Pérez de León

Director de Tesis: Ing. Orlando Zaldivar Zamorategui

México, D. F.

1996



TESIS CON
FALLA DE ORIGEN

TESIS CON
FALLA DE ORIGEN



Universidad Nacional
Autónoma de México



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.

TESIS

COMPLETA

A Dios que me dio la vida

A mis Padres Luis y Evita por todo su amor y apoyo

A Gaby por todo su amor y apoyo durante las etapas más duras en mi vida

A mis hermanos Blanca y Alonso por ser una chispa de alegría en mi vida

A mis amigos a quienes siempre recordaré con cariño

A mi familia y a la familia de mi esposa por ser un ejemplo a seguir

A mi segunda familia FLAG a quienes debo todo su amor y la oportunidad para conseguir lo que hasta este momento soy y tengo

Al ingeniero Orlando por su apoyo y estímulo

A los grandes hombres que han cambiado mi vida: Cristo, mi Papa Luis, mi suegro Salvador, mis abuelos Jesús y Bruno, mis tíos Jesús, Francisco, Bruno, Rene, Beto, Arturo y Jaime, mis cuñados Conrado, Salvador, José(todos), Antonio, Jaime, mis maestros Alfredo Sánchez, Jesús Sotomayor, Alfonso Zamarripa, Eduardo Segoviano, Ramon Coahuila, Javier González, Javier Contreras (esto no le quita lo terco), Franco Galindo, Gerardo Sánchez, Luis Sánchez, Sergio Ferragut, José Luis Cerecero, Carlos Guerrero, Ulises Mejía, José González, y todos los demás.

A Red Uno por hacerme todo un Ingeniero

En especial a Gabino Salcido a quien por su inteligencia y trabajo estamos aquí

Luis M. Salcido

A mi madre que me ha apoyado incondicionalmente y ha sido un ejemplo del sacrificio y de la lucha por alcanzar lo que queremos en la vida.

A ella que a pesar de las enfermedades nunca ha perdido las ganas de vivir y de seguir luchando para salir adelante y que seguramente nunca dejará de hacerlo.

Madre, quiero decirte que nunca terminaré de agradecer todo lo que has hecho por mí y que seguiré luchando para que juntos salgamos adelante.

Quiero dedicarte este trabajo que terminado con la ayuda de mis compañeros me permitirá culminar la etapa más importante de mi vida hasta este momento.

Gracias Mamá. Te quiero.

A mi padre quien nunca ha perdido la fé en mí e igualmente se ha esforzado para que la familia salga adelante.

Papá, quiero expresarte mi cariño y agradecimiento y decirte que para mejorar nuestra relación nos hace falta platicar y así entendernos mejor.

Gracias Papá.

A Dulce Maria que me ha apoyado incondicionalmente en las etapas difíciles y que me motivó a iniciar este trabajo.

Gracias Dul.

A mis tíos Antonio y David que representan los pocos recuerdos agradables que guardo de mis demás familiares.

A Rubén y José Luis con quienes he pasado momentos muy agradables y compartido también penas y glorias.

A mis amigos de toda la vida Laura, Marisol, Julián, Felipe, Paulino, Albano, Arturo, Marco, Chepe, Saúl y a todos aquellos que no menciono por falta de tiempo pero que no por ello son menos importantes.

A mis compañeros de trabajo quienes me han brindado su amistad y tiempo.

A todos mis profesores, por tratar de transmitirme sus conocimientos.

Al Ing. Orlando Zaldivar por su apoyo en la elaboración de este trabajo.

A todos aquellos que compartan conmigo la idea de que siempre tenemos la oportunidad de ser mejores.

A todos ustedes, muchas gracias.

José Daniel Jiménez Ventura

A mis padres por su apoyo y dedicación,

A mis hermanos:

**Carlos, Martha y Jorge
por su apoyo,**

**Y en especial a mi abuelita Elpidia
por su apoyo.**

Beatriz Solano Palacios.

A mis Padres:

**Que con su apoyo y amor
sembraron el sendero
que
que estoy caminando.**

A mi Esposa e Hija:

**Que son para mi la fuente
de inspiración y energía
me alimenta día a día.**

A mis Hermanos:

**Que me han brindado
todo su apoyo, amor y
amistad**

A mis profesores:

**Que han compartido su
sabiduría y amistad**

A mis Amigos:

**Con quienes he compartido
parte de mi vida, brindándome
su comprensión y apoyo.**

ENRIQUE URIBE PUGA.

CLAUDIA TORRES PEREZ DE LEON.

AGRADECIMIENTOS

HUJO:

Por ser mi motivación mas grande de superación, por brindarme la oportunidad de realizarme en una de mis facetas como mujer y porque eres una de las personas que más quiero . . .

A PERI:

Por ser más que una MADRE HAS SIDO MI MEJOR AMIGA, por todos los momentos de dedicación, por toda la confianza que me has brindado, por el apoyo incondicional que siempre me has dado y por creer una vez más en mi . . .

A MI PAPA:

Por darme la oportunidad de poder concluir uno de los objetivos por el que luchaste y ver culminada tu obra en la educación de tus hijas . . .

A LETY:

Por apoyarme siempre en todos los momentos, por ser "mi maestra, amiga y confidente" y por enseñarme el camino

A LA PERSONA QUE ME HA BRINDADO ESTABILIDAD EMOCIONAL:

Gracias por transmitirme tus conocimientos y sabiduría en todos los ámbitos, por apoyarme incondicionalmente, por enseñarme a ser una buena madre, por mostrarme el camino para ser una buena profesionista, por estar conmigo siempre que lo necesito y por darme lo mejor de tí . . .

A OSCAR:

Por haberme apoyado y ayudado durante toda la carrera, por haberte desvelado conmigo haciendo tareas, por regalarme una parte de tu vida . . .

A TODA MI FAMILIA Y AMIGOS:

Por todo su apoyo y ayuda incondicional . . .

ESTO ES DE USTEDES !!!

Capítulo 1 Introducción

1.1 Modelo de referencia OSI	2
1.1.1 Capas del Modelo de referencia OSI	2
1.1.1.1 Capa física	2
1.1.1.2 Capa de enlace	3
1.1.1.3 Capa de red	4
1.1.1.4 Capa de transporte	4
1.1.1.5 Capa de sesión	6
1.1.1.6 Capa de presentación	7
1.1.1.7 Capa de aplicación	8
1.1.2 Transmisión de datos en el modelo OSI	9
1.1.3 Servicios	10
1.1.3.1 Terminología OSI	10
1.1.3.2 Sevicios orientados a conexión y sin conexión	12
1.1.3.2.1 Relación entre servicios y protocolos	16
1.2 Tecnología de redes de datos	17
1.2.1 Ethernet	17
1.2.1.1 Norma IEEE 802.3 y Ethernet	17
1.2.2 Token Ring	21
1.2.2.1 Formatos de tramas y tokens	22
1.2.2.2 Protocolo de control de acceso al medio	23
1.2.2.3 Monitor	26
1.2.2.4 Topología de anillo cableado en estrella	26
1.2.3 FDDI (Fiber Distributed Data Interface).	29
1.2.3.1 Fibras ópticas	29
1.2.3.2 Topología	33
1.2.3.3 Arquitectura	35
1.2.3.3.1 Capa física	36
1.2.3.4 Protocolo MAC	37
1.2.3.5 Formato de las tramas	39
1.3 Protocolos de redes de datos	41
1.3.1 Windows NT	41
1.3.1.1 Descripción general	41
1.3.1.2 Plataformas capaces de ejecutar Windows NT	43
1.3.1.3 Windows NT vs. Windows NT Advanced Server	44
1.3.1.4 Componentes de Windows NT	44
1.3.1.4.1 Productos componentes de Windows NT	44
1.3.1.4.2 Subsistemas disponibles en Windows NT	45
1.3.1.4.3 Consistente interface de usuario entre subsistemas	46
1.3.1.5 Compartiendo datos entre aplicaciones	46
1.3.1.6 Kernel vs. modos usuario	46
1.3.1.7 Capacidades de Windows NT	47
1.3.1.7.1 Multiproceso simétrico	47
1.3.1.7.2 Modelo de memoria usado por Windows NT	47
1.3.1.7.3 Uso de memoria virtual en Windows NT	47
1.3.1.8 Aspectos de seguridad en Windows NT	48
1.3.1.9 Aplicaciones de NT	50

1.3.2 NetWare	53
1.3.2.1 Descripción general	53
1.3.2.2 Sistema operativo NetWare	54
1.3.2.2.1 Software de workstation	54
1.3.2.2.2 Shell de NetWare (NETx.COM)	55
1.3.2.2.3 Opciones shell	56
1.3.2.2.4 Shell NetWare de memoria expandida (EMSNETx.EXE)	56
1.3.2.2.5 Shell NetWare de memoria extendida (XMSNETx.EXE)	56
1.3.2.2.6 Soporte workstation	57
1.3.2.3 Windows	57
1.3.2.4 Macintosh	57
1.3.2.5 Unix	57
1.3.2.6 OSI	58
1.3.2.7 Protocolos múltiples	58
1.3.2.8 Utilerías	59
1.3.2.9 Aspectos de Performance en NetWare	59
1.3.2.9.1 Procesamiento distribuido	59
1.3.2.10 CACHE del Directorio(Directory Caching)	60
1.3.2.11 Directory Hashing	61
1.3.2.12 File Caching	61
1.3.2.13 Elevator Seeking	62
1.3.2.14 Capacidades del sistema de tolerancia a errores	62
1.3.2.14.1 Proceso de verificación Read-After-Write	63
1.3.2.15 Duplicación de FATs y DETs	63
1.3.2.16 Disk Mirroring	64
1.3.2.17 Disk Duplexing	65
1.3.2.18 Transaction Tracking System	65
1.3.2.19 Monitoreo UPS	65
1.3.2.20 Especificaciones de NetWare v3.11	66
1.3.3 TCP/IP	67
1.3.3.1 Gráfica de direcciones	73
1.3.3.2 TCP	74
1.3.3.3 Encabezado TCP	75
1.3.3.4 UDP (User Datagram Protocol)	75
1.3.3.4.1 UDP Header	76
1.3.3.5 IP (Internet Protocol)	76
1.3.3.5.1 Header del datagrama IP	76
1.3.3.6 Internet Control Message Protocol (ICMP)	78
1.3.3.7 Routing Information Protocol (RIP)	79
1.3.3.7.1 Estructura del paquete RIP	81
1.4 Interconectividad de redes	81
1.4.1 Séptima capa del modelo OSI	82
1.4.1.1 Repetidores	82
1.4.2 Internetworking en la capa de enlace de datos	83
1.4.3 Conmutadores LAN	84
1.4.4 Enrutamiento en redes	85

Capítulo 2 Fundamentos de ATM.

2.1 Fibra óptica	89
2.1.1 Introducción	89
2.1.2 Lo esencial de las fibras ópticas	89
2.1.2.1 Refracción y fibra	89
2.1.2.2 Capacidad de ancho de banda de una fibra	93
2.1.3 Un ejemplo de señales de fibra óptica: SONET	93
2.1.4 SONET y el SDH	94
2.1.5 Como trabaja SONET	97
2.2 Modelo de referencia de protocolo B-ISDN	100
2.2.1 Funciones de las capas	102
2.2.2 Capa Física	103
2.2.2.1 El subnivel del medio físico (PM)	103
2.2.2.2 Funciones del subnivel del medio físico (PM)	103
2.2.2.3 Medios físicos	104
2.2.2.3.1 Estándares ANSI	105
2.2.2.3.2 CCITT/ITU-T	105
2.2.2.3.3 Foro ATM	105
2.2.2.4 Interfaces basadas en celdas	106
2.2.2.5 Funciones del subnivel de convergencia de transmisión (TC)	107
2.2.2.6 Acoplamiento de la velocidad de celdas	108
2.2.2.7 Control de error del encabezado (HEC)	108
2.2.2.8 La delimitación de las celdas	109
2.2.3 Capa ATM	111
2.2.3.1 La estructura de la celda	111
2.2.3.2 El encabezado de la celda	111
2.2.3.3 Valores pre-asignados del encabezado	112
2.2.3.4 Control de flujo genérico	112
2.2.3.5 Identificador de la ruta virtual (VPI)	112
2.2.3.6 Identificador del canal virtual (VCI)	113
2.2.3.7 Tipos de carga de pago	113
2.2.3.8 Prioridad de pérdida de celda	113
2.2.3.9 El control de error del encabezado	114
2.2.4 Capa de adaptación de ATM (AAL)	115
2.2.4.1 AAL Tipo 0	116
2.2.4.2 AAL Tipo 1	117
2.2.4.2.1 Subcapa de segmentación y reensamblaje	117
2.2.4.2.2 Subcapa de convergencia	118
2.2.4.3 AAL Tipo 2	119
2.2.4.4 AAL Tipo 3 / 4	120
2.2.4.4.1 Subcapa de segmentación y reensamblaje	121
2.2.4.4.2 Subcapa de convergencia	122
2.2.4.5 AAL Tipo 5	126
2.3 Conmutación ATM	127
2.3.1 Elementos de conmutación	127
2.3.1.1 Elementos de conmutación tipo Matriz	128
2.3.1.1.1 Buffers de entrada	130
2.3.1.1.2 Buffers de salida	131

2.3.1.1.3	Buffers de punto de cruce	132
2.3.1.1.4	Estrategias de arbitraje	132
2.3.1.2	Elemento de conmutación de memoria central	134
2.3.1.3	Elemento de conmutación tipo bus	135
2.3.1.4	Elemento de conmutación tipo anillo	136
2.3.1.5	Aspectos del rendimiento	137
2.3.1.6	Aspectos tecnológicos	138
2.3.2	Redes de conmutación	139
2.3.2.1	Redes de una etapa	139
2.3.2.1.1	Matriz de conmutación extraída	140
2.3.2.1.2	Red tipo embudo	141
2.3.2.1.3	Redes de conmutación mezclada	141
2.3.2.2	Redes mult-etapa	142
2.3.2.2.1	Redes de una ruta	142
2.3.2.2.2	Redes mult-ruta	144
2.3.2.3	Procesamiento del encabezado de celdas en la manufactura del conmutador	149
2.3.2.3.1	Elementos de conmutación de auto-ruteo	150
2.4	Señalización	151
2.4.1	Introducción	151
2.4.2	Arquitectura de protocolo para el Relase 1	153
2.4.3	Meta-Señalización	155
2.4.3.1	General	155
2.4.3.2	Aplicación y alcance	155
2.4.3.3	Resultado de los protocolos	157
2.4.3.3.1	Formateo de mensajes	157
2.4.3.3.2	Procedimientos	162
2.4.4	Capa de adaptación ATM para la señalización	163
2.4.4.1	Parte común	164
2.4.4.2	Parte de servicio específico	164
2.4.5	Protocolos de señalización para el Relase 1	168
2.4.5.1	Interface usuario-red para la señalización	169
2.4.5.2	Interface red-nodo de la señalización	173
2.4.5.2.1	Modificaciones al B-ISDN	173
2.4.5.2.2	Evolución del protocolo	176
2.4.6	Requerimientos para protocolos de señalización Relase 2	177
2.5	Protocolos de enrutamiento de ATM	179
2.5.1	P-NNI Fase 1: QoS Support	182
2.5.2	P-NNI Fase 1: Escalabilidad y alcance	187
2.6	Emulación LAN	190
2.6.1	Tipos de conexión y componentes LANE	193
2.6.2	LANE operación	196
2.6.3	Unión y registro	196
2.6.4	Transferencia de datos	197
2.6.5	BUS inteligente	198
2.6.6	LANE y redes virtuales	198
2.7	Protocolos de modo nativo	200
2.7.1	Servicios integrados	200

2.7.2 IP sobre ATM	204
2.7.2.1 Encapsulamiento de paquetes	204
2.7.2.2 Resolución de direcciones	204
2.8 Control de congestionamiento	205
2.8.1 Definición	205
2.8.2 Determinación del impacto del congestionamiento	205
2.8.3 Control del comportamiento del congestionamiento	206
2.8.4 Categorías del control de congestionamiento	209
2.8.5 Manejo del congestionamiento	211
2.8.6 Asignación de recursos	211
2.8.7 Uso de parámetros de control de descarte	212
2.8.8 Control de admisión de conexiones especificadas	212
2.8.9 Ingeniería de redes	212
2.9 Ingeniería de tráfico	213
2.9.1 Filosofía	213
2.9.1.1 Características de los parámetros de las fuentes de tráfico	213
2.9.1.2 Especificaciones y mediciones del desempeño	214
2.9.1.3 Adecuación del modelado	215
2.9.1.4 Modelos de la fuente	215
2.9.2 Parámetros generales de modelado de las fuentes	216
2.9.3 Procesos de arribo de Poisson y de Markov	216
2.9.4 Modelos de sistemas de colas	220
2.9.5 Proceso de Bernoulli y aproximación Gaussiana	223
2.9.6 Desempeño de métodos de buffer	225
2.9.7 Desempeño CBR determinístico	230
2.9.8 Tiempo de respuesta aleatorio (VBR)	231
2.9.9 Ganancia de multiplexaje estadístico	233
Capítulo 3 Planteamiento del problema.	
3.1 Antecedentes.	237
3.2 Organización y estructura.	239
3.3 Distribución física.	240
3.4 Análisis y evaluación de las redes actuales.	243
3.4.1 Generalidades.	243
3.4.2 Red empresa A.	248
3.4.3 Red empresa B.	253
3.4.4 Red empresa C.	257
3.4.5 Red empresa D.	260
3.4.6 Red de Finanzas.	263
3.4.7 Red de Administración.	266
3.4.8 Red de Recursos Humanos.	269
3.4.9 Red de Telecomunicaciones.	272
3.5 Necesidades y problemática	275

3.6	Visión a corto y mediano plazo.	275
Capítulo 4	Requerimientos de la red.	
4.1	Tipo de Red	277
4.1.1	Esquema LAN	277
4.1.1.1	Red de Conmutación Ethernet	277
4.1.1.2	Red Distribuida FDDI	282
4.1.1.3	Red ATM	287
4.1.2	Esquema WAN	292
4.1.3	Otros accesos	294
4.2	Disponibilidad de la Red	296
4.3	Monitoreo y control de la Red	298
4.4	Tráfico de la Red	299
4.4.1	Protocolos de Red	299
4.4.2	Protocolos de Enrutamiento	299
4.4.3	Protocolos de Administración de Red	299
4.5	Tiempos de conexión	300
4.6	Número de conexiones	303
4.7	Selección de la configuración de la Red	307
4.8	Interfaces	310
4.8.1	Red WAN	310
4.8.2	Red LAN	311
Capítulo 5	Análisis y Justificación de equipos.	
5.1	Justificación de equipos	313
5.1.1	Justificación de los conmutadores ATM	313
5.1.2	Justificación de los concentradores	320
5.1.3	Justificación de los enrutadores	321
5.2	Consideraciones de la instalación	326
5.2.1	Dimensionamiento de equipos	328
5.3	Inspección del sitio para montaje de estaciones	329
5.3.1	Descripción física	330
5.3.2	Instalación eléctrica	
5.3.3	Fuentes de interferencia	331
5.4	Características de los equipos	332
5.4.1	Características técnicas de enrutadores Cisco	332

5.4.1.1	Arquitectura modular	332
5.4.1.2	Capacidad de procesamiento	332
5.4.1.3	Capacidad de memoria real	332
5.4.1.4	Capacidad de memoria cache	332
5.4.1.5	Tipo de microprocesador	333
5.4.1.6	Fuente de poder	333
5.4.1.7	Procesador central	333
5.4.1.8	Servicios de conmutación de circuitos	334
5.4.1.9	Servicios de conmutación de paquetes	334
5.4.1.10	Interfaces seriales	334
5.4.1.11	Interfaces de área local (LAN)	335
5.4.1.12	Protocolos de transmisión de área extendida (Wan)	335
5.4.1.13	Protocolos de área local (LAN)	335
5.4.1.14	Protocolos de enrutamiento	336
5.4.1.15	Protocolos de administración de red	336
5.4.1.16	Seguridad	337
5.4.1.17	Puenteo	337
5.4.1.18	Soporte TCP/IP cubriendo los siguientes RFC's	338
5.4.1.19	Características de mantenimiento de TCP/IP	338
5.4.1.20	Características de soporte OSI	339
5.4.1.21	Características de soporte de Novell IPX	339
5.4.1.22	Certificado de aprobación	340
5.4.1.23	Confiabilidad	340
5.4.2	Características técnicas de los equipos Cabletron	341
5.4.2.1	Arquitectura de red	341
5.4.2.2	Características	342
5.4.2.3	Estándares de red	343
5.4.2.4	Concentradores MMAC's	343
5.4.2.5	Funciones generales	343
5.4.2.5.1	Interoperabilidad	343
5.4.2.5.2	Flexibilidad	343
5.4.2.5.3	Adaptabilidad	344
5.4.2.5.4	Modularidad	344
5.4.2.5.5	Redundancia	344
5.4.2.5.6	Capacidad de administración	345
5.4.2.6	Características	345
5.4.2.7	Descripción	345
5.4.2.8	Capacidades	348
5.4.2.9	Arquitectura del módulo de administración	348
5.4.2.9.1	Procesador RISC y960	348
5.4.2.9.2	Flash EPROMS	348
5.4.2.10	Estándares de seguridad	347
5.4.2.11	Fuentes de alimentación redundantes	347
5.4.2.12	Módulos para la administración de redes	347
5.4.2.13	Módulo repetidor multicanal Ethernet	348
5.4.2.13.1	Características	349
5.4.2.14	Módulos para redes Ethernet	349
5.4.2.15	Módulo de administración y puenteo Ethernet (EMME)	350
5.4.2.16	Módulo concentrador activo para Token Ring	350
5.4.2.17	Módulos de interface para puertos Ethernet	351
5.4.2.18	Concentradores 10 Base-T SNMP MRXI/MRXI-2	351
5.4.2.19	Concentrador 10 Base-T MRXI-24	351
5.5	Características técnicas de los conmutadores ATM de FORE	352

5.5.1 Hardware del sistema	352
5.5.2 Software del sistema	353
5.5.2.1 Software de interconectividad	353
5.5.2.2 Software de administración de red	353
5.5.3 Especificaciones generales	353
5.5.4 Conmutadores de acceso para LAN modelo ForeRunner LAX-20	354
5.5.4.1 Hardware del sistema	354
5.5.4.2 Software del sistema	355

Capítulo 6 Instalación

6.1 Esquema de la red	358
6.2 Distribución de equipos	360
6.3 Esquema de direccionamiento	362
6.4 Pruebas	370

Conclusiones	372
Glosario	375
Bibliografía	455

CAPITULO 1 INTRODUCCION

En este capítulo se proporciona una visión general de conceptos en redes, además de proporcionar los elementos teóricos que respaldan el desarrollo de los capítulos subsecuentes y brinda un panorama técnico para entender las discusiones que se abordarán posteriormente.

1. Introducción

1.1 Modelo de referencia OSI

La Organización Internacional de Normas (ISO), como un primer paso hacia la normalización internacional de varios protocolos, elaboró una propuesta cuyo modelo aparece en la figura 1.1. A este modelo se le conoce como Modelo de Referencia OSI (Interconexión de Sistemas Abiertos) de la ISO, porque precisamente se refiere a la conexión de sistemas heterogéneos es decir, a sistemas dispuestos a establecer comunicaciones con otros distintos. En forma abreviada se conoce sencillamente como modelo OSI.

El modelo OSI tiene siete capas. Los principios aplicados para el establecimiento de las siete capas fueron los siguientes:

1. Una capa se creará en situaciones donde se necesita un nivel diferente de abstracción.
2. Cada capa deberá efectuar una función bien definida.
3. La función que realizará cada capa deberá seleccionarse con la intención de definir protocolos normalizados internacionalmente.
4. Los límites de las capas deberán seleccionarse tomando en cuenta la minimización del flujo de información a través de las interfaces.
5. El número de capas deberá ser lo suficientemente grande para que funciones diferentes no tengan que ponerse juntas en la misma capa y, por otra parte, también deberá ser lo suficientemente pequeño para que su arquitectura no llegue a ser difícil de manejar.

El modelo OSI, por sí mismo, no es una arquitectura de red, dado que no especifica, en forma exacta, los servicios y protocolos que se utilizarán en cada una de las capas. Sólo indica lo que cada capa deberá hacer. Sin embargo, la ISO también ha generado normas para todas las capas, aunque éstas, estrictamente hablando, no forman parte del modelo. Cada una de ellas se ha publicado como normas internacionales independientes.

1.1.1 Capas del modelo de referencia OSI

1.1.1.1 Capa física

La capa física se ocupa de la transmisión de bits a lo largo de un canal de comunicación. Su diseño deberá asegurar que cuando un extremo envía un bit con valor 1, éste se reciba exactamente como un bit con ese valor en el otro

extremo, y no como un bit de valor 0. Preguntas comunes aquí son: cuántos voltios deberán utilizarse para representar un bit de valor 1 ó 0; cuántos microsegundos deberá durar un bit; la posibilidad de realizar transmisiones bidireccionales en forma simultánea; la forma de establecer la conexión inicial y cómo interrumpirla cuando ambos extremos terminan su comunicación; o bien, cuántas puntas terminales tiene el conector de la red y cuál es el uso de cada una de ellas. Los problemas de diseño a considerar aquí son los aspectos mecánico, eléctrico, de procedimiento de interface y el medio de transmisión física, que se encuentra bajo la capa física. Se puede considerar que el diseño de la capa física cae dentro del dominio del ingeniero eléctrico.

1.1.1.2 Capa de enlace

La tarea primordial de la capa de enlace consiste en, partir de un medio de transmisión común y corriente, y transformarlo en una línea sin errores de transmisión para la capa de red. Esta tarea la realiza al hacer que el emisor trocee la entrada de datos en tramas de datos (típicamente constituidas por algunos cientos de octetos), y las transmita en forma secuencial y procese las tramas de asentimiento, devueltas por el receptor. Como la capa física básicamente acepta y transmite un flujo de bits sin tener en cuenta su significado o estructura, recae sobre la capa de enlace la creación o reconocimiento de los límites de la trama. Esto puede llevarse a cabo mediante la inclusión de un patrón de bit especial al inicio y al término de la trama. Si estos patrones de bits pueden aparecer entre los datos, deberá tenerse un cuidado especial para evitar cualquier confusión al respecto.

La trama puede destruirse por completo debido a una ráfaga de ruido en la línea, en cuyo caso el software de la capa de enlace, perteneciente a la máquina emisora, deberá retransmitir la trama. Sin embargo, múltiples transmisiones de la misma trama introducen la posibilidad de duplicar la misma. Por ejemplo, el duplicado de una trama podría enviarse, si el acuse de recibo que regresa al receptor se hubiera destruido. Corresponde a esta capa resolver los problemas causados por daño, pérdida o duplicidad de tramas. La capa de enlace ofrece diferentes clases de servicios a la capa de red, cada uno de ellos con distinta calidad y precio.

Otro de los problemas que aparecen en la capa de enlace es el referente a cómo evitar que un transmisor muy rápido sature a un receptor muy lento. Se deberá emplear un mecanismo de regulación de tráfico que permita que el transmisor conozca el espacio de memoria que en ese momento tiene el receptor. Frecuentemente, y por conveniencia, los procedimientos de regulación de flujo y control de errores se tratan en forma conjunta.

Otra dificultad aparece cuando la línea tiene la capacidad de utilizarse para transmitir datos bidireccionalmente. El problema radica en que los asentamientos para el tráfico de A a B compiten por el uso de la línea con las tramas de datos del tráfico que va de B hacia A.

1.1.1.3 Capa de red

La capa de red se ocupa del control de la operación de la subred. Un punto de suma importancia en su diseño, es la determinación sobre cómo encaminar los paquetes del origen al destino. Las rutas podrían basarse en tablas estáticas que se encuentran "cableadas" en la red y que difícilmente podrían cambiarse. También, podrían determinarse al inicio de cada conversación, por ejemplo en una sesión de terminal. Por último, podrían ser de tipo dinámico, determinándose en forma diferente para cada paquete, reflejando la carga real de la red.

Si en un momento dado hay demasiados paquetes presentes en la subred, ellos mismos se obstruirían mutuamente y darían lugar a cuellos de botella. El control de tal congestión dependerá también de la capa de red. El software deberá saber, por lo menos, cuántos paquetes o caracteres o bits se enviaron a cada cliente, con objeto de producir información de facturación. Cuando un paquete cruza una frontera nacional con precios distintos en cada lado, el cálculo de la cuenta puede llegar a complicarse.

También pueden surgir otros problemas cuando un paquete tenga que desplazarse de una red a otra para llegar a su destino. El direccionamiento utilizado en la segunda red puede ser diferente al empleado en la primera. La segunda podría no aceptar el paquete en su totalidad, por ser demasiado grande. Los protocolos podrían ser diferentes, etcétera, la responsabilidad, para resolver problemas de interconexión de redes heterogéneas recaerá, en todo caso, en la capa de red.

En redes de difusión el problema del encaminamiento es simple, por lo cual la capa de red es normalmente muy delgada o incluso inexistente.

1.1.1.4 Capa de transporte

La función principal de la capa de transporte consiste en aceptar los datos de la capa de sesión, dividirlos, siempre que sea necesario, en unidades más pequeñas, pasarlos a la capa de red y asegurar que todos ellos lleguen correctamente al otro extremo. Además, todo este trabajo se debe hacer de manera eficiente, de tal forma que aisle la capa de sesión de los cambios inevitables a los que está sujeta la tecnología del hardware.

Bajo condiciones normales, la capa de transporte crea una conexión de red distinta para cada conexión de transporte solicitada por la capa de sesión. Si la conexión de transporte necesita un gran caudal, ésta podría crear múltiples conexiones de red, dividiendo los datos entre las conexiones de la red con objeto de mejorar dicho caudal. Por otra parte, si la creación o mantenimiento de la conexión de una red resulta costoso, la capa de transporte podría multiplexar varias conexiones de transporte sobre la misma conexión de red para reducir dicho costo. En todos los casos, la capa de transporte se necesita para hacer el trabajo de multiplexión transparente a la capa de sesión.

La capa de transporte determina qué tipo de servicio debe dar a la capa de sesión, y en último término a los usuarios de la red. El tipo más popular de conexión de transporte corresponde al canal punto a punto sin error, por medio del cual se entregan los mensajes en el mismo orden en el que fueron enviados. Sin embargo, el transporte de mensajes aislados sin garantizar el orden de distribución y la difusión de mensajes a destinos múltiples es otra posibilidad de servicio de transporte. El tipo de servicio se determina cuando se establece la conexión.

La capa de transporte es una capa del tipo origen-destino o extremo a extremo. Es decir, un programa en la máquina origen lleva una conversación con un programa parecido que se encuentra en la máquina destino, utilizando las cabeceras de los mensajes y los mensajes de control. Los protocolos, de las capas inferiores, son entre cada máquina y su vecino inmediato, y no entre las máquinas origen y destino, las cuales podrían estar separadas por muchos IMPs (procesadores de intercambio de mensajes). En la figura 1.1 se ilustra la diferencia entre las capas 1 a 3, que están encadenadas, y las capas 4 a 7, que son de extremo a extremo.

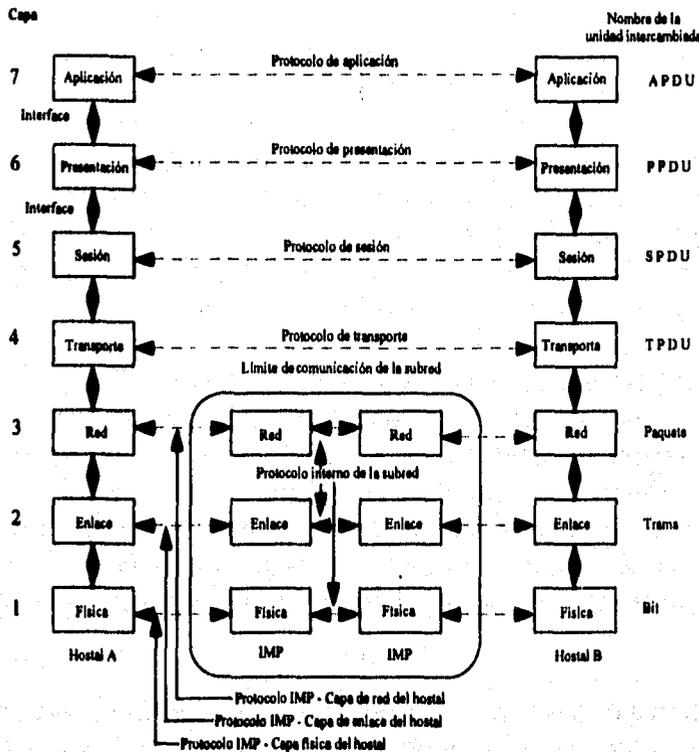


Figura 1.1

Algunos hosts son de multiproceso, lo cual implica que múltiples conexiones estarán entrando y saliendo en cada uno de ellos. Se necesita alguna forma para decir qué mensaje pertenece a qué conexión. La cabecera de transporte, es un lugar en donde puede colocarse esta información.

Además de multiplexar varios flujos de mensaje en un canal, la capa de transporte debe ocuparse del establecimiento y liberación de conexiones a través de la red. Esto requiere algún mecanismo de denominación, de tal forma que un proceso en una máquina tenga una manera para describir con quién desea conversar. También debe haber un mecanismo para regular el flujo de información, de manera que un host muy rápido no pueda desbordar a otro menos rápido.

1.1.1.5 Capa de sesión

La capa de sesión permite que los usuarios de diferentes máquinas puedan establecer sesiones entre ellos. A través de una sesión se puede llevar a cabo un transporte de datos ordinario, tal y como lo hace la capa de transporte, pero mejorando los servicios que ésta proporciona y que se utilizan en algunas aplicaciones. Una sesión podría permitir al usuario acceder a un sistema de tiempo compartido a distancia, o transferir un archivo entre dos máquinas.

Uno de los servicios de la capa de sesión consiste en gestionar el control de diálogo. Las sesiones permiten que el tráfico vaya en ambas direcciones al mismo tiempo, o bien, en una sola dirección en un instante dado. Si el tráfico sólo puede ir en una dirección en un momento dado, la capa de sesión ayudará en el seguimiento de quien tiene el turno.

La administración del testigo es otro de los servicios relacionados con la capa de sesión. Para el caso de algunos protocolos resulta esencial que ambos lados no traten de realizar la misma operación en el mismo instante. Para manejar estas actividades, la capa de sesión proporciona testigos que pueden ser intercambiados. Solamente el extremo con el testigo puede realizar la operación crítica.

Otro de los servicios de la capa de sesión es la sincronización. Considérense, por ejemplo, los problemas que podrían ocurrir cuando se trata de hacer una transferencia de archivos de dos horas entre dos máquinas en una red con un tiempo medio de una hora entre caídas. Después de abortar cada archivo, la transferencia completa tendría que iniciarse de nuevo con la siguiente caída de red. Para eliminar este problema, la capa de sesión proporciona una forma para insertar puntos de verificación en el flujo de datos, con objeto de que, después de cada caída, solamente tengan que repetirse los datos que se encuentren después del último punto de verificación.

1.1.1.6 Capa de presentación

La capa de presentación realiza ciertas funciones que se necesitan a menudo como para buscar una solución general para ellas, más que dejar que cada uno de los usuarios resuelva los problemas. En particular y, a diferencia de las capas inferiores, que únicamente están interesadas en el movimiento fiable de bits de un lugar a otro, la capa de presentación se ocupa de los aspectos de sintaxis y semántica de la información que transmite.

Un ejemplo típico de servicio de la capa de presentación es el relacionado con la codificación de datos conforme a lo acordado previamente. La mayor parte de los programas de usuario no intercambian ristas de bits binarios aleatorios, sino, más bien, cosas como nombres de personas, datos, cantidades de dinero y facturas. Estos artículos están representados por ristas de caracteres, números enteros, números de punto flotante, así como por estructuras de datos constituidas por varios elementos más sencillos. Las computadoras pueden tener diferentes códigos para representar las ristas de caracteres (por ejemplo, ASCII y EBCDIC), enteros (por ejemplo, complemento a uno o complemento a dos), etcétera. Para posibilitar la comunicación de computadoras con diferentes representaciones, la estructura de los datos que se van a intercambiar puede

definirse en forma abstracta, junto con una norma de codificación que se utilice en el "cable". El trabajo de manejar estas estructuras de datos abstractas y la conversión de la representación utilizada en el interior de la computadora a la representación normal de la red, se lleva a cabo a través de la capa de presentación.

La capa de presentación está relacionada también con otros aspectos de representación de la información. Por ejemplo, la compresión de datos se puede utilizar aquí para reducir el número de bits que tienen que transmitirse, y el concepto de criptografía se necesita utilizar frecuentemente por razones de privacidad y autenticación.

1.1.1.7 Capa de aplicación

La capa de aplicación contiene una variedad de protocolos que se necesitan frecuentemente. Por ejemplo, hay centenares de tipos de terminales incompatibles en el mundo. Considérese la situación de un editor orientado a pantalla que desea trabajar en una red con diferentes tipos de terminales, cada uno de ellos con distintas formas de distribución de pantalla, de secuencias de escape para insertar y borrar texto, de movimiento de cursor, etc.

Una forma de resolver este problema consiste en definir una terminal virtual de red abstracta, con la que los editores y otros programas pueden ser escritos para tratar con ella. Con objeto de transferir funciones de la terminal virtual de una red a una terminal real, se debe escribir un software que permita el manejo de cada tipo de terminal. Por ejemplo, cuando el editor mueve el cursor de la terminal virtual al extremo superior izquierdo de la pantalla, dicho software deberá emitir la secuencia de comandos apropiados para que la terminal real ubique su cursor en el sitio indicado. El software completo de la terminal virtual se encuentra en la capa de aplicación.

Otra función de la capa de aplicación es la transferencia de archivos. Distintos sistemas de archivo tienen diferentes convenciones para denominar un archivo, así como diferentes formas para representar las líneas de texto, etcétera. La transferencia de archivos entre dos sistemas diferentes requiere de la solución de éstas y de otras incompatibilidades. Este trabajo, así como el correo electrónico, la entrada de trabajo a distancia, el servicio de directorio y otros servicios de propósito general y específico, también corresponden a la capa de aplicación.

1.1.2 Transmisión de datos en el modelo OSI

En la figura 1.2 se muestra un ejemplo de cómo pueden transmitirse los datos mediante el empleo del modelo OSI. El proceso emisor tiene algunos datos que desea enviar al proceso receptor. Este entrega los datos a la capa de aplicación, la cual añade entonces la cabecera de aplicación, *AH* (la cual puede ser nula), a la parte delantera de los mismos y entrega el elemento resultante a la capa de presentación.

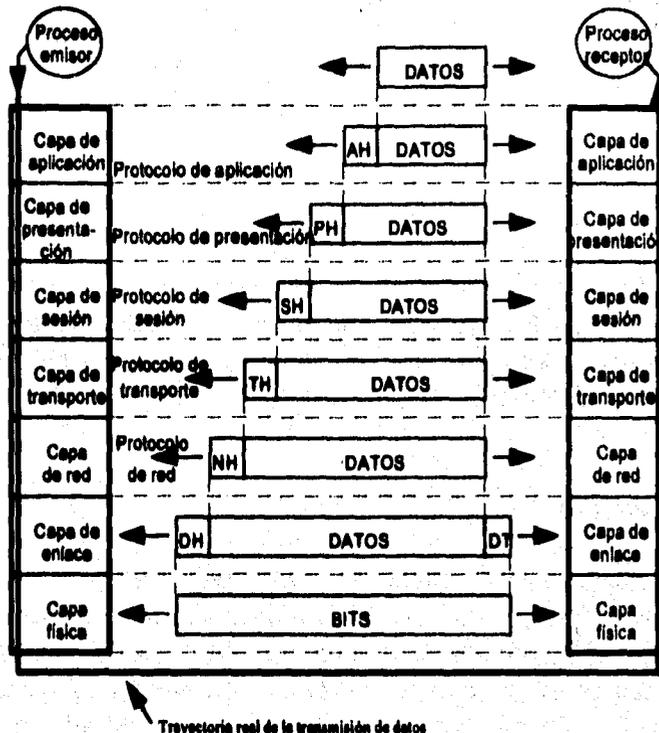


Figura 1.2

La capa de presentación transforma este elemento de diferentes formas, con la posibilidad de incluir una cabecera en la parte frontal, dando el resultado a la capa de sesión. Es importante observar que la capa de presentación no sabe qué parte de los datos que le dió la capa de aplicación, corresponden a *AH*, y cuáles son los que corresponden a los verdaderos datos del usuario. Ni debería saberlo.

Este proceso se sigue repitiendo hasta que los datos alcanzan la capa física, lugar en donde efectivamente se transmiten a la máquina receptora. En la otra máquina, se van quitando una a una las cabeceras, a medida que los datos se transmiten a las capas superiores, hasta que finalmente llegan al proceso receptor.

La idea fundamental, a lo largo de este proceso, es que si bien la transmisión efectiva de datos es vertical, como se muestra en la figura anterior, cada una de las capas está programada como si fuera una transmisión horizontal. Cuando la capa de transporte emisora obtiene, por ejemplo, un mensaje de la capa de sesión le asigna una cabecera de transporte y lo envía a la capa de transporte receptora. Desde el punto de vista de esta capa, el hecho de que debe realmente entregar el mensaje a la capa de red de su propia máquina, es un detalle técnico sin importancia. Una analogía de este hecho es, por ejemplo, cuando un diplomático de habla *Uighur* se dirige a las Naciones Unidas, piensa como si estuviera dirigiéndose personalmente a los otros diplomáticos ahí congregados.

El hecho de que le esté hablando sólo a su traductor, se ve como un simple detalle técnico.

1.1.3 Servicios

La verdadera función de cada una de las capas OSI consiste en proporcionar servicios a las capas superiores. A continuación se verá con mayor detalle, qué es un servicio, pero primero se dará una breve información sobre la terminología empleada en el modelo OSI.

1.1.3.1 Terminología OSI

Se llaman entidades a los elementos activos que se encuentran en cada una de las capas. Las entidades pueden ser software (como un proceso), o hardware (como un chip inteligente de E/S). Las entidades de la misma capa, pero de diferentes máquinas, se conocen como entidades pares o iguales. A las entidades de la capa 7 se les conoce como entidades de aplicación; a las de la capa 6 como entidades de presentación, etcétera.

Las entidades de la capa N desarrollan un servicio que utiliza la capa $(N+1)$, en este caso a la capa N se le denomina proveedor del servicio y a la capa $(N+1)$ usuario del servicio. La capa N puede utilizar los servicios de la capa $(N-1)$ con objeto de proporcionar su servicio. El servicio que ofrece puede ser de varias clases, por ejemplo, una comunicación rápida y costosa, o bien, una comunicación lenta y económica.

Los servicios se encuentran disponibles en el SAP (Punto de Acceso al Servicio). Los SAP de la capa N son los lugares en donde la capa $(N+1)$ puede acceder a los servicios que se ofrecen. Cada uno de los SAP tiene una dirección que lo identifica de forma particular. Para aclarar este punto, los SAP en el sistema telefónico son los enchufes en los que se conectan los teléfonos y las direcciones de los SAP son los números telefónicos correspondientes a dichos enchufes. Para

poder llamar a alguien, se debe conocer la dirección de su SAP. En el sistema postal, de manera análoga, las direcciones de los SAP son las direcciones de las calles y de las oficinas postales. Para poder enviar una carta, se debe conocer la dirección del SAP del destinatario. En el sistema UNIX de Berkeley, los SAP son los enchufes y las direcciones de los SAP son los números de los enchufes.

Para que se lleve a cabo el intercambio de información entre dos capas, deberá existir un acuerdo sobre un conjunto de reglas acerca de la interface. En una interface típica, la entidad de la capa ($N+1$) pasa una IDU (Unidad de Datos de la Interface) a la entidad de la capa N , a través del SAP, como se muestra en la figura 1.3. El IDU consiste en una SDU (Unidad de Datos del Servicio) y de alguna información de control. La SDU es la información que se pasa, a través de la red, a la entidad par y posteriormente a la capa ($N+1$). La información de control es necesaria porque ayuda a que las capas inferiores realicen su trabajo (por ejemplo, el número de bytes en el SDU), pero no forma parte de los datos.

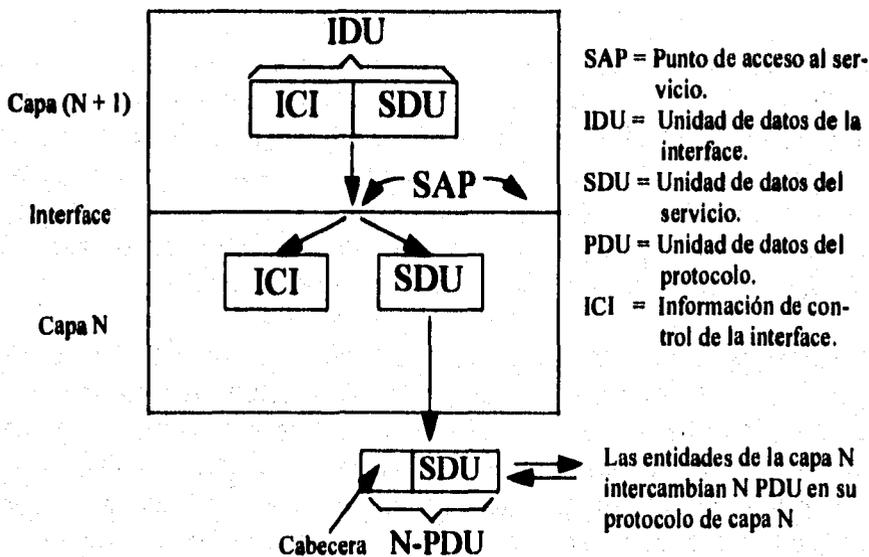


Figura 1.3

Para hacer la transferencia de una SDU, podrá ser necesario su fragmentación por parte de la entidad de la capa N en varias partes, de tal forma que a cada una de ellas se le asigne una cabecera y se envíe como una PDU (Unidad de Datos del Protocolo) distinta. Las entidades pares utilizan las cabeceras de la PDU para llevar a cabo su protocolo de igual a igual. Por medio de ellos se identifica cuáles son las PDU que contienen datos y cuáles las que llevan información de control; además, proveen la secuencia numérica y las cuentas, etc. Con frecuencia a las PDU de transporte, sesión y aplicación se les conoce como TPDU (Unidad de Datos del Protocolo de Transporte), SPDU (Unidad de Datos del Protocolo de Sesión) y APDU (Unidad de Datos del Protocolo de Aplicación), respectivamente. No es muy común oír hablar de los tipos de PDU.

1.1.3.2 Servicios, orientados a conexión y sin conexión

Las capas pueden ofrecer dos tipos de diferentes servicios a las capas que se encuentran sobre ellas: uno orientado a conexión y otro sin conexión.

El servicio orientado a la conexión se modeló basándose en el sistema telefónico. Para poder hablarle a alguien se debe tomar el teléfono, marcar el número, hablar y colgar. Similarmente, para utilizar una red con servicio orientado a conexión, el usuario del servicio establece primero una conexión, la utiliza y después termina la conexión. El aspecto fundamental de la conexión es que actúa en forma parecida a la de un tubo: el que envía, introduce objetos por un extremo, y el receptor los recoge, en el mismo orden por el otro extremo.

A diferencia de esto, el servicio sin conexión se modela con base en el sistema postal. Cada mensaje (carta), lleva consigo la dirección completa de destino y cada uno de ellos se encamina, en forma independiente, a través del sistema. Normalmente, cuando dos mensajes se envían al mismo destino, el primero que se envíe será el primero en llegar. Es posible, sin embargo, que el primero que se envíe sufra un retardo y llegue antes el que se envió en segundo lugar. Con un servicio orientado a conexión es imposible que suceda esto.

Cada servicio se caracteriza por la calidad del servicio; algunos de ellos son fiables en la medida que nunca pierden la información que transportan. Por lo general, un servicio fiable se realiza haciendo que el receptor notifique haber recibido cada mensaje, para que el transmisor esté seguro de que su mensaje llegó a destino. El proceso de notificación introduce un exceso de tráfico y retardos, que a menudo son convenientes, pero también son algunas veces indeseables.

La transferencia de archivos es una situación típica en la que es deseable y apropiado tener un servicio orientado a conexión fiable. El propietario de un archivo quiere tener la seguridad de que todos los bits lleguen correctamente y en el mismo orden en el que se enviaron. Muy pocos clientes preferirían un servicio que, aun cuando lo hiciera con mucha rapidez, ocasionalmente mezclara en forma desordenada o perdiera la información de algunos bits durante la transferencia de archivos.

El servicio orientado a conexión fiable tiene dos variantes mínimas: secuencia de mensajes y flujo de octetos. En la primera de ellas, se mantienen los límites del mensaje. Cuando se envían dos mensajes de 1K, éstos llegan como dos mensajes distintos de 1K, y nunca como un mensaje de 2K. En la segunda

variante, la conexión es simplemente un flujo de octetos sin límites de mensaje. Cuando llegan al receptor 2K octetos, no hay manera de saber si se enviaron como un mensaje de 2K, dos mensajes de 1K o 2048 mensajes de un octeto. Si las páginas de un libro se enviaran por una red, para una composición fotográfica, como mensajes separados, podría ser importante mantener los límites del mensaje. Por otra parte, con una terminal accediendo a un sistema remoto de tiempo compartido, lo único que se necesita es el flujo de octetos de la terminal a la computadora.

Como se mencionó antes, en algunas aplicaciones no se pueden aceptar los retardos introducidos por el proceso de asentimientos; una de éstas es el tráfico de voz digitalizada. Para los usuarios del teléfono resulta preferible oír un bit de ruido en una línea o una palabra mutilada de cuando en cuando, en lugar de introducir un retardo esperando una señal de acuse de recibo.

No todas las aplicaciones necesitan conexiones; por ejemplo, a medida que el correo electrónico llegue a ser más común ¿podría retrasarse el correo electrónico de mensajes basura? Probablemente el emisor de este tipo de correo no desee tener problemas para establecer y posteriormente romper una conexión, sólo para enviar un mensaje. Tampoco es esencial tener un envío 100% fiable, especialmente si eleva su costo. Todo lo que se necesita, a fin de cuentas, es un medio de envío de mensajes sencillo que tenga una alta probabilidad, pero no una garantía de alcanzar su destino. Un servicio sin conexión que no es fiable (es decir, que no tenga asentimientos), se conoce con frecuencia como servicio datagrama, por analogía con el servicio de telegramas, el cual tampoco proporciona acuse de recibo de la información al emisor.

En algunas situaciones convendría no tener que establecer una conexión para enviar un mensaje pequeño, pero sí sería fundamental que el proceso sea fiable. Para estas aplicaciones se proporcionaría el servicio de datagramas con asentimientos de información, cuyo servicio es parecido al enviar una carta certificada y solicitar un acuse de recibo. Cuando éste regresa, el emisor está completamente seguro de que la carta se entregó a la persona interesada. Otro servicio alternativo es el servicio de pregunta/respuesta, en el que la persona que envía, transmite un datagrama sencillo que contiene una solicitud, la contestación contiene una respuesta (primitiva de servicio). Un servicio está formalmente especificado por un conjunto de primitivas (operaciones), a disposición de todos los usuarios de otras unidades para acceder el servicio. Estas primitivas le indican al servicio que debe efectuar una acción o notifican la acción tomada por una entidad par. Como se muestra en la figura 1.4, las primitivas de servicio en el modelo OSI pueden dividirse en cuatro clases.

Solicitud	Una entidad desea que el servicio realice un trabajo
Indicación	Una entidad es informada acerca de un evento
Respuesta	Una entidad desea responder a un evento
Confirmación	Una entidad va a ser informada acerca de una solicitud

Figura 1.4

La primera clase de primitiva es la primitiva *petición o solicitud (request)*. Esta se utiliza para que un trabajo se realice, por ejemplo, establecer una conexión o enviar datos. Una vez que se ha efectuado el trabajo, se le avisa a la entidad corresponsal mediante la primitiva *indicación (indication)*. Por ejemplo, después de una *petición de conexión (CONNECT.request)*, en notación OSI, la entidad que se está direccionando obtiene una indicación de *conexión (CONNECT.indication)* con la cual se le anuncia que alguien desea establecer una conexión con ella. La entidad que recibió la *CONNECT.indication* utiliza entonces la primitiva *respuesta de conexión (CONNECT.response)* para decir si acepta o rechaza la conexión propuesta. En cualquier caso, la entidad que emite la *CONNECT.request* inicial, sabe lo que pasó a través de la primitiva *confirmación de la conexión (CONNECT.confirm)*. Las primitivas pueden tener parámetros y, efectivamente, la mayoría los tiene. Los parámetros para una *CONNECT.request* podrían especificar la máquina a la que se va a conectar, el tipo de servicio que se desea, así como el tamaño máximo del mensaje utilizado en la conexión. Los parámetros de una *CONNECT.indication* podrían contener la identidad de "él que llama", el tipo de servicio que se desea y el tamaño máximo del mensaje propuesto. Si la entidad llamada no está de acuerdo con el tamaño máximo del mensaje propuesto, podría hacer una contrapropuesta en su primitiva de respuesta, la cual estaría a disposición de "él que llamó" originalmente en la primitiva de confirmación. Los detalles de esta negociación son parte del protocolo. En caso de existir dos propuestas en conflicto sobre el tamaño máximo del mensaje, por ejemplo, el protocolo podría especificar que siempre que suceda esto se escogerá aquella que tenga el menor costo. Haciendo un paréntesis en la terminología, el modelo OSI evita cuidadosamente el empleo de los términos "abre una conexión" y "cierra una conexión", porque, para los ingenieros eléctricos un "circuito abierto" es aquel que tiene una abertura o separación, y la electricidad sólo puede fluir por "circuitos cerrados". Los científicos en computadoras nunca estarían de acuerdo en tener la

información fluyendo en circuito cerrado. Para mantener ambas partes en paz, los términos oficiales al respecto son "establece una conexión" y "libera una conexión", respectivamente.

Los servicios pueden ser confirmados o no confirmados. En un servicio confirmado, hay una *petición*, una *indicación*, una *respuesta* y una *confirmación*. En un servicio sin confirmar, solamente hay una *petición* y una *indicación*. La expresión **CONNECT** siempre considerará un servicio confirmado, porque el corresponsal remoto deberá estar de acuerdo en establecer una conexión. Por otra parte, la transferencia de datos puede ser confirmada o sin confirmar, dependiendo de si el emisor necesita o no tener un acuse de recibo de la información. En las redes se utilizan los dos tipos de servicio. Para tener una idea más concreta del concepto de servicio, considérese un ejemplo sencillo con servicio orientado a conexión, con ocho primitivas de servicio definidas de la siguiente manera:

1. **CONNECT.request** - Solicitud para establecer una conexión.
2. **CONNECT.indication** - Aviso de llamada a la entidad solicitada.
3. **CONNECT.response** - Utilizada por la entidad corresponsal como un medio para para aceptar/rechazar las llamadas.
4. **CONNECTION.confirm** - Notifica al que llama si la llamada fue aceptada.
5. **DATA.request** - Solicitud para que se envíen los datos.
6. **DATA.indication** - Aviso de la llegada de datos.
7. **DISCONNECT.request** - Solicitud para liberar la conexión.
8. **DISCONNECT.indication** - Aviso al llamado acerca de la solicitud de desconexión.

En este ejemplo, **CONNECT** es un servicio confirmado (es decir, necesita una respuesta explícita), en tanto que **DISCONNECT** es un servicio sin confirmar (no es necesario tener respuesta). Podría ser de utilidad hacer una analogía con el sistema telefónico, para observar la manera como se emplean estas primitivas. Considérense, por ejemplo, los pasos necesarios para llamar por teléfono a la tía Laura e invitarla a comer a la casa:

1. **CONNECT.request** - Marcar el número telefónico de la tía Laura.
2. **CONNECT.indication** - Su teléfono suena.
3. **CONNECT.response** - Ella descuelga el teléfono.
4. **CONNECT.confirm** - Usted escucha que terminó de sonar.
5. **DATA.request** - Usted le hace la invitación.
6. **DATA.indication** - Ella escucha su invitación.
7. **DATA.request** - Ella contesta que efectivamente le gustaría ir.
8. **DATA.indication** - Usted escucha su aceptación.
9. **DISCONNECT.request** - Usted cuelga el teléfono.
10. **DISCONNECT.indication** - Ella oye que usted colgó y cuelga también.

En la figura 1.5 se muestra la misma secuencia de pasos como una serie de primitivas de servicio, incluyendo la confirmación de desconexión final. Cada uno de los pasos toma en cuenta una interacción entre dos capas en una de las computadoras. Cada una de las *peticiones* o *respuestas* genera una *indicación* o *confirmación* en el otro extremo, un instante después. En este ejemplo, los usuarios del servicio (usted y la tía Laura) están en la capa (N+1) y el proveedor del servicio (el sistema telefónico) está en la capa N.

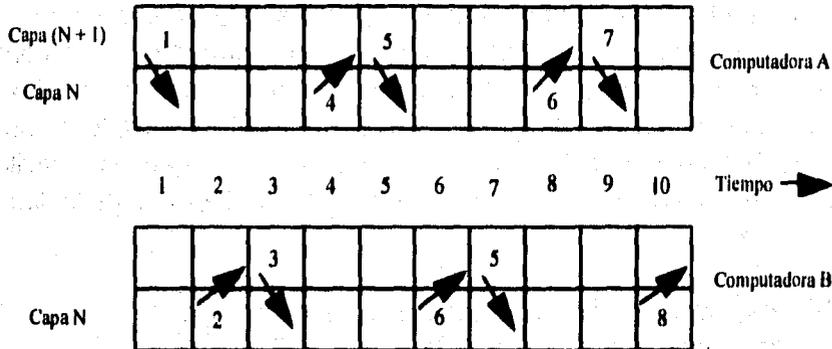


Figura 1.5

1.1.3.2.1 Relación entre servicios y protocolos

Los conceptos de servicio y protocolo tienen un significado diferente, a pesar de que con frecuencia se les confunde. Un *servicio* es un conjunto de primitivas (operaciones) que una capa proporciona a la capa superior. El servicio define las operaciones que la capa efectuará en beneficio de sus usuarios, pero no dice nada respecto a cómo se realizan dichas operaciones. Un servicio se refiere a una interface entre dos capas, siendo la capa inferior la que provee el servicio y la capa superior la que utiliza el servicio. Un *protocolo*, a diferencia del concepto de servicio, es un conjunto de reglas que gobiernan el formato y el significado de las tramas, paquetes o mensajes que son intercambiados por las entidades corresponsales dentro de una capa. Las entidades utilizan protocolos para realizar sus definiciones de servicio, teniendo libertad para cambiar el protocolo, pero asegurándose de no modificar el servicio visible a los usuarios. De esta manera, se observa con claridad cómo los conceptos de servicio y protocolo están completamente desacoplados. Sería conveniente hacer una analogía con los lenguajes de programación. Un servicio es como un tipo de datos abstracto que define las operaciones que pueden efectuarse sobre un objeto, pero no especifica la manera como se realizan estas operaciones. Un protocolo se relaciona con la *realización* de un servicio y, como tal, no es visible para el usuario del servicio.

1.2 Tecnología de redes de datos

1.2.1 Ethernet

1.2.1.1 Norma IEEE 802.3 y Ethernet

La IEEE ha producido varias normas para las redes tipo LAN. A estas normas se les conoce, en forma colectiva, como IEEE 802, en las que se incluyen as correspondientes a CSMA/CD, paso de testigo en bus y paso de testigo en anillo. Estas normas difieren en la capa física y la subcapa MAC, pero resultan compatibles en la capa de enlace. Las normas IEEE 802 han sido adoptadas por el ANSI (Instituto Nacional Americano de Normalización) como una norma nacional americana, por la NBS (Oficina Nacional de Normas) como una norma gubernamental y por la ISO (Organización Internacional de Normas) como una norma internacional (conocida como ISO 8802).

Las normas se dividen en partes, cada una de ellas publicada como un manual separado. La norma 802.1, da una instrucción al conjunto de normas y define las primitivas de interface. La norma 802.2 describe la parte superior de la capa de enlace, que utiliza el protocolo LLC (Control lógico de enlace). Las partes 802.3 a 802.5, describen las tres normas para las redes tipo LAN; es decir, las normas CSMA/CD, paso de testigo en bus y paso de testigo en anillo respectivamente. Cada norma cubre los protocolos de la capa física y la subcapa MAC.

La norma IEEE 802.3 se utiliza en las redes tipo LAN con protocolo 1-persistente CSMA/CD. Para revisar esta idea, recuérdese que cuando una estación desea transmitir, escucha la información que fluye a través del cable. Si el cable se encuentra ocupado, la estación espera hasta que esté inactivo, en caso contrario transmite de inmediato. Si dos o más estaciones, en forma simultánea comienzan a transmitir a través de un cable inactivo, generan una colisión. Estas estaciones, terminarán su transmisión, esperarán un tiempo aleatorio y repetirán de nuevo todo el proceso.

La norma 802.3 tiene una historia interesante. Su inicio verdadero se debió al sistema ALOHA, desarrollado por Abramson en Hawaii. A esta primera versión, se le incluyó la detección de portadora, y la compañía Xerox construyó un sistema CSMA/CD de 2.94 Mbps, para conectar hasta 100 estaciones personales de trabajo en un cable de 1 km de longitud. A este sistema se le llamó Ethernet, en honor del *éter luminífero*, a través del cual se pensó alguna vez que se propagaban las ondas electromagnéticas.

La Ethernet desarrollada por Xerox tuvo tanto éxito, que las compañías Xerox, DEC e Intel propusieron una norma para la Ethernet de 10 Mbps, la cual

constituyó la base para la 802.3. La norma que se publicó como la 802.3 difiere de la especificación correspondiente a la Ethernet en el sentido de que describe una familia completa de sistemas 1-persistente CSMA/CD operando a velocidades que van desde 1 a 10 Mbps, en varios medios físicos. La norma inicial también da los parámetros para un sistema de banda de base de 10 Mbps, utilizando un cable coaxial de 50 ohms. Otros conjuntos de parámetros correspondientes a diferentes medios físicos y velocidades, se encuentran en estudio en la actualidad. El estudio que se presenta a continuación se concentrará en la versión de la banda de base a 10 Mbps.

Mucha gente (incorrectamente) utiliza el nombre de "Ethernet" en un sentido genérico, para referirse a todos los protocolos CSMA/CD, aun cuando éste sólo se refiere a un producto específico que desarrolla el 802.3.

Dado que si el nombre de "Ethernet" se refiere al cable (es decir, el éter), iniciaremos este estudio con dicho concepto. Hay dos tipos de cable coaxial que se utilizan comúnmente conocidos como "Ethernet grueso" y "Ethernet delgado". El Ethernet grueso es de color amarillo, con unas marcas que se encuentra cada 2.5 m, con objeto de indicar los lugares en donde van los conectores (la norma 802.3 en realidad no necesita que el cable sea amarillo, pero sugiere que así sea). El Ethernet delgado es más pequeño y más flexible, y utiliza conectores tipo BNC común y corriente para formar uniones en T, en lugar de usar los otros conectores. Este también, es mucho más económico, pero sólo puede utilizarse para distancias cortas. Los dos tipos de cable son compatibles y pueden conectarse en diferentes formas. En ciertas aplicaciones, y bajo algunas condiciones restrictivas, el par de cable trenzado puede llegar a emplearse en lugar del cable coaxial.

Todos los desarrollos hechos con la 802.3, incluyendo a Ethernet, utilizan directamente la codificación Manchester, como se muestra en la figura 1.6.

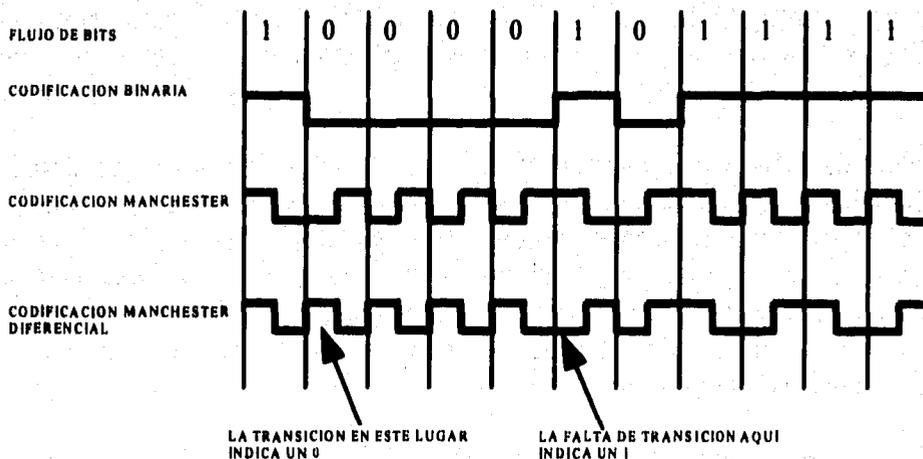


Figura 1.6

Gracias a la presencia de una transición en la parte media de cada bit, es posible hacer que el receptor se sincronice con el emisor. En cualquier instante, el cable puede estar en alguno de los tres estados siguientes: transmitiendo un bit 0 (señal baja seguida por una alta), transmitiendo un 1 (señal alta seguida de una baja), o bien, en un estado inactivo (0 volts). La señal alta tiene un valor de +0.85 volts, en tanto que la señal baja es de -0.85 volts, dando un valor de 0 volts de cc.

En la figura 1.7 se muestra la configuración usual de Ethernet, en ella puede identificarse un transceptor que se encuentra sujeto al cable en forma segura, de tal manera que su conector haga contacto con el núcleo interior. El transmisor-receptor contiene la electrónica necesaria para poder manejar la detección por portadora y de colisión. Cuando se detecta una colisión, el transmisor-receptor también coloca una señal especial de invalidación en el cable, para asegurar que todos los demás transmisores receptores tengan conocimiento de que ha ocurrido una colisión.

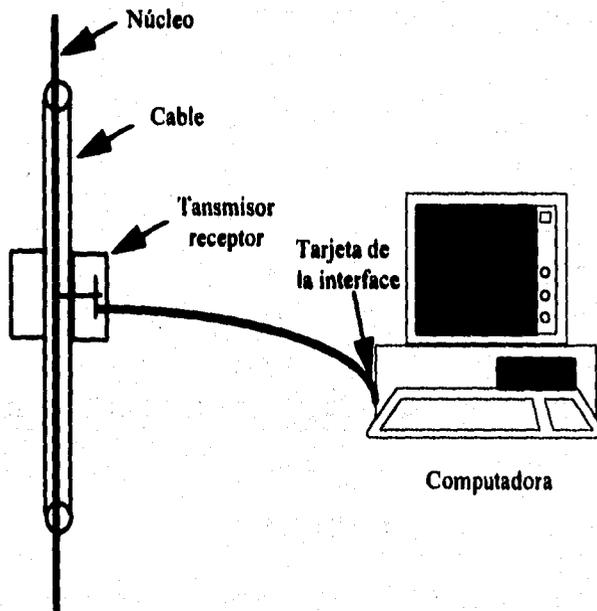


Figura 1.7

Un cable de un transmisor-receptor conecta el transmisor-receptor a una tarjeta de interface en la computadora. El cable transmisor-receptor puede llegar a tener una longitud de hasta 50 metros, y contiene cinco pares de cables trenzados individualmente aislados. Dos pares están dedicados a los datos de entrada y salida, en tanto que el quinto par, que no siempre se utiliza, permite que la computadora alimente a los circuitos electrónicos del transmisor-receptor. Algunos transmisores-receptores son capaces de tener hasta ocho computadoras periféricas conectadas a ellos, con objeto de reducir el número de transmisores-receptores necesarios.

El cable del transmisor-receptor termina en la tarjeta de la interface, localizada en el interior de la computadora. Esta tarjeta de interface contiene un chip controlador que transmite y recibe tramas hacia y desde el transmisor-receptor, respectivamente. El controlador es responsable de ensamblar los datos de información en el formato propio de la trama, así como de calcular los códigos de redundancia de las tramas de salida, y la verificación de ellos en las tramas de entrada. Algunos chips controladores también manejan un conjunto común de memorias temporales dedicadas a las tramas de entrada, una cola de memorias temporales a ser transmitidas, transferencias DMA con las computadoras host y algunos otros aspectos relacionados con la administración de la red.

La longitud máxima permitida para un cable 802.3 es de 500 metros. Para hacer que la red se extienda sobre una distancia mayor, es necesario utilizar múltiples cables, conectados mediante repetidores, como se muestra en la figura 1.8.

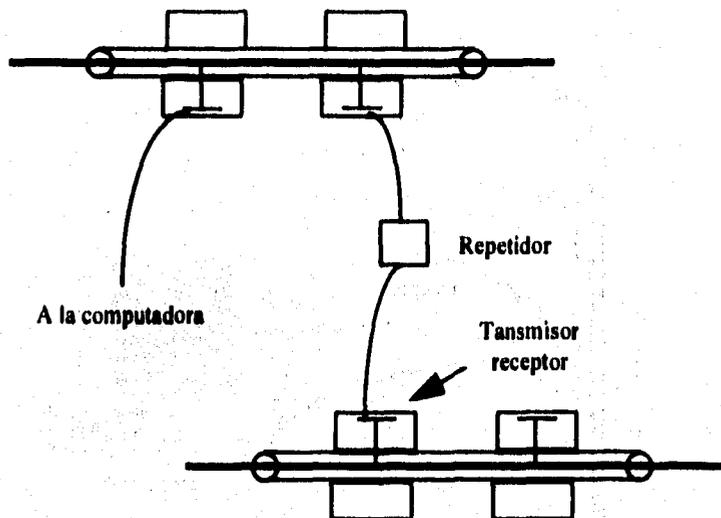


Figura 1.8

Un repetidor es un dispositivo de la capa física, el cual se encarga de recibir, amplificar y transmitir señales en ambas direcciones. Por lo que se refiere al software, una serie de cables conectados con repetidores, no es diferente a un solo cable. Un sistema puede estar constituido por varios segmentos de cable y varios repetidores, pero no es posible que más de dos transmisores-receptores se encuentren separados por una distancia mayor de 2.5 km, ni tampoco es posible que exista una trayectoria entre dos transmisores-receptores, que atraviese más de cuatro repetidores.

1.2.2 Token Ring

Una red local con topología de anillo está integrada por un conjunto de estaciones conectadas en serie, por medio de enlaces (unidireccionales) punto a punto (de par trenzado, cable coaxial o fibra óptica), de manera que se forma una trayectoria cerrada o anillo que permite la comunicación entre éstas.

Cuando una estación recibe datos por un enlace los retransmite bit a bit por el otro enlace a la misma velocidad que los recibió. Debe observarse que cada estación introducirá un retardo durante el proceso de regeneración y repetición de los bits.

Las estaciones que integran el anillo envían los datos en forma de tramas que también contienen información de control y las direcciones de las estaciones de origen y de destino.

De la misma forma que en otros tipos de redes locales (donde el medio físico se comparte entre todas las estaciones), una estación que esté preparada para transmitir una o varias tramas deberá esperar su turno de acuerdo al protocolo de acceso al medio. Cuando una estación tenga el permiso para transmitir, insertará las tramas al anillo (una a la vez). Cada trama viajará por el anillo (en una sola dirección), pasando por todas las estaciones.

Aunque en la actualidad se conocen las diversas técnicas para controlar el acceso al medio en una red con topología en anillo, la técnica más común se conoce como "Token Ring". Esta técnica, basada en la circulación de un patrón de bits único (token) que otorga el permiso de transmisión fue adoptada por el comité IEEE 802 encargado de los estándares para redes de área local y metropolitana. En 1989, el IEEE emitió el estándar IEEE 802.5 que describe el método de acceso y las especificaciones de la capa física para una red del tipo Token Ring. Este estándar es compatible con las redes Token Ring de IBM.

El estándar IEEE 802.5 describe el funcionamiento de una red Token Ring con las siguientes características:

- Topología: Anillo
- Medio: Par trenzado. El uso de otros medios está sujeto a futuras consideraciones.
- Señalización: Manchester Diferencial.
- Velocidad: 4 y 16 Mbps.
- Protocolo de control de acceso al medio: Paso de token.

1.2.2.1 Formatos de tokens y tramas

En una red Token Ring se usan dos formatos básicos: token y trama. Ambos se muestran en la figura 1.9.

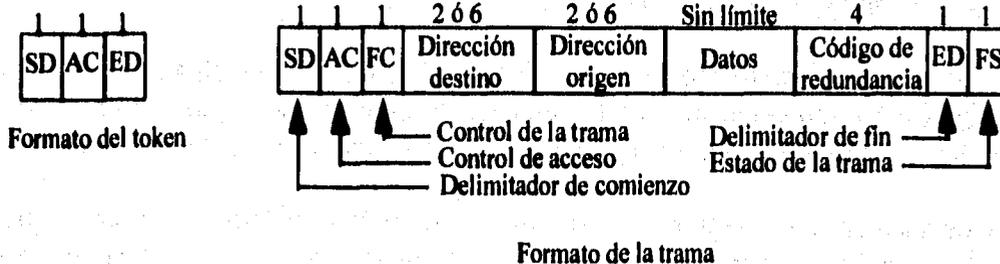


Figura 1.9

El token es el permiso de transmisión y la trama permite transmitir mensajes de las capas MAC o LLC.

Bajo condiciones actuales, el primer bit de la trama irá alrededor del anillo y regresará al extremo que transmite, antes de que se haya transmitido la trama completa. Solamente un anillo muy grande será capaz de contener dentro una trama corta. En consecuencia, la estación transmisora deberá vaciar el contenido del anillo mientras ésta continúa transmitiendo. Esto significa, que los bits que hayan terminado una vuelta, moviéndose alrededor del anillo, regresan al extremo transmisor y son retirados.

Una estación puede mantener el testigo durante el tiempo de retención de testigo que es de 10 ms, a menos que una instalación establezca un valor diferente. Si hay suficiente tiempo, para enviar más tramas, después de haberse transmitido la primera de ellas, éstas también podrán enviarse. Después de haberse transmitido todas las tramas que estaban pendientes, o bien, que la transmisión de otra trama llegue a exceder el tiempo de retención del testigo, la estación se encargará de regresar la trama del testigo de 3 octetos y la colocará sobre el anillo.

Los campos correspondientes al *Delimitador de comienzo* y *Delimitador de fin*, marcan el inicio y final de la trama. Cada uno contiene patrones inválidos en codificación Manchester (HH y LL) para distinguirlos de los octetos de datos. El octeto de *control de acceso* contiene el bit del testigo y, también, el *bit de monitor*, los *bits de prioridad* y los *bits de reserva*. El octeto de *control de trama* distingue las tramas de datos con respecto a varias tramas de control.

Después, vienen los campos correspondientes a la *dirección del destinatario* y *dirección de origen*. A éstos les siguen los datos, cuya longitud puede ser tan

grande como sea necesario, suponiendo que la trama todavía se pueda llegar a transmitir dentro del tiempo de retención del testigo.

Un octeto interesante, es el correspondiente al estado de la trama; en el que están contenidos los bits A y C. Cuando una trama llega a la interface de una estación con la dirección del destinatario, la interface copia la trama en la estación, entonces también pone a uno el bit C. Una estación puede llegar a fallar durante el proceso de copiado de una trama, como consecuencia de falta de espacio en la memoria temporal, o bien, debido a otras razones.

Cuando la estación emisora vacía el contenido de la trama, procedente del anillo, revisa los bits A y C, se pueden presentar tres combinaciones diferentes:

1. $A = 0$ y $C = 0$: cuando el destinatario no está presente o no está conectado.
2. $A = 1$ y $C = 0$: cuando el destinatario está presente, pero la trama no es aceptada.
3. $A = 1$ y $C = 1$: cuando el destinatario está presente y la trama está copiada.

Este arreglo brinda un asentimiento automático para cada una de las tramas. Si se llega a rechazar una trama, estando presente la estación, el extremo transmisor tiene la opción de intentar enviarla nuevamente más tarde. Los bits A y C se encuentran doblemente presentes en el Estado de la trama para incrementar la fiabilidad, en vista de que no están incluidos en el código de redundancia.

El delimitador de fin contiene un bit E que se activa siempre que cualquier interface detecte un error. También contiene un bit que puede utilizarse para marcar la última trama en una secuencia lógica, como si fuera un bit de fin de archivo.

1.2.2.2 Protocolo de control de acceso al medio

En el caso de las redes Token Ring, el control de acceso al medio está distribuido entre todas las estaciones del anillo. Es decir, es un esquema que no depende de ninguna estación y por lo tanto es bastante robusto.

Mientras no esté transmitiendo ninguna estación, estará circulando por el anillo un token y todas las estaciones estarán en estado de repetición (retransmiten por un enlace todos los bits recibidos por el otro). La recepción del token ofrece la oportunidad de transmitir una trama o una secuencia de tramas.

Cuando una estación tenga uno o varios paquetes listos para transmitir, les deberá agregar información de control y las direcciones de origen y destino y

deberá esperar la llegada de un token. En el instante en que la estación detecte que se están repitiendo los bits de un token, se cambiará el valor de uno de los bits del token convirtiéndole en el campo AC de una trama de información (MAC o LLC). La estación pasará del estado de repetición al estado de transmisión. Inmediatamente después se insertarán al anillo los demás campos de la trama. Durante la transmisión se determina una secuencia de verificación de trama que se adiciona después del campo de información.

En este momento, las otras estaciones continúan en estado de repetición y ninguna de éstas podrá transmitir datos por el anillo dado que no hay un token circulando. Para evitar que una estación transmita indefinidamente, se define un tiempo máximo de posesión del token, después del cual deberá emitirse un nuevo token que proporcione la oportunidad de transmitir tramas a las otras estaciones.

Cada trama transmitida se repetirá de una estación a otra y durante la repetición se analizará su campo de control (FC). En caso de tratarse de una trama de tipo MAC, perteneciente al protocolo de acceso, la información será procesada por todas las estaciones del anillo. Si la trama es de tipo LLC, lo cual indica que transporta información entre usuarios, la estación que reconozca su dirección dentro del campo de dirección destino, hará una copia de la trama. En cualquiera de los dos casos se continúa en el estado de repetición.

Dado que las estaciones forman una trayectoria cerrada se observa que debe contarse con un mecanismo para evitar que las tramas circulen por el anillo indefinidamente y garantizar que las otras estaciones puedan transmitir. Para ello, la estación que transmitió la trama debe realizar dos funciones: retirar la trama del anillo y emitir un nuevo token después de terminar la transmisión.

Cuando una estación termina la transmisión de una o varias tramas, verifica si su dirección ha aparecido en el campo de dirección de origen de los bits que está recibiendo (se verifica si la trama transmitida ha dado una vuelta al anillo). Mientras no aparezca esta dirección, la estación continuará en estado de transmisión enviando al anillo bits de relleno. Cuando se cumple la condición, la estación transmite un nuevo token.

Después de esto, la estación continúa en estado de transmisión (enviando bits de relleno) hasta que termine de recibir la trama que transmitió. Lo anterior se hace con el fin de no repetir los bits de la trama o tramas enviadas y de esta forma retirarlas del anillo. Una vez retiradas las tramas transmitidas, la estación pasa al estado de repetición. Debe observarse que una estación en el estado de transmisión no repite los bits recibidos.

En el estándar IEEE 802.5 se define un mecanismo de prioridades con 8 niveles, donde los niveles se asignan dinámicamente dependiendo de la clase de servicio requerido por el usuario. El esquema funciona de tal forma que las estaciones que

tengan tramas con la misma prioridad tengan la misma posibilidad de acceso al anillo.

El esquema de control de acceso al medio con prioridades es una variante del esquema explicado anteriormente. Para poder manejarlo, el token cuenta con un campo que indica la prioridad del token y otro campo que permite reservar el siguiente token.

Ahora debe considerarse que para poder transmitir una trama, no basta con recibir un token. También debe cumplirse la condición de que el token tenga una prioridad menor o igual a la prioridad de la trama que quiera transmitirse.

Cuando una estación está repitiendo el campo AC de una trama, podrá solicitar que el siguiente token sea enviado a una determinada prioridad cambiando el valor de los bits de reservación siempre y cuando la prioridad de la trama que desea transmitir sea mayor que la prioridad que aparece en estos bits. Conforme el campo AC de una trama va pasando por todas las estaciones, aquellas que tengan una trama lista para transmitir intentarán hacer una reservación en este campo. Cuando regrese la trama a la estación transmisora, se tendrá en el campo RRR la máxima prioridad reservada. El nuevo token se transmitirá con una prioridad igual al máximo valor entre:

- La prioridad actual del token.
- La máxima prioridad reservada.
- La prioridad de las tramas listas para transmitir por esta estación (si es que las hay).

Con esto, se garantiza que el próximo token será usado por la estación que tenga las tramas de mayor prioridad.

Si el nivel de prioridad asignado al nuevo token es mayor que el nivel que tenía anteriormente, la estación que emitió el token almacenará en una pila los valores de las prioridades anterior y actual. De esta forma, cuando ya no se tengan más tramas para transmitir con la prioridad actual o mayor, la estación que haya incrementado la prioridad del token a este nivel será la encargada de regresar la prioridad del token al nivel que tenía anteriormente. Se puede observar que todas las estaciones del anillo son responsables del esquema de prioridades.

Para finalizar esta parte relativa al protocolo de control de acceso al medio, se describirá brevemente una técnica opcional para mejorar la eficiencia en la transmisión de datos sobre el anillo. Esta técnica, conocida como "liberación temprana del token" (Early Token Release), permite que la estación transmisora libere el token tan pronto como complete la transmisión de la trama sin importar si ha regresado o no el encabezado de la trama. Dado que el token se libera con

una prioridad igual al último valor de prioridad recibido, este esquema afecta el funcionamiento de las prioridades.

1.2.2.3 Monitor

Para la detección y solución de ciertas condiciones de error que puedan presentarse en el anillo, se designa a una estación como estación monitor activo. Las otras estaciones permanecen como monitores pasivos y están listas para sustituir al monitor activo en cualquier momento.

Los dos principales problemas que pueden presentarse en el anillo y que se resuelven por la estación monitor activo son los siguientes:

Pérdida de token: Para detectar una pérdida de token, la estación monitor activo tiene un temporizador que se restablece cada vez que pasa una trama válida (token o trama). El valor asignado a este temporizador debe ser mayor al tiempo necesario para recorrer el anillo completo. Cuando expira el tiempo, el monitor emite un nuevo token.

Trama circulando de manera indefinida: Para detectar el caso en que una estación no haya retirado del anillo una trama transmitida, el monitor utiliza un bit del token conocido como bit del monitor o bit M. Cada vez que pase una trama cambiará el bit M de "0" a "1". Si el monitor recibe una trama con el bit M puesto en "1", determinará que la estación transmisora no eliminó la trama del anillo y por lo tanto no liberó un nuevo token. En este caso, el monitor realizará ambas funciones.

1.2.2.4 Topología de anillo cableado en estrella

Existe un límite práctico en el número de estaciones que pueden conectarse a un anillo. Esto se debe principalmente al retardo acumulado en las estaciones y al "jitter".

El problema del retardo acumulado se debe a que en cada estación se realizan ciertas operaciones con los bits recibidos (búsqueda de direcciones, búsqueda de ciertos patrones de bits como el token, modificación del valor de un bit, etcétera).

Por otro lado, el jitter tiene su origen en el proceso de recuperación de la señal de reloj a partir del tren de bits recibido. Esta función, que se lleva a cabo en todas las estaciones del anillo, se ve afectada entre otras cosas por el ruido e imperfecciones en los circuitos de recepción (jitter no sistemático). El jitter o

desviación en el reloj se acumula (de una estación a otra) a lo largo de la trayectoria recorrida por las tramas, causando alteraciones en los datos recibidos.

Además de los problemas anteriores, un número muy grande de estaciones en un anillo incrementa los problemas de mantenimiento (localización de fallas) y hace que la red sea menos confiable.

Para permitir la construcción de redes locales más confiables y de fácil mantenimiento, el anillo se reestructuró en una estrella con la ayuda de concentradores. Cada concentrador permite el acceso a un número limitado de estaciones. Sin embargo, pueden conectarse varios concentradores para formar una red de varias estrellas.

Esta topología, que es la base de las redes de IBM, tiene las ventajas de contar con un acceso centralizado (que facilita el aislamiento de fallas) y simplifica la instalación de nuevos concentradores. Las estaciones pueden conectarse y desconectarse de los concentradores sin afectar el funcionamiento de la red. Además, en caso de que se presenten fallas en una estación, ésta se desconectará automáticamente del concentrador.

En este punto es necesario aclarar que aunque la topología del cableado es de estrella y aunque se tengan conectadas varias estrellas, se sigue teniendo una trayectoria cerrada y por lo tanto no cambia el funcionamiento descrito para un anillo y se siguen teniendo los problemas de retardo acumulado y el jitter.

En el caso de redes muy grandes, el total de las estaciones puede dividirse entre múltiples anillos. Cada anillo puede formarse por una secuencia de concentradores y el conjunto de anillos se conectaría por medio de puentes, quienes se encargan del enrutamiento de las tramas de un anillo hacia otro de manera transparente para los usuarios. Esta separación de la red en varios anillos ofrece principalmente las siguientes ventajas:

- La falla en un anillo no afecta el funcionamiento de los otros anillos de la red.
- Es posible mejorar el desempeño de cada uno de los anillos si se agrupan las estaciones de manera que el tráfico entre los anillos sea mínimo.

En las redes Token Ring de IBM se permite un máximo de 260 estaciones por anillo, en redes a 16 Mbps. Este número puede ser ilimitado si se emplean puentes. Sus concentradores, conocidos como unidades de acceso multiestaciones (MAUs), permiten el acceso de hasta 8 estaciones. La máxima distancia entre el MAU y la estación es de 100 m y la máxima separación entre MAUs es de 200 m.

Como conclusión tenemos que la topología de anillo funcionando en conjunto con el esquema de paso de token, da como resultado una red ampliamente confiable

en la que se da la misma oportunidad de acceso a las estaciones que tengan tramas con el mismo nivel de prioridad. Las restricciones en el número de estaciones por anillo pueden resolverse fácilmente separando las estaciones entre múltiples anillos. Con esta técnica, puede conectarse un número ilimitado de estaciones a una sola red.

El protocolo de acceso empleado en las redes Token Ring es la base del esquema de acceso para redes de mayor velocidad (100 Mbps) conocidas como FDDI.

1.2.3 FDDI (Fiber Distributed Data Interface)

1.2.3.1 Fibras ópticas

Los desarrollos recientes en el campo de la tecnología óptica han hecho posible la transmisión de información mediante pulsos de luz. Un pulso de luz puede utilizarse para indicar un bit de valor 1; la ausencia de un pulso indicará la existencia de un bit de valor 0. La luz visible tiene una frecuencia de alrededor de 10^{14} Hz, por lo que el ancho de banda de un sistema de transmisión óptica presenta un potencial enorme.

Un sistema de transmisión óptica tiene tres componentes: el medio de transmisión, la fuente de luz y el detector. El medio de transmisión es una fibra ultradelgada de vidrio o silicio fundido. La fuente de luz puede ser un LED (diodo emisor de luz, DEL), o un diodo láser; cualquiera de los dos emite pulsos de luz cuando se le aplica una corriente eléctrica. El detector es un fotodiodo que genera un pulso eléctrico en el momento que se recibe un rayo de luz. Al colocar un LED o un diodo láser en el extremo de una fibra óptica, y un fotodiodo en el otro, se tiene una transmisión de datos unidireccional que acepta una señal eléctrica, la convierte y la transmite por medio de pulsos de luz y, después, reconvierte la salida en una señal eléctrica, en el extremo receptor.

Este sistema de transmisión tendrá fugas de luz y prácticamente, sería de poco uso, excepto si no existiera un interesante principio de la física. Cuando un rayo de luz pasa de un medio a otro, por ejemplo, del silicio fundido al aire, el rayo se refracta (se desvía) en la frontera silicio/aire, como se muestra en la figura 1.10. En ella se puede observar la incidencia del rayo de luz sobre dicha frontera, a un ángulo Alfa1, emergiendo a un ángulo Beta1, en donde la cantidad de refracción dependerá de las propiedades de los medios (en particular, de sus índices de refracción). Para ángulos de incidencia que se encuentren por encima de un valor crítico, la luz se refracta y regresa al silicio; nada de ella escapa al aire. Así, el rayo de luz que incida por encima del mencionado ángulo crítico, queda atrapado en el interior de la fibra, como se muestra en la parte b) de la figura 1.10, y puede propagarse a lo largo de varios kilómetros sin tener, virtualmente ninguna pérdida.

En la figura 1.10 el dibujo b) sólo muestra un único rayo, pero dado que cualquier rayo de luz incidente, por encima del ángulo crítico, se reflejará internamente, existirá una gran cantidad de rayos diferentes rebotando a distintos ángulos. A esta situación se le conoce como fibra multimodo.

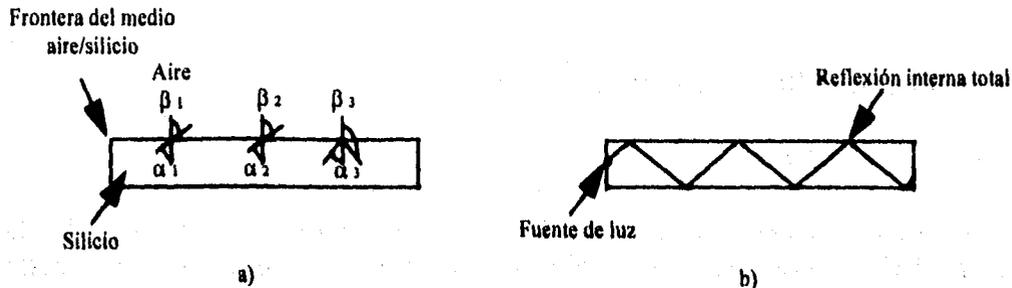


Figura 1.10

Sin embargo, si el diámetro de la fibra se reduce al valor de la longitud de onda de la luz, la fibra actúa como una guía de ondas, y la luz se propagará en línea recta, sin rebotar, produciendo así una fibra de un solo modo. Las fibras de un solo modo necesitan diodos láser (cuyo costo es elevado) para su excitación y no LED (que son más económicos), pero con aquéllos se asegura una mayor eficiencia y pueden utilizarse en distancias muy largas. En la actualidad los sistemas de fibras ópticas son capaces de hacer transmisiones de datos de 1000 Mbps en 1 kilómetro. En el laboratorio se han podido alcanzar velocidades mayores, pero con distancias más cortas. Experimentalmente se ha demostrado que los láseres potentes pueden llegar a excitar fibras de 100 km de longitud sin necesidad de utilizar repetidores, aunque la velocidad es más lenta.

Los enlaces de fibras ópticas están siendo empleados en diferentes países en la instalación de líneas telefónicas de larga distancia, y esta tendencia seguramente continuará en las siguientes décadas, y será cada vez mayor la sustitución del cable coaxial por fibras, en un número más grande de rutas.

Las fibras también forman la base de LAN, aunque su tecnología es más compleja. El problema fundamental consiste en que, aunque en las fibras LAN pueden realizarse conexiones tipo vampiro, mediante la fusión de fibra proveniente del ordenador con la fibra LAN, el procedimiento para construir un conector resulta ser sumamente delicado y, en general, se pierde una cantidad considerable de luz.

Una solución a este problema es darse cuenta que una red en anillo es en realidad una colección de enlaces punto a punto, tal y como se muestra en la figura 1.11. La interface que existe entre cada una de las computadoras permite el paso del flujo de los pulsos de luz al siguiente enlace, y también sirve como una unión en T por medio de la cual la computadora envía y acepta mensajes.

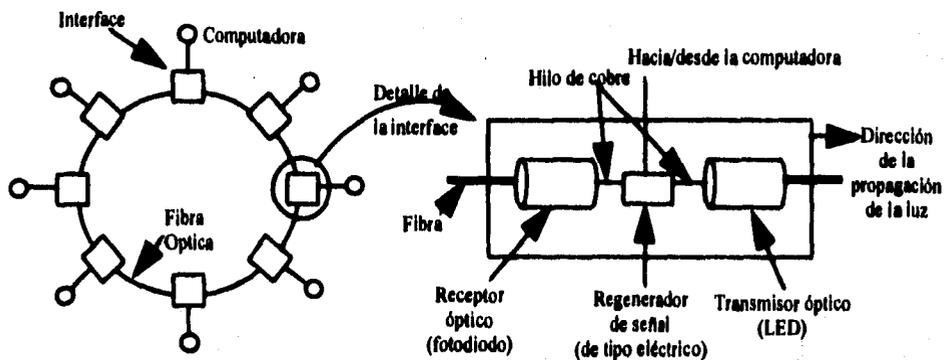


Figura 1.11

Dos tipos de interface son los que se utilizan. Uno de tipo pasivo que consiste de dos conectores fusionados con una fibra principal; uno de los conectores tiene un LED o diodo láser en uno de sus extremos (para transmisión), y en el otro tiene un fotodiodo (para recepción). La conexión es completamente pasiva y, por lo tanto, es muy fiable porque la puesta fuera de servicio de un LED o fotodiodo no destruye el anillo; sino que sólo inhabilita una computadora.

El otro tipo de interface, es el repetidor activo. La luz incidente se convierte en una señal eléctrica y se regenera a su máximo valor, si éste ha disminuido, y así puede retransmitirse nuevamente como luz. La interface con la computadora es un cable de cobre común y corriente, que se encuentra contenido en el generador de señales. Si se llega a estropear un repetidor activo, se rompe el anillo y la red se desactiva. Por otra parte, y dado que la señal se regenera en cada interface, los enlaces individuales de computadora a computadora pueden tener varios kilómetros de longitud sin existir, virtualmente, un límite en el tamaño total del anillo. Las interfaces pasivas pierden luz en cada una de las uniones, de tal manera que el número de computadoras, así como la longitud total del anillo, se ven seriamente restringidas.

La topología de anillo no es la única alternativa para construir una LAN con el empleo de fibras ópticas; también es posible tener el hardware necesario para el proceso de difusión por medio del uso de la estrella pasiva, cuya configuración se ilustra en la figura 1.12. En este diseño, cada una de las interfaces cuenta con una fibra que va desde su transmisor hasta un cilindro de silicio, con las fibras de entrada fusionadas a un extremo del cilindro. De la misma manera, las fibras fusionadas en el otro extremo del cilindro, salen hacia cada uno de los receptores. Siempre que una interface emita un pulso de luz, éste se difunde en el interior de una estrella pasiva para iluminar a todos los receptores, y así llevar a cabo el proceso de difusión. La estrella pasiva, efectivamente, realiza una función booleana, tipo OR, con todas las señales que llegan, y transmite el resultado por todas las líneas hacia el exterior. Dado que la energía que llega se divide entre

todas las líneas que salen, el número de nodos en la red está limitado por la sensibilidad de los fotodiodos.

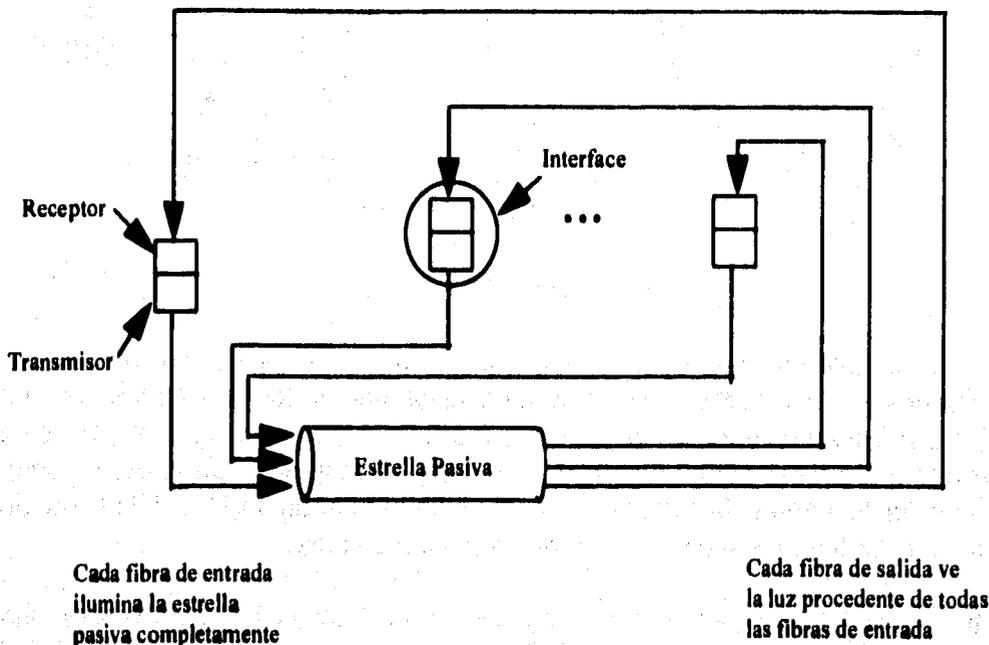


Figura 1.12

La comparación entre el cable coaxial y la fibra óptica es muy instructiva. Las fibras proporcionan un ancho de banda extremadamente grande y tienen una pérdida de potencia muy pequeña, razón por la que se emplean para distancias muy largas entre repetidores. Las fibras, no se ven afectadas por alteraciones de voltaje o corriente en las líneas de potencia, por interferencia electromagnética o por químicos corrosivos dispersos en el aire, de tal forma que pueden emplearse en ambientes industriales expuestos a condiciones muy severas en las que, los cables serían inadecuados. Las fibras son también muy delgadas, lo que representa un factor positivo muy importante para las compañías que tienen una gran cantidad de cables y conductos abultados.

Del lado negativo se encuentra el hecho de que hay poca familiaridad con la tecnología de las fibras ópticas y requiere una habilidad que los ingenieros en redes aún no tienen. El empalme o unión de dos o más fibras es difícil, y más todavía su derivación. Las fibras ópticas son inherentemente unidireccionales y el costo de las interfaces es mucho mayor que el de las respectivas interfaces de tipo eléctrico. Las ventajas de las fibras ópticas, sin embargo, son tantas que el empeño y trabajo que se está dando para mejorar su tecnología y reducir su costo es muy grande e importante.

FDDI es un estándar originalmente propuesto por el Grupo de Trabajo X3T9.5 del Instituto Nacional de Estándares (ANSI) para ser utilizado principalmente como: a) enlace entre computadoras y dispositivos periféricos de alta velocidad (la especialidad del subcomité X3T9), b) red local de alta velocidad para aplicaciones que requieren tasas de transmisión superiores a las proporcionadas por las redes locales IEEE 802, y c) espina dorsal para la interconexión de redes locales de baja velocidad. FDDI tiene ahora reconocimiento internacional en la norma 9314 de la Organización Internacional para la Estandarización (ISO).

El funcionamiento de FDDI está basado en los mecanismos de operación de otras redes locales, en particular los especificados en la norma IEEE 802.5. A continuación se describe la topología de una red FDDI, su arquitectura interna, la función de la capa física, el protocolo de acceso al medio utilizado y el formato de las tramas que circulan en la red.

1.2.3.2 Topología

La topología básica de FDDI está formada por un anillo doble que soporta una distancia máxima de 200 Km y 1000 conexiones físicas. Las estaciones de la red pueden conectarse al anillo directamente o a través de un concentrador. De hecho, la topología más general de FDDI es un anillo (doble), como se observa en la figura 1.13.

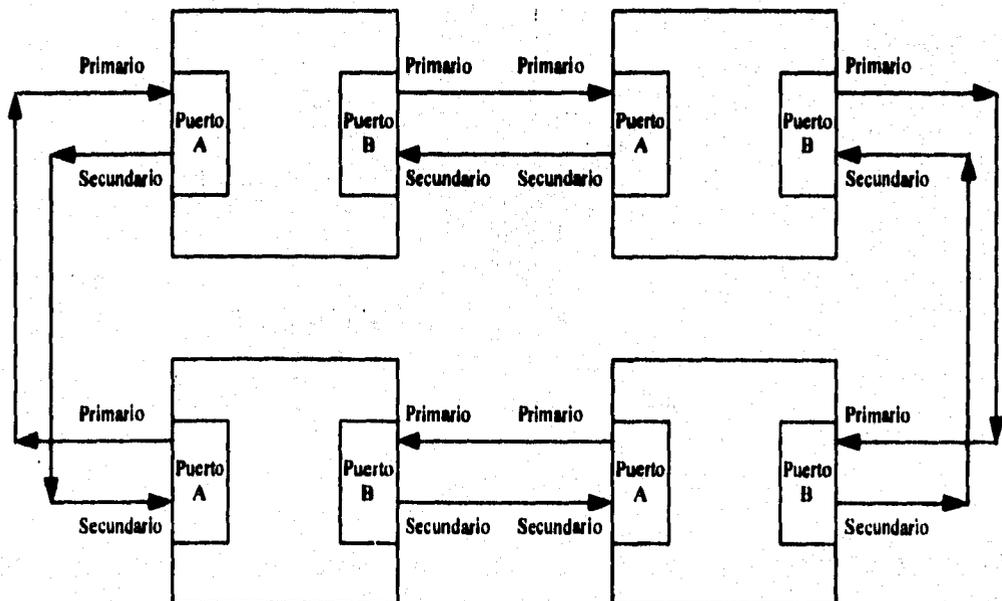


Figura 1.13

Los dos anillos en contra-rotación son la base de la tolerancia a fallas de la red. Cuando ocurre una falla en el enlace que une a dos nodos (estaciones o concentradores) o en algún nodo, los dos nodos que se encuentran alrededor de la falla se reconfiguran internamente y, utilizando los enlaces que fluyen en sentido opuesto, crean un nuevo anillo como se muestra en la figura 1.14.

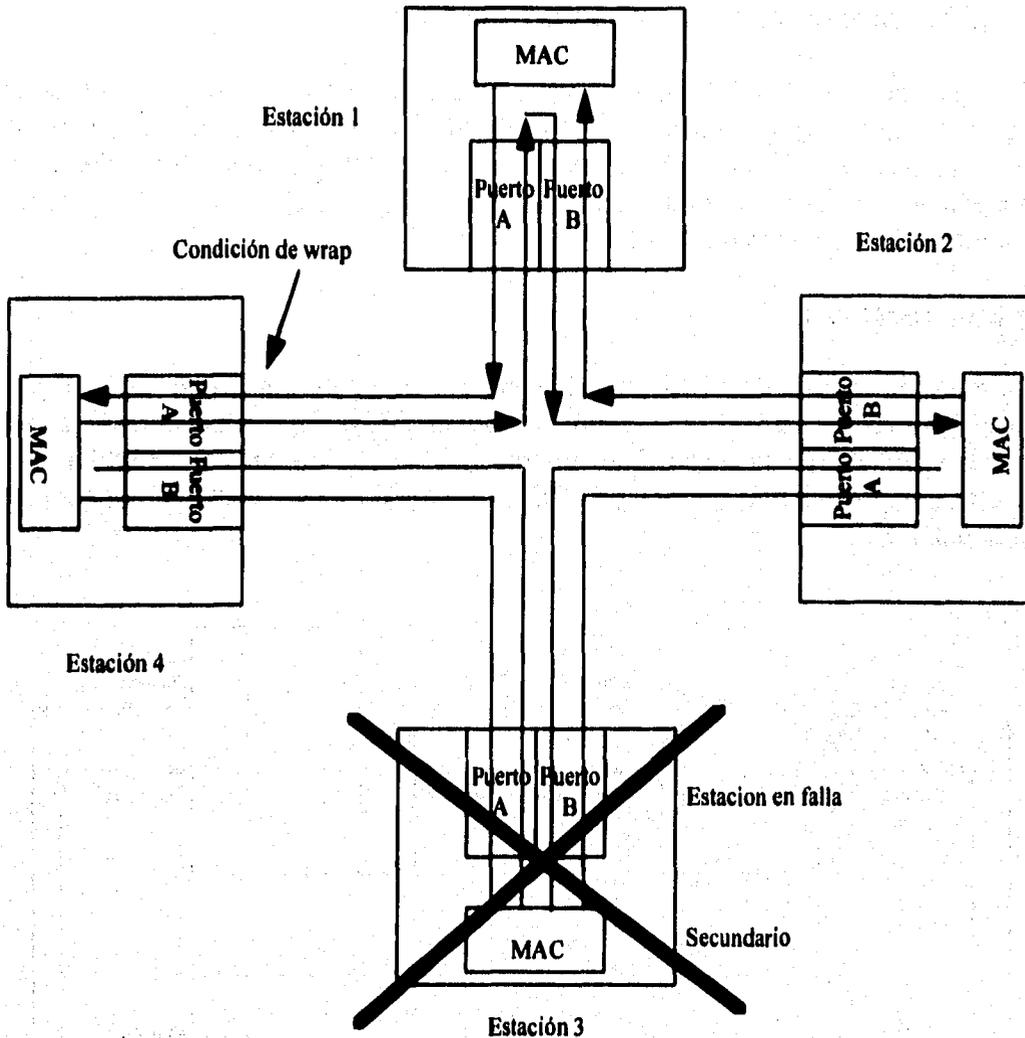


Figura 1.14

Las estaciones pueden conectarse a los dos anillos (DAS: Estaciones de Conexión Doble) o únicamente al anillo principal (SAS: Estaciones de Conexión Sencilla). Las estaciones DAS son más robustas que las estaciones SAS ya que una falla en un anillo no las desconecta de la red, pero son mucho más costosas. Un concentrador también puede tener conexión doble o sencilla a la red, pero todas las estaciones que se conectan a él son estaciones SAS.

1.2.3.3 Arquitectura

La arquitectura de la norma FDDI mantiene un esquema común con la arquitectura IEEE 802 y está constituida como se aprecia en la figura 1.15.

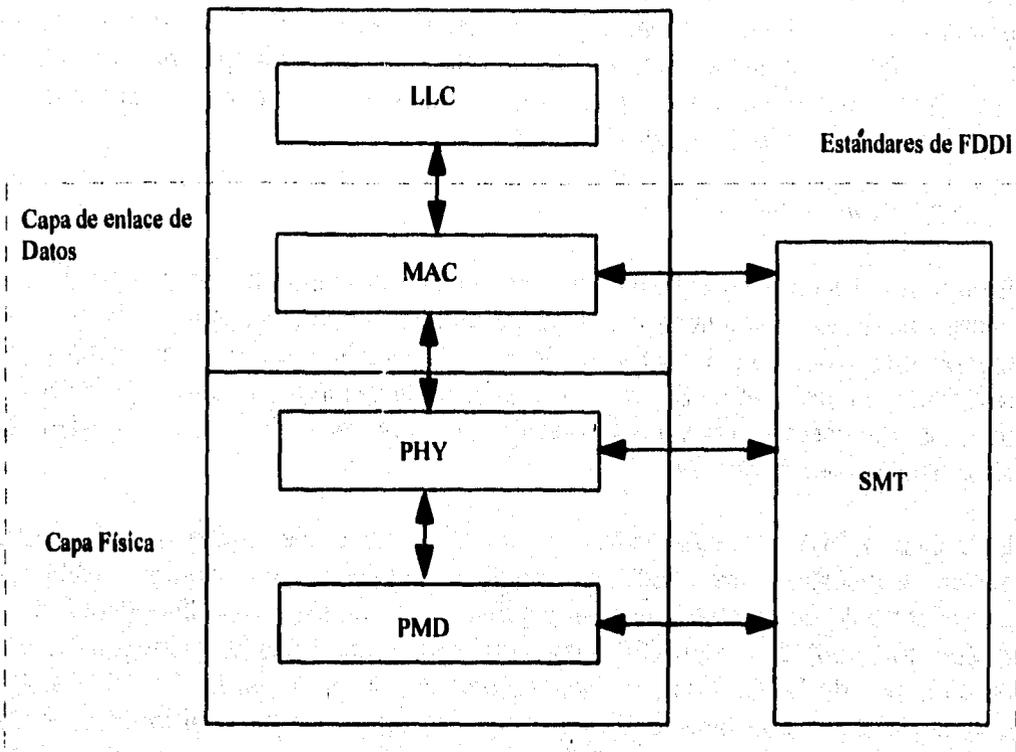


Figura 1.15

- 1) Capa física (PL)
- 2) Capa de enlace de datos (DLL)
- 3) Administración de estaciones (SMT)

La capa física se encuentra dividida en dos partes: la subcapa dependiente del medio físico (PMD) y el protocolo de la capa física (PHY). La subcapa PMD proporciona la comunicación digital en banda base entre los nodos de la red. Especifica, por ejemplo, las características de los transmisores, receptores, cables y conectores. La subcapa PHY es la interface entre la capa de enlace de datos y la subcapa PMD. Básicamente se encarga de la codificación (y decodificación) de la información que circula en la red.

La capa de enlace de datos para redes locales contiene tradicionalmente dos subcapas. En FDDI sólo se especifica la subcapa de control de acceso al medio (MAC) y opcionalmente se utiliza la subcapa de control del enlace lógico (LLC) definida por la norma IEEE 802.2. La subcapa MAC proporciona un mecanismo de acceso determinista al medio de transmisión, y su principal función es permitir la transmisión de unidades de datos (tramas) entre los nodos de la red.

La administración de estaciones proporciona las funciones necesarias para administrar la operación de las diferentes subcapas de FDDI, y permitir que los nodos trabajen conjuntamente en la red. SMT se encarga, por ejemplo, de la detección y recuperación de fallas en el anillo, y establecer las políticas de asignación del ancho de banda de la red.

1.2.3.3.1 Capa física

En una red Token Ring el flujo de bits se codifica utilizando el código Manchester diferencial. Este código tiene la propiedad de que la señal transmitida tiene por lo menos una transición en cada bit, lo que permite mantener sincronizados los relojes de las estaciones. Sin embargo, esta codificación no se utiliza en FDDI por razones de costo y complejidad técnica ya que requeriría una velocidad de señalización de 200 Mbauds.

La subcapa PHY de FDDI utiliza una codificación doble: todos los datos que deben transmitirse se codifican primero utilizando un código 4B/5B y posteriormente los bits se transmiten siguiendo una codificación NRZI (NonReturn to Zero Inverted). El código 4B/5B convierte grupos de 4 bits de datos a transmitir en símbolos de 5 bits. Los símbolos escogidos para representar los 16 posibles grupos de datos son tales que existe un máximo de un bit 0 al inicio de cada símbolo y un máximo de dos bits 0 al final. Los bits de los símbolos son transmitidos utilizando la codificación, NRZI que produce una transición en la señal cuando se transmite un bit 1. Esta doble codificación, 4B/5B y NRZI, garantiza entonces que existe una transición en la señal al menos cada tres bits, lo que permite la sincronización de los relojes a una velocidad de señalización de 125 Mbauds.

El uso de símbolos de 5 bits para representar cada uno de los 16 grupos posibles de datos de 4 bits deja 16 símbolos sin utilizar. Algunos de estos símbolos (I, J, K, T, R y S) tienen funciones específicas en el formato de las tramas FDDI.

La codificación empleada por PHY es independiente del medio de transmisión utilizado. Las características del medio físico son consideradas en la subcapa PMD. Originalmente, ésta especificaba únicamente la conexión entre nodos a través de fibra óptica multimodal (MMF-PMD) y soportaba una distancia máxima entre nodos de 2 km. Para soportar distancias entre nodos de hasta 60 km se desarrolló posteriormente la especificación SMF-PMD que utiliza fibra óptica

monomodal y reemplaza los LEDs en los transmisores por lasers. En el mercado existen también redes FDDI de bajo costo basadas en par trenzado no blindado.

1.2.3.4 Protocolo MAC

El protocolo MAC utilizado por las estaciones en una red FDDI está basado en el protocolo IEEE 802.5, al cual se realizaron algunas modificaciones para mejorar su desempeño en altas velocidades.

El acceso al medio está controlado por la posesión de un privilegio denominado token. Si ninguna estación en la red quiere transmitir, el token (una trama especial que indica que el medio está libre) circula sobre el anillo. Cuando una estación quiere transmitir, espera el token, lo remueve del anillo y transmite su trama. En 802.5 la estación que transmite una trama pone en circulación un nuevo token en la red después de: a) terminar su transmisión, y b) recibir el encabezado de esta trama después de una vuelta completa alrededor del anillo. La alta velocidad de transmisión de FDDI, el tamaño máximo que pueden tener las tramas y la extensión física que puede alcanzar la red hacen que el tiempo de transmisión de una trama pueda ser pequeño en comparación al retardo de propagación de la trama alrededor del anillo. Por esta razón, para aumentar la eficiencia en el uso de la red, la estación que transmite pone en circulación un nuevo token inmediatamente después de terminar una transmisión, sin esperar la ocurrencia del evento (b) mencionado arriba.

A este esquema básico se agregan otros mecanismos de asignación del ancho de banda que permiten transmitir varias tramas consecutivas y multiplexar en el tiempo tráfico continuo y en ráfagas. Dado que en FDDI la estación que transmite no espera el regreso de su trama para transmitir un nuevo token, no puede utilizarse el esquema de prioridades de 802.5, basado en la reservación del siguiente token a una determinada prioridad utilizando el encabezado de la trama actualmente en circulación. En su lugar se utiliza una variante del algoritmo de asignación de capacidad de 802.4 (Token Bus).

Una estación con tráfico continuo requiere recibir el token periódicamente dentro de un cierto rango de tiempo. La periodicidad se establece durante la inicialización del anillo al valor mínimo solicitado por las estaciones (TTRT). El protocolo MAC de FDDI asegura que el valor promedio del tiempo de rotación del token es igual al valor negociado y que es siempre inferior a dos veces éste. A cada estación con requerimientos de tráfico continuo se le asigna un tiempo de transmisión SA durante el cual puede enviar tramas cada vez que capture un token. Esta asignación asegura un cierto ancho de banda para la transmisión de tramas de información "síncronas".

Para la transmisión el tráfico en ráfagas, con requerimientos de ancho de banda menos predecibles y tiempos de respuesta menos críticos, se utilizan tramas de información "asíncronas". Estas tramas pueden o no ser enviadas cuando se captura un token dependiendo de la velocidad de rotación del token. Cada estación tiene un temporizador TRT que mide el tiempo entre llegadas consecutivas del token. Si este tiempo es superior a TTRT entonces la estación no puede enviar tramas asíncronas. Si el token llega a tiempo entonces la estación puede enviar tramas asíncronas durante el tiempo igual a la diferencia entre TTRT y TRT. Esta diferencia se almacena en el temporizador THT que se habilita únicamente durante la transmisión de tramas asíncronas. Dependiendo del valor de THT es posible enviar tramas en ocho diferentes niveles de prioridad.

Una característica adicional de FDDI hace posible que dos (o más) estaciones puedan establecer diálogos asíncronos extendidos, utilizando tokens restringidos que permiten reservar temporalmente todo el ancho de banda que no se usa para la transmisión síncrona. Un token restringido es un token especial que transporta una dirección DA y que sólo puede ser capturado, para la transmisión de tramas asíncronas, por la estación con dirección DA.

A diferencia de 802.5, en FDDI no hay una estación particular encargada de monitorear el anillo. Esta función se distribuye entre todas las estaciones y tiene como objetivo detectar y corregir una condición inválida de funcionamiento en el anillo. La existencia de esta condición es detectada por las estaciones cuando no ven circular un token en un determinado intervalo de tiempo. Para corregir esta condición, las estaciones de FDDI ejecutan un algoritmo distribuido de elección, y la estación ganadora inserta en el anillo un nuevo token. Si la condición inválida no puede resolverse debido, por ejemplo, a una ruptura en el anillo, las estaciones invocan un proceso de guía (beacon) que finaliza hasta que el anillo se restaura (por intervención manual o automáticamente).

1.2.3.5 Formato de las tramas

Las tramas en una red FDDI están formadas por los siguientes campos, ver figura 1.16.

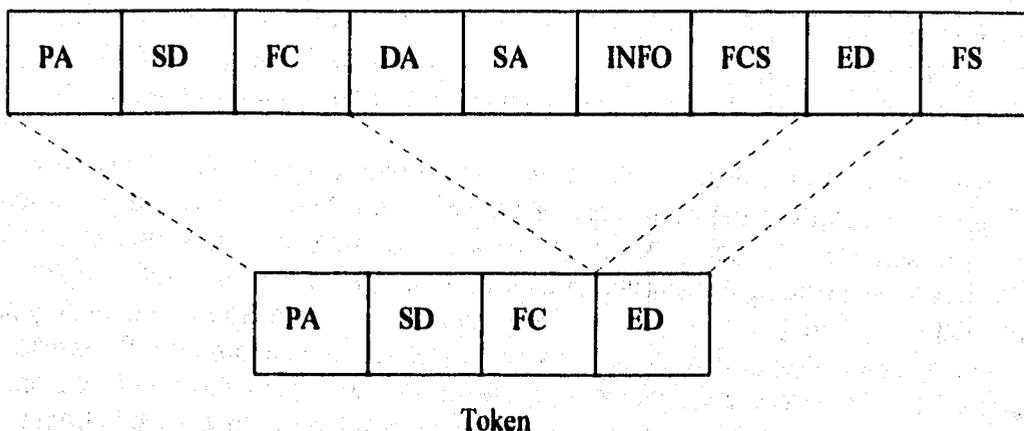


Figura 1.16

Preámbulo (PA): Sincroniza la trama con el reloj de cada estación. El originador de la trama envía este campo con 16 símbolos I (idle); los nodos que repiten la trama alrededor del anillo pueden cambiar la longitud de este campo de acuerdo a sus requerimientos de sincronización.

Delimitador de Inicio (SD): Indica el comienzo de la trama. Consta de un símbolo J seguido de un símbolo K.

Control de la Trama (FC): Identifica el tipo de la trama. Este campo está constituido por los bits CLFFZZZZ. El bit C especifica la clase de la trama (asíncrona o síncrona); el bit L indica si la longitud de los campos de direcciones es de 16 ó 48 bits; los bits FF indican si la trama contiene información del usuario (LLC) o información de control del protocolo MAC; y los bits ZZZZ especifican la prioridad de la trama LLC o el tipo de trama MAC.

Dirección Destino (DA): Especifica la estación a la cual va dirigida la trama. Puede ser una dirección única o de grupo. En una misma red pueden coexistir estaciones con direcciones de 16 bits y estaciones con direcciones de 48 bits.

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

Información (INFO): Contiene datos del usuario o información de control MAC. La longitud máxima de una trama es de 4500 bytes, incluyendo 2 bytes del preámbulo.

Secuencia de Verificación de Trama (FCS): Este campo de 32 bits sirve para detectar si hubo errores durante la transmisión de la trama. El FCS se calcula utilizando los campos FC, DA, SA e INFO.

Delimitador de Fin (ED): Consta de un símbolo T (dos si se trata de un token) e indica el final de la trama. Como símbolo T no forma parte de los 16 símbolos de datos, el DE no puede confundirse con símbolos de otros campos de la trama.

Estado de la Trama (FS): Contiene tres indicadores E (error), A (dirección) y C (copiado). Cuando la estación emisora transmite una trama coloca en el campo FS tres símbolos R (reset). Al circular esta trama sobre la red, si una estación detecta un error en la transmisión coloca en el indicador E el símbolo S (set); si una estación detecta su dirección en el campo DA cambia a S el indicador A, y si además copia la trama cambia el indicador C a S. Los indicadores A y C permiten que la estación emisora determine, al regresar su trama, si la estación receptora: no existe (o no es activa), existe pero no copió la trama, o existe y copió la trama.

A manera de conclusión, tenemos que la especificación y desarrollo de FDDI se basaron en la experiencia obtenida durante la normalización y la operación de las redes IEEE 802, y en el análisis de las necesidades de los usuarios que debía satisfacer una red de alta velocidad. Debido a esto, FDDI ha sido utilizada con gran éxito en las tres aplicaciones de redes locales para las cuales fue creada. Sin embargo, continúa evolucionando y ahora su área de aplicación no se limita únicamente a ambientes locales; el desarrollo de la especificación SMF-PMD abre la puerta a su uso como red metropolitana. Este nuevo ambiente aumenta los requerimientos impuestos a FDDI y da origen a FDDI-II.

1.3 Protocolos de Redes de Datos

1.3.1 Windows NT

1.3.1.1 Descripción general

Meses antes que la primera unidad saliera de la fábrica, Microsoft Windows NT ya estaba causando alboroto. Este producto generó una buena cantidad de especulación sobre los beneficios de un sistema operativo con multitareas y múltiples vías de ejecución, que tuviera la ventaja adicional de usar la familiar interface de Windows.

Windows NT es un sistema operativo de 32 bits, en todos los aspectos. Esto significa que las instrucciones se ejecutan más rápido, que la máquina gráfica de 32 bits y los manejadores de dispositivo de 32 bits dibujan las pantallas con más rapidez, y que la transferencia de datos a los diversos sistemas de almacenamiento también es más rápida.

NT también es un sistema de multitareas con prioridad y de múltiples vías de ejecución. Puede ejecutar varias aplicaciones, cada una en sus propios espacios protegidos simultáneamente. Las aplicaciones especialmente escritas pueden tener subtareas (vías) que le permiten ejecutarse con más eficiencia, NT maneja un nuevo sistema de archivos (NTFS) que reemplaza el sistema de FAT de DOS y provee algunos beneficios nuevos tales como nombres largos de archivos.

Además de proveer este conjunto de características, NT tiene características avanzadas poderosas, como la seguridad de nivel C2, que satisface los requisitos de los clientes de gobierno. Por esta razón, por lo menos al principio, NT será potencialmente útil para dos grupos de usuarios: los que en la actualidad usan las estaciones de trabajo avanzadas para realizar tareas especializadas, como el CAD, el modelaje u otras tareas que requieran procesamiento y uso de gráficos intensivo y los que necesitan un servidor de aplicación para las aplicaciones de negocio críticas como las bases de datos. Algunas características avanzadas, como la capacidad de adaptación de NT (la habilidad de correr en un amplio rango de *hardware*, incluyendo máquinas basadas en procesadores Alpha y de RISC), redes incorporadas, seguridad de alto nivel, tolerancia a fallos, herramientas de supervisión de rendimiento y administración y sus conexiones a plataformas importantes de sistemas de redes y *mainframe*, hacen que NT sea "demasiado" para la mayoría de las PC's de escritorio. Estas características también contribuyen a los requisitos de recursos de NT: Se recomienda una máquina basada en 486 o RISC, 16 MB de memoria RAM y un disco duro grande.

NT es un sistema operativo muy extenso, porque puede usarse como un cliente de escritorio o como un servidor potente, porque puede ejecutar las nuevas aplicaciones de 32 bits y también las aplicaciones existentes de DOS y de 16 bits de Windows, porque puede correrse en un espectro de máquinas que incluyen las máquinas MIPS basadas en RISC y las Alpha AXP.

Las aplicaciones son un factor e indicador clave de un sistema operativo exitoso. La meta de Microsoft es proporcionar a sus clientes una interface de usuario consistente y aplicaciones basadas en un rango de plataformas: desde una computadora personal hasta un servidor con un multiprocesador RISC, todos son capaces de trabajar con Windows y sus aplicaciones.

Microsoft continuará extendiendo el alcance del sistema operativo Windows en las siguientes máquinas:

- **Low-end:** Optimizar Windows para la miniaturización y para máquinas portátiles.
- **Portátiles/Móviles:** Aumentar el soporte de Windows para *pen computing* y capacidades multimedia.
- **Mid-range:** Construir el éxito de Windows mediante el mejoramiento y refinamiento de sus capacidades.
- **High-end:** Con Windows NT, extender el poder de Windows a una plataforma servidor, capacidades workstation high-end. Proporcionar portabilidad a otra arquitectura de chip, soporte de multiproceso, seguridad y tolerancia a errores.

Todos estos tipos de máquinas ejecutarán software basado en Windows y presentarán plataformas para futuras aplicaciones Windows e innovaciones. Esto sucederá a través de un producto y una estrategia: Microsoft Windows.

Microsoft comenzó a desarrollar sistemas operativos en 1981 cuando liberó MS-DOS 1.0 para la computadora personal IBM. Cuando Intel Corporation presentó el microprocesador 80286, Microsoft e IBM desarrollaron en conjunto OS/2 1.0 para tomar ventaja de sus características avanzadas.

Sin embargo, con las limitaciones inherentes en el diseño de OS/2, específicamente que fue escrito en lenguaje ensamblador 80286 y esto impedía su portabilidad, Microsoft dejó el desarrollo de OS/2 por completo a IBM. Microsoft comenzó a considerar las cualidades que debía tener el sistema operativo ideal.

En 1988 Dave Cutler, anteriormente líder del equipo de desarrollo del sistema operativo VMS para Digital Equipment Corporation, se unió a Microsoft para crear el nuevo sistema operativo - Windows NT.

El nuevo sistema tenía ambiciosas metas de diseño:

- Diseño modular.
- Subsistemas de medio ambiente.
- Modelo device-driver en capas; drivers instalables.
- Asignar un tiempo a cada proceso. No monopolizar.
- Multiproceso simétrico.
- Microkernel genérico.
- Administración de recursos orientada a objetos.
- Control de acceso centralizado.
- Procesos se ejecutan en espacios de direcciones separadas.
- Kernel privilegiado, pero aplicaciones no privilegiadas.

Una de las metas de diseño clave del sistema operativo Windows NT fue que pudiera ser portable. Tres estrategias fueron aplicadas para lograr portabilidad:

- Escribir el código en un lenguaje de alto nivel.
- Aislar código dependiente del hardware en módulos fácilmente localizables.
- Ocultar diferencias de hardware.

La mayoría del código fuente para Windows NT está escrito en C o C++, con algún requerimiento de ensamblador. Estos lenguajes de alto nivel hacen relativamente fácil portar Windows NT a diferentes tipos de workstations. La misma fuente puede ser recompilada para crear versiones de Windows NT que son específicas para cada conjunto de instrucciones de procesador.

1.3.1.2 Plataformas capaces de ejecutar Windows NT

Windows NT corre sobre workstations CISC (Intel 80386DX, 80486 y Pentium) y workstations RISC (MIPS R4000 y DEC Alpha AXP).

Actualmente Windows NT corre sobre workstations basadas en el Intel 80386 y 80486, MIPS R4000, y procesadores DEC Alpha AXP. Esto es una notable realización dadas las considerables diferencias entre el conjunto de instrucciones de estos procesadores. Los procesadores MIPS y DEC son RISC (Reduced Instruction Set Computers). Esto significa que soportan un pequeño número de instrucciones, cada una de las cuales ejecuta una operación relativamente simple. En contraste, los procesadores Intel son CISC (Complex Instruction Set Computers). Esto es, soportan un gran conjunto de instrucciones más complejas.

1.3.1.3 Windows NT vs. Windows NT Advanced Server

La única diferencia entre Windows NT y Windows NT Advanced Server se encuentra en algunas de sus características de trabajo en red.

Características Windows NT	Características Windows NT Advanced Server
File server, print server, application server	File server, print server, application server
Peer-to-peer networking	Peer-to-peer networking
Participa en los dominios Windows NT	Participa en los dominios Windows NT
Servicio de acceso remoto (solamente una sesión)	Servicio de acceso remoto (hasta 64 sesiones)
Duplicación (sólo al importar)	Duplicación(importar y exportar)
	Ejecutar validaciones logon en los dominios NT
	Servicios Macintosh
	Incluye manejadores de disco con tolerancia a errores
	Herramientas para administración del dominio

Tabla 1.1

1.3.1.4 Componentes de Windows NT

1.3.1.4.1 Productos componentes de Windows NT

Windows NT es un sistema operativo modular, compuesto por un grupo de módulos relativamente independientes:

- Subsistemas de medio ambiente - la porción modo usuario de Windows NT, la cual corre programas escritos para diferentes sistemas operativos (mediante su emulación) así como también programas escritos específicamente para Windows NT. Ejemplos son el subsistema Windows NT 32-bit (Win32), el subsistema OS/2 y el subsistema POSIX.
- NT *ejecutivo* - la porción modo kernel de Windows NT, la cual consiste de:
 - Servicios *ejecutivos* - Administra I/O, incluyendo seguridad.
 - Administradores - módulos que administran I/O, objetos, seguridad, comunicaciones de interprocesos (IPC), memoria virtual y procesos.
 - Manejadores de dispositivos - módulos que traducen sus llamadas en accesos a hardware.

- Kernel - maneja sólo procesador(es); mas como un microkernel. Note que se refiere al componente kernel del modo kernel, no al modo kernel entero.
- Capa de abstracción de hardware (HAL) - aísla la interface del hardware del hardware mismo, haciendo a Windows NT más portable.

1.3.1.4.2 Subsistemas disponibles en Windows NT

Algunas de las metas más importantes para Windows NT se centran en la necesidad de correr diferentes tipos de aplicaciones en la misma aplicación gráfica. Windows NT corre aplicaciones escritas para sistemas operativos existentes tales como MS-DOS, OS/2, y Microsoft Windows 3.1. También corre aplicaciones escritas para interfaces de programa más recientes tales como POSIX y Win32.

Windows NT soporta esta variedad de aplicaciones mediante el uso de subsistemas de medio ambiente. Los subsistemas de medio ambiente son procesos de Windows NT que emulan medio ambientes de diferentes sistemas operativos. El NT ejecutivo proporciona servicios genéricos que todos los subsistemas de medio ambiente pueden llamar para ejecutar funciones básicas de sistema operativo. Los subsistemas construidos a partir de los servicios del ejecutivo producen medio ambientes que satisfacen las necesidades específicas de las aplicaciones de su cliente. Implementando funciones comunes de sistema operativo y separándolas de los aspectos específicos del medio ambiente se reduce el esfuerzo requerido para desarrollar nuevos subsistemas de medio ambiente y hacer más fácil su mantenimiento.

Los subsistemas de Windows NT son transparentes para el usuario. Los subsistemas apropiados son cargados cuando inicia Windows NT o cuando un usuario corre una aplicación que utiliza el subsistema.

En el caso de aplicaciones basadas en MS-DOS y Windows 3.1, es agregada una capa extra de código entre el subsistema Win32 y la aplicación. Las aplicaciones basadas en MS-DOS corren en una máquina virtual DOS (VDM) que emula MS-DOS 5.0. Aplicaciones basadas en Windows 3.1 corren en una VDM que ha sido modificada para incluir una capa Windows en Win32 (WOW), permitiendo que llamadas a la API de Windows 3.1 sean traducidas a llamadas a la API Win32.

1.3.1.4.3 Consistente interface de usuario entre subsistemas

Windows NT se presenta a los usuarios con la interface Windows 3.1. Esta interface de usuario es proporcionada por el subsistema Win32. El subsistema Win32 tiene la exclusiva responsabilidad de desplegar la salida en el sistema de monitor y manejar la entrada de usuario. En términos de arquitectura, esto significa que los otros subsistemas de medio ambiente deban llamar funciones del subsistema Win32 para desplegar la salida. También significa que el subsistema Win32 debe pasar acciones de entrada del usuario a los otros subsistemas de medio ambiente cuando el usuario interactúa con las otras ventanas de subsistema.

1.3.1.5 Compartiendo datos entre aplicaciones

Cuando una aplicación basada en Win32 se prepara para ejecutarse, es ligada a una librería dinámica, WIN32.DLL, la cual contiene declaraciones para todas las funciones en la API Win32.

Dado que aplicaciones basadas en Win32, aplicaciones Windows de 16 bits, y aplicaciones MS-DOS comparten el mismo subsistema (el subsistema Win32) estas aplicaciones pueden compartir datos a través del intercambio dinámico de datos (DDE) y ligado de objetos (OLE).

Las comunicaciones entre las aplicaciones y los subsistemas están coordinadas por el Interprocess Communication Manager (IPC Manager), usando llamadas a procesos locales (LPCs). "Local" se refiere a que la función es ejecutada en la misma computadora en la que es llamada.

1.3.1.6 Kernel vs. modos usuario

El ejecutivo Windows NT es central para la mayoría de las funciones de sistema operativo. Esto hace importante proteger al ejecutivo de subsistemas y aplicaciones con mal funcionamiento. Los desarrolladores de Windows NT acordaron correr el ejecutivo en un modo de proceso privilegiado (llamado modo kernel), mientras los subsistemas y todas las otras aplicaciones corren en un modo de proceso no privilegiado (llamado modo usuario).

Dado que el ejecutivo corre en modo kernel, tiene acceso a toda la memoria en la workstation y puede acceder a cualquier instrucción de máquina que necesite. Todo el otro código, incluyendo los subsistemas de medio ambiente, corren en modo usuario y pueden sólo acceder memoria privada o memoria que el ejecutivo permite sea compartida.

1.3.1.7 Capacidades de Windows NT

1.3.1.7.1 Multiproceso simétrico (SMP)

Windows NT es un sistema operativo de multiproceso simétrico (SMP). Esto significa que puede usar uno o más procesadores en una sola computadora, mientras sean del mismo tipo y estén configurados de forma similar. Los procesadores permiten correr una mezcla de código de aplicación y sistema operativo. De esta manera, diferentes partes del sistema operativo pueden correr en diferentes procesadores al mismo tiempo.

La capa de abstracción de hardware oculta los detalles del hardware de multiproceso simétrico del resto del sistema operativo. El kernel de Windows NT trabaja con la capa de abstracción de hardware para manejar los procesadores múltiples. El kernel controla el código que corre en cada procesador en un tiempo dado.

1.3.1.7.2 Modelo de memoria usado por Windows NT

En Windows NT, la memoria se accesa usando un *flat* de 32 bits, un esquema de direccionamiento lineal. El esquema de memoria flat usado en Windows NT contrasta con el esquema segmentado usado en Windows para el sistema operativo MS-DOS. En Windows para MS-DOS, la memoria es partida en muchos segmentos de tamaño variable, cada uno con una longitud máxima de 64K. Este límite de 64K tiene muchas dificultades cuando se crean aplicaciones largas.

Una dirección de 32 bits en Windows NT puede acceder hasta 4 GB de memoria. Cuando una aplicación intenta acceder memoria, simplemente especifica una dirección de memoria de 32 bits. Este esquema de direccionamiento lineal ayuda a que Windows NT sea portable dado que es compatible con el direccionamiento de memoria de procesadores tales como MIPS R4000 y DEC Alpha AXP.

La memoria de usuario está dividida en páginas de 4K.

1.3.1.7.3 Uso de memoria virtual en Windows NT

El archivo de página es llamado PAGEFILE.SYS y, a diferencia de Windows 3.x, no está oculto.

La paginación de datos en el disco incrementa la cantidad de memoria virtual disponible para una aplicación, permitiéndole ignorar la localización de un

segmento de memoria. El término *virtual* es usado aquí dado que el manejador de memoria lleva a cabo la paginación "tras bambalinas" haciendo aparecer como si la computadora tuviera más memoria física de la que tiene actualmente. Efectivamente, la memoria virtual disponible en una computadora es igual a la memoria física más el espacio en disco duro que el manejador de memoria virtual utiliza para hacer swap de código y datos.

1.3.1.8 Aspectos de seguridad en Windows NT

Los requerimientos de seguridad Windows NT proveen la motivación para una variedad de estos aspectos, incluyendo:

- **Mandato Logon** - cada usuario tiene una cuenta y debe dar su password para acceder a ella, lo cual asocia a cada persona con una identificación de usuario. Esto permite a NT identificar usuarios.
- **Control de acceso discrecional** - el propietario de un recurso puede especificar qué usuarios o grupos pueden acceder recursos y qué tipos de accesos tienen permitidos (lectura, escritura, etc.)
- **Protección de memoria** - las tareas no pueden acceder memoria que no tienen asignada excepto a través de mecanismos específicos de compartición.
- El mandato logon y el control de acceso discrecional hacen que Windows NT cumpla con el **rango de seguridad C2** (establecido por el gobierno de los Estados Unidos).

Antes era algo sencillo: Los programadores escribían aplicaciones para un sistema operativo particular, y los usuarios instalaban ese sistema operativo para ejecutar esos programas. Esta correspondencia directa ya no existe. Por esta razón, es una buena idea diferenciar entre productos de sistema operativo e interfaces para programas de aplicación (APIs).

Una API es una definición formal de una colección de llamadas a función (y otros protocolos) que un programa usa para comunicarse con el mundo exterior. La comunicación puede ser un acceso a memoria, un sistema de archivo o una red de área local; el recibir entradas del usuario desde el teclado y ratón; mostrar texto y gráficos en la pantalla o la impresora; capturar y reproducir sonido y música; iniciar otros procesos; dividir un programa en múltiples vías de ejecución; y comunicarse con otros programas.

Normalmente, una API también implica una cierta organización de memoria y datos de un tamaño específico (comunmente 16 ó 32 *bits*), así como los formatos de archivo de los manejadores de dispositivo, los archivos ejecutables y las bibliotecas de enlace dinámico o DLLs.

Un sistema operativo, por otra parte, es una porción de software que trabaja con uno o más APIs y que puede ejecutar programas escritos para esas APIs. En la mayoría de los casos, un sistema operativo apoya una API nativa, y también apoya otras APIs usando capas de traducción.

Windows NT significa el fin de la API sencilla y única de Windows. La API nativa de 16 bits que Windows apoya ahora se llama Win16, y la API nativa de 32 bits que Windows NT apoya se llama Win32. Windows NT también corre la mayoría de los programas escritos para Win16, mediante una capa de traducción que convierte las llamadas de función de 16 bits del programa a las funciones de 32 bits implementadas en el sistema operativo.

Win32 es mucho más que una versión de Win16 de 32 bits. Sus muchas mejoras incluyen multiprocesamiento con prioridad, vías de ejecución, un nuevo sistema de archivo, gráficos extendidos, conectividad, comunicación entre procesos, apoyo para el Unicode y seguridad.

Si no se necesitan las mejoras de Win32, pero es necesario lograr una mejora de rendimiento al crear programas de 32 bits que corren bajo Windows 3.1, hay otra API de Windows llamada Win32s (la "s" significa "subconjunto").

Win32s es básicamente una versión de 32 bits de Win16 sin la mayoría de las mejoras de Win32. Windows 3.1 corre los programas de Win32s mediante capa de traducción que convierte las llamadas a función de 32 bits hechas desde la aplicación, a las funciones nativas de 16 bits implementadas en el sistema operativo.

Algo que hace las cosas más interesantes, es que un ejecutable de Win32s es también un ejecutable nativo de Windows NT. De manera que, los programadores de aplicaciones que crean programas de Win32s para ejecutar bajo Windows 3.1 están creando al mismo tiempo ejecutables de Windows NT (aunque no aprovechan muchas de las características de NT).

En 1993 surge una cuarta API de Windows llamada Win32c (la "c" significa "común", aunque en un momento significó compatible). Win32c es la API nativa de un producto que en la actualidad tiene el nombre de código Chicago.

Win32c es otro subconjunto de Win32, pero mucho más grande que Win32s. Por ejemplo, Win32c incluye múltiples vías de ejecución y muchas de las mejoras gráficas. En efecto, Win32c incluye casi todo lo que tiene Win32 con la excepción de las mejoras de seguridad. Al igual que Win32s, los ejecutables de Win32c son ejecutables nativos de Windows NT.

Tarde o temprano, casi todos los programadores de Windows querrán pasar sus programas existentes a una API de 32 bits. La ruta más directa es Win32s. El

cambio de Win16 a Win32s no es exactamente transparente, pero es mucho más simple que pasar un programa de Windows a la plataforma de la Macintosh o incluso al Presentation Manager de OS/2. Muchos programadores de aplicaciones razonablemente grandes han encontrado que el trabajo básico requiere menos de una semana. El resultado es un programa de 32 bits que logra el máximo impacto en el mercado al ejecutarse bajo Windows 3.1 y NT. En suma, los programadores pueden pasar a Win32s sin arriesgarse en el caso de que Windows NT no sea un éxito.

Avanzar más allá de Win32s para usar las características adicionales de Win32c o Win32 realmente depende de la aplicación. Por ejemplo, las múltiples vías de ejecución son importantes para los programas que pasan mucho tiempo haciendo trabajos grandes. Pero un programa que ya tiene buena respuesta no necesita esta característica.

Con la presentación eventual de la versión final de Windows, Win32c se convertirá en el API más popular. Aparte del código creado para contratos de gobierno que requiere características de seguridad, es probable que sea una rara aplicación la que necesite una característica de Win32 que no tenga apoyo en Win32c. El único problema es que, para algunas aplicaciones, la mejora de rendimiento de 32 bits que se gana al pasar de Win16 a Win32s puede ser contrarrestada por la recarga de la capa de traducción que se necesita en Windows 3.1 para ejecutar programas de Win32s. Esto todavía no puede predecirse con exactitud.

Para una referencia rápida, aquí están las capas y la lista de anotaciones: Win32 es un superconjunto de Win32c, que es un superconjunto de Win32s, que es una versión de 32 bits de Win16. Windows 3.1 ejecuta directamente programas de Win16 y los programas de Win32 mediante una capa de traducción. Windows NT ejecuta programas de Win32, Win32s y Win32c directamente y programas de Win16 mediante una capa de traducción.

1.3.1.9 Aplicaciones de NT

Dar el salto de Windows de 16 bits a Windows NT de 32 bits en una transición importante para la industria de la computadora. Aún así, Windows NT es más que sólo una versión de 32 bits de Windows. Esta ofrece muchos aumentos de funcionalidad sobre Windows, que pueden o no aprovechar las aplicaciones de NT.

Ante todo, los programadores querrán aprovechar el apoyo de múltiples vías de ejecución de Windows NT. Esta característica permite dividir una aplicación en múltiples vías de ejecución que corren simultáneamente. En suma, un programa puede realizar trabajos extensos en segundo plano mientras que sigue respondiendo totalmente al usuario.

Después de unas pocas experiencias con aplicaciones múltiples bien diseñadas, ya los usuarios no tolerarán los familiares indicadores del reloj de arena.

Otra característica segura para las futuras aplicaciones de Windows NT es el apoyo de Unicode que brida NT. El Unicode es una extensión del conjunto de caracteres ASCII que usa 16 bits, en vez de 8, para los caracteres, y que permite la representación de cada carácter en cada idioma escrito que se use probablemente en la comunicación con computadoras (incluyendo los caracteres chinos, japoneses y coreanos), así como algunos juegos de símbolos.

Es probable que el Unicode reemplace a ASCII dentro de algún tiempo y Windows NT es el primer sistema operativo importante que lo apoya. La programación verdaderamente internacional se ha convertido en una realidad.

Los gráficos mejorados de Windows NT son harina de otro costal. Cualquier programa existente que se convierta a Windows NT recibe el rendimiento gráfico de 32 bits de gratis. ¿Pero, qué paso con las mejoras a la máquina gráfica de NT?

Muchas de estas mejoras están en el área de los gráficos de vector, que es la representación de imágenes compuestas de líneas y áreas rellenas. Al arsenal de funciones gráficas de vector que actualmente se encuentra en Windows 3.1, Windows NT añade curvas complejas de Bezier (usadas en el trabajo de diseño), transformaciones de matrices (usada para cambiar de tamaño, inclinar y rotar imágenes) y vías de acceso al estilo PostScrip (usadas para crear contornos complejos arbitrarios usando diversas terminaciones y uniones de líneas).

Sin embargo, en los años noventa, los gráficos de vector han llegado a ser una área especializada, en general relegada al CAD (Diseño Asistido por Computadora) o los programas de dibujo. Dos de los nombres importantes en los gráficos de vector para Windows, Corel y Micrografx, han estado haciendo transformación de matriz y curvas de Bezier por años. No está claro si estas compañías abandonarán sus métodos exclusivos a favor del apoyo incorporado de Windows NT.

Si bien los gráficos de vector se han limitado a un sector de las aplicaciones especializadas, los gráficos de barrido (raster), la captura, almacenamiento, manipulación y reproducción de imágenes de la vida real basadas en los mapas de bits, han pasado tomando la delantera, particularmente en aplicaciones de multimedios. Windows NT ahora apoya la rotación y las máscaras de los mapas de bits (que permite el mostrar imágenes no rectangulares), pero de nuevo, éstas se han convertido en técnicas comunes que no necesariamente requieren apoyo de sistema operativo. Mejoras gráficas más útiles, como la inclusión de la expansión y comprensión de mapa de bits y el color independiente de dispositivo, se destinan para versiones futuras de este sistema operativo.

Los programadores empresariales probablemente estarán menos preocupados por el Unicode y los gráficos, pero probablemente se llamará su atención con otras características avanzadas de Windows NT. Aquí, las características de conectividad y comunicación entre procesos (IPC) de Windows NT son los atractivos principales.

Windows NT apoya los modelos tradicionales de comunicación entre procesos, como "pipes" (un sistema bidireccional de comunicación en el que los programas pueden pasar información de ida y vuelta) y las "casillas de correo" (un sistema de una sola dirección de comunicación en el que un programa deja información para otro). Y sí, estos servicios pueden trabajar en redes y, en efecto, se hicieron para las mismas.

Además, Windows NT también apoya llamadas a procedimientos remotos (RPC), con las que unas aplicaciones pueden arrancarse unas a otras a través de una red para realizar sus operaciones. Otra característica de NT es el DDE de red (network-DDE), una versión para red del intercambio dinámico de datos, un sistema de comunicación entre procesos (IPC) basado en el mecanismo de mensajes de Windows.

Un sistema operativo como Windows NT provee tanto oportunidades como retos para el programador de aplicaciones. En la actualidad, no son posibles los pronósticos precisos. Por ejemplo, quién pudiera haber adivinado hace diez años que una oscura función de DOS denominada "termina y permanece residente" (TSR) hubiera desatado una multitud de aplicaciones nuevas del tipo denominado desplegables (que aparecen y desaparecen de pronto). De forma similar, las verdaderas ventajas de Windows NT aún están por descubrirse.

1.3.2 NetWare

1.3.2.1 Descripción general

Novell Advanced NetWare es un sistema operativo de red independiente del hardware, por lo cual puede correr en una gran variedad de redes. Ha estado en el mercado desde 1983 y es el sistema operativo ampliamente más usado.

Novell desarrolló originalmente el NetWare como el sistema operativo para el equipo Novell-S Net. Una red que utiliza una topología de estrella y un servidor propietario basado en el microprocesador Motorola MC 68000. Debido a que este microprocesador no tenía ningún sistema operativo estándar, Novell decidió desarrollar el suyo partiendo de cero, y lo optimizó para redes; diseñando de paso todas sus características, alrededor de la funcionalidad de la red. Novell es una compañía norteamericana la cual fabrica el sistema operativo para redes (LAN's) más popular: "NETWARE".

Introducido por primera vez en el mercado en 1983 NetWare de Novell es el sistema operativo para redes más conocido en el mercado. NetWare de Novell tiene una base instalada sobre 7 millones de usuarios, 700,000 NetWares vendidos y el mayor porcentaje del mercado compartido de redes.

Estadísticas realizadas por *Fortune* en 1991 nos muestran que Novell tiene la mayor base instalada en Sistema Operativo para red .

La estrategia que Novell ha seguido para su sistema operativo es:

- Independencia de Interface
- Independencia de protocolo
- Independencia de S.O. de la estación de trabajo
- Ser el estándar de estándares en el futuro

Cuando comenzó el éxito de las PC's, los autores de NetWare, vieron que este software escrito con C, podría fácilmente convertirse a la arquitectura de la familia Intel 8088 y que podría soportar virtualmente cualquier red en el mercado. Debido a que el ROM BIOS de la IBM PC XT, fue diseñado para un sistema operativo (DOS) de un solo usuario, con la deficiencia para el ambiente multiusuario ya que el NetWare es particularmente multiusuario, los programadores de NetWare decidieron ignorar el ROM BIOS y decidieron comunicarse directamente con el hardware, para eliminar efectivamente cualquier limitación.

Lograron con ello, permitir a NetWare procesar requerimientos de otra estación de trabajo.

La única desventaja de esta forma de operar, es la imposibilidad de NetWare de utilizar las interfaces (drivers) del DOS, para disco duro. Novell surte estas interfaces para discos compatibles con IBM y muchos fabricantes surten sus propios drivers para NetWare.

NetWare prácticamente no tiene interface, como el ROM BIOS o el DOS cuando se utiliza como servidor de archivos, lo cual permite una mayor velocidad y un mayor grado de seguridad y tolerancia a las fallas. Esto resultaría imposible si se utilizara la estructura de archivos de DOS.

Una LAN Novell tiene dos componentes principales de software:

- Sistema operativo NetWare
- Software de workstation

1.3.2.2 Sistema operativo NetWare

El sistema operativo NetWare reside en el servidor de archivos y controla la compartición de los dispositivos del servidor.

1.3.2.2.1 Software de workstation

El sistema operativo local (normalmente DOS o OS/2) reside en la workstation. El software que actúa como director de tráfico entre NetWare y el sistema operativo local se conoce como *shell* (máquinas DOS) o *requester* (máquinas OS/2). Este programa reside en la workstation. El *shell/requester* intercepta cada solicitud hecha por el usuario y la dirige al servidor de archivos o al sistema operativo local, dependiendo del tipo de solicitud.

Cada estación de trabajo corre bajo su propio sistema operativo. Para definir una estación de trabajo como parte de la red, debe cargarse el shell de la red por encima del sistema operativo de la computadora. El shell conserva muchas de las funciones y comandos del sistema operativo, permitiendo a la estación de trabajo mantener su apariencia normal. El shell meramente añade más funciones y flexibilidad al sistema operativo local (figura 1.17).

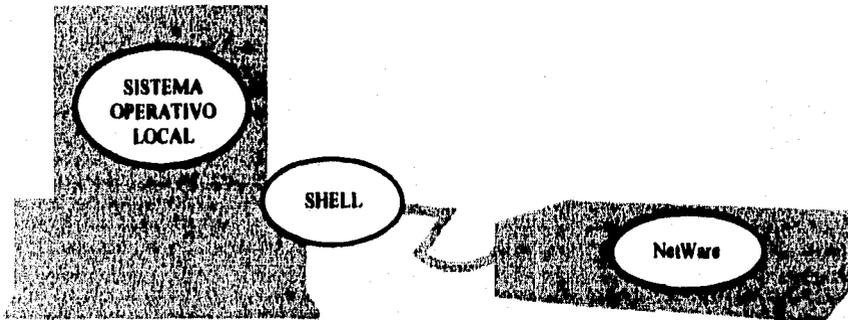


Figura 1.17

1.3.2.2 Shell NetWare (NETx.COM)

El programa NETx.COM contiene el shell NetWare. NETx.COM yace entre la capa de aplicación y DOS, monitoreando todas las transmisiones de datos que se lleven a cabo.

El shell NetWare usa el programa IPX para el logro de las comunicaciones, los siguientes son puntos importantes:

El shell usa el programa IPX (IPX.COM) para asignar direcciones de origen y destino a un paquete de datos.

IPX usa un driver LAN para controlar las transmisiones a través de la tarjeta de red. El driver LAN es parte de un software que sirve de interface entre el sistema operativo o shell y la tarjeta.

IPX.COM es creado cuando se ejecuta el programa WSGEN.EXE durante la instalación en la workstation (figura 1.18).

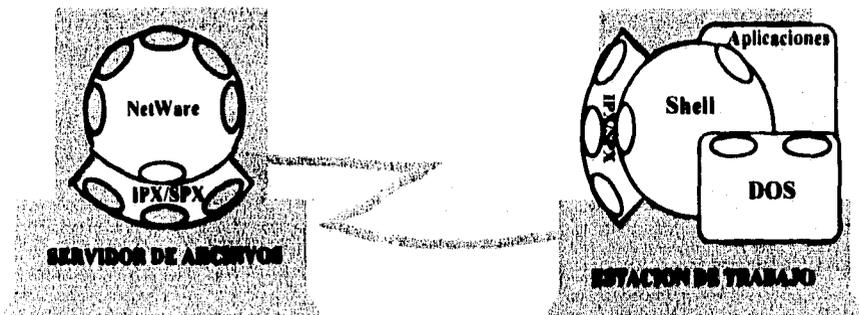


Figura 1.18

1.3.2.2.3 Opciones shell

NETx.COM es el shell estándar, el cual usa memoria convencional DOS; dos opciones adicionales del shell NetWare están disponibles:

Shell de memoria expandida (EMSNETx.EXE)
Shell de memoria extendida (XMSNETx.EXE)

1.3.2.2.4 Shell NetWare de memoria expandida (EMSNETx.EXE)

La memoria expandida es memoria especial adicional más allá del límite de 640KB de memoria principal (convencional). El shell NetWare de memoria expandida es una opción para usuarios de memoria expandida. Este shell:

- Proporciona más espacio de memoria disponible para aplicaciones workstation (aproximadamente 34KB)
- Trabaja con todas las versiones de NetWare.

1.3.2.2.5 Shell NetWare de memoria extendida (XMSNETx.EXE)

Memoria extendida es memoria lineal por arriba del límite de DOS de 1MB. Este tipo de memoria puede ser usada sólo por sistemas operativos o programas que son capaces de direccionarla directamente, tales como NetWare, OS/2 o UNIX.

Tal como el shell de memoria expandida, el shell NetWare de memoria extendida libera 34KB de memoria para proporcionar más espacio para aplicaciones workstation, y trabaja con todas las versiones de NetWare.

Este shell es una opción para usuarios que usan memoria extendida (figura 1.19).

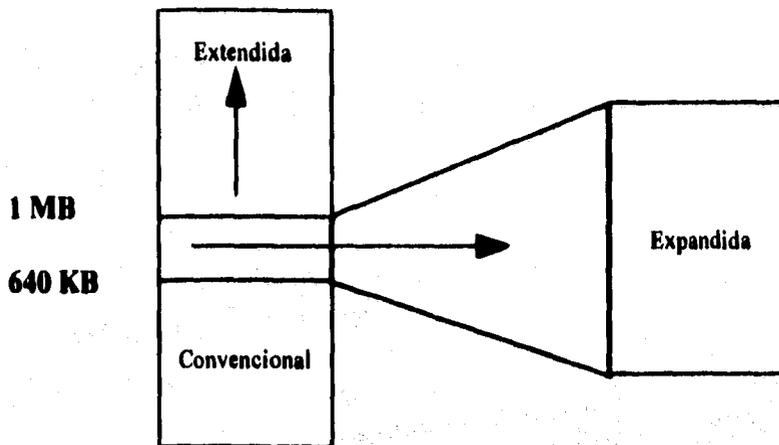


Figura 1.19

1.3.2.2.6 Soporte workstation

NetWare 3.11 proporciona módulos NetWare cargables (NLMs) y soporte para expandir el medio ambiente de la red. NLMs son programas (utilerías) que pueden ser cargadas o descargadas de la memoria del servidor de archivos mientras el servidor de archivos está trabajando.

NetWare v3.11 soporta los siguientes sistemas operativos y medio ambientes workstation, además de DOS y OS/2:

1.3.2.3 Windows

NetWare v3.11 soporta Windows 3.0

1.3.2.4 Macintosh

NetWare v3.11 soporta workstations Macintosh en una red NetWare a través del opcional NetWare para Macintosh v3.0 y sus NLMs asociados que soportan el protocolo AFP.

1.3.2.5 UNIX

NetWare v3.11 soporta workstations UNIX a través del producto opcional NetWare NFS y sus NLMs asociados que soportan el protocolo NFS.

1.3.2.6 OSI

NetWare v3.11 soporta OSI GOSIP a través del uso del producto opcional NetWare FTAM y sus NLMs asociados que soportan el protocolo FTAM (figura 1.20).

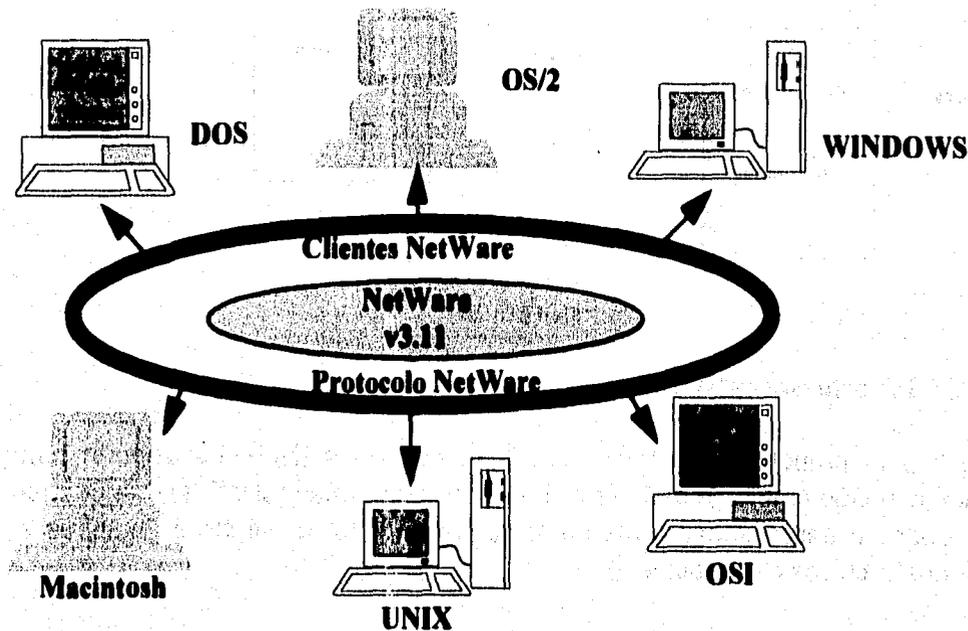


Figura 1.20

1.3.2.7 Protocolos múltiples

NetWare v3.11 permite aumentar las capacidades de la red mediante el uso de múltiples protocolos. Las siguientes interfaces proporcionan esta capacidad:

Interface Open Data-Link (ODI)

Interface STREAMS

Interface de aplicación C-Library (CLIB)

Interface de capa de transporte (TLI)

1.3.2.8 Utilerías

Las utilerías NetWare aumentan la funcionalidad del sistema operativo NetWare. Están clasificadas como utilerías workstation o de servidor de archivos, dependiendo de dónde sean ejecutados los comandos.

Las utilerías workstation se clasifican en utilerías de línea de comando y utilerías de menú. Las utilerías de servidor de archivos se clasifican como comandos de consola y módulos cargables NetWare (NLMs), (figura 1.21).

Las redes NetWare v3.11 son monitoreadas y administradas mediante estas utilerías. Algunas utilerías workstation ofrecen gran funcionalidad cuando son accedidas por un supervisor.

	ESTACION DE TRABAJO	SERVIDOR DE ARCHIVOS
LINEA COMANDO	X	
CONSOLA		X
MENU	X	
NLMs		X

Figura 1.21

1.3.2.9 Aspectos de Performance en NetWare

Las siguientes páginas de esta sección presentan aspectos de *performance* de la familia NetWare.

1.3.2.9.1 Procesamiento distribuido

El procesamiento distribuido es un tipo de procesamiento en el cual cada workstation ejecuta sus propias aplicaciones. Cuando un usuario requiere datos del servidor de archivos, son bajados a la memoria de la workstation y procesados ahí (figura 1.22).

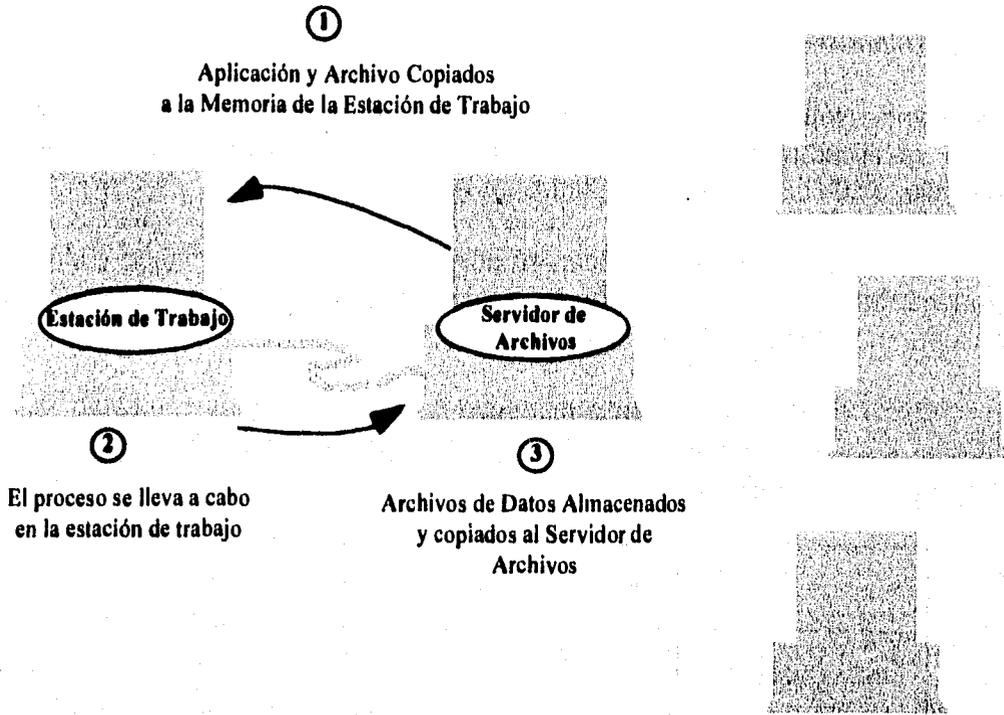


Figura 1.22

1.3.2.10 CACHE del directorio (Directory Caching)

Directory caching es el proceso de copiar la tabla del directorio NetWare (DET) y la FAT del disco duro en la memoria RAM del servidor. Cuando es hecha una petición para almacenar datos en el disco duro, el servidor lee la localización de los datos de la tabla almacenada en memoria. Esto permite al servidor localizar el DET mucho más rápido que si tuviera que leerlo del disco duro (figura 1.23).

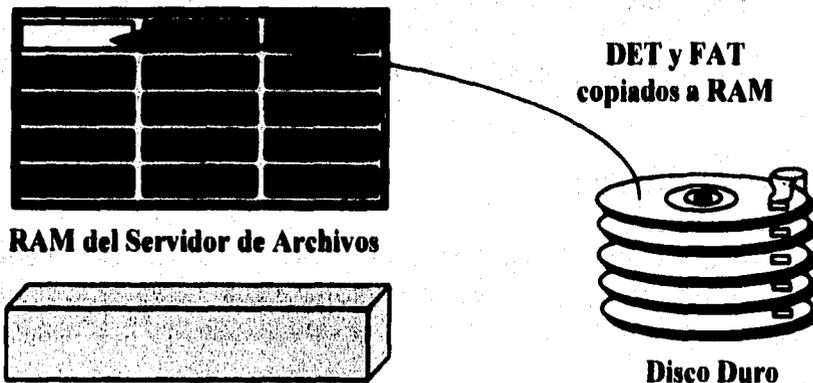


Figura 1.23

1.3.2.11 Directory Hashing

Es el proceso de indexar la FAT. Esto permite al servidor encontrar las direcciones correctas sin examinar todos los datos de las tablas, la ventaja que esto ofrece es reducir el tiempo de respuesta del disco I/O en un 30% en comparación con las tablas FAT no indexadas (figura 1.24).

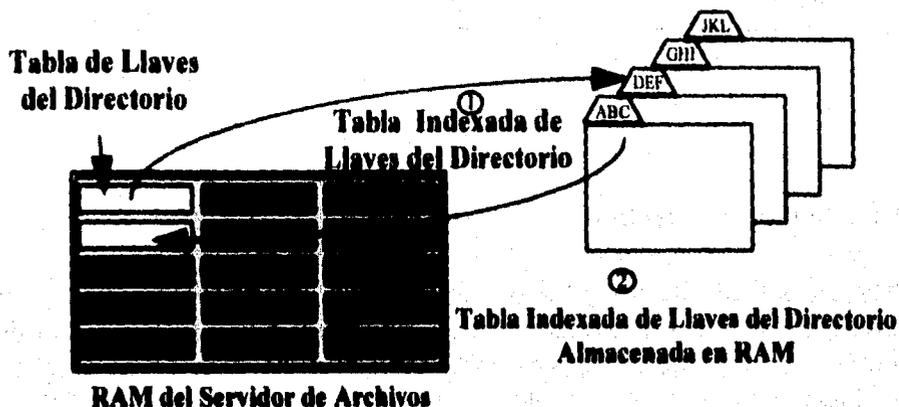


Figura 1.24

1.3.2.12 File Caching

El file caching permite al servidor almacenar en memoria archivos y programas usados con frecuencia. Cuando un archivo es solicitado por primera vez, es llevado del disco a la memoria del servidor donde es almacenado. Cuando este archivo se solicite posteriormente será traído de la memoria RAM del servidor (figura 1.25).

Los archivos caché son accedidos 100 veces más rápido que los archivos que deben ser leídos del disco duro.

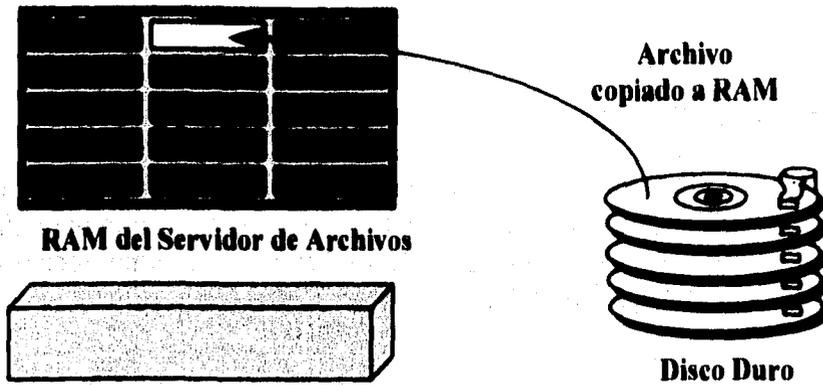


Figura 1.25

1.3.2.13 Elevator seeking

Elevator seeking es un proceso administrador de disco diseñado para priorizar buffers cuando hay solicitudes I/O de acuerdo a sus direcciones de disco. Esto permite a las cabezas lectura/escritura en el disco duro llevar a cabo un fluido movimiento de entrada y salida para la recuperación de los datos. Elevator seeking decremента el tiempo de lectura de disco y por lo tanto, el deterioro del mismo (figura 1.26).

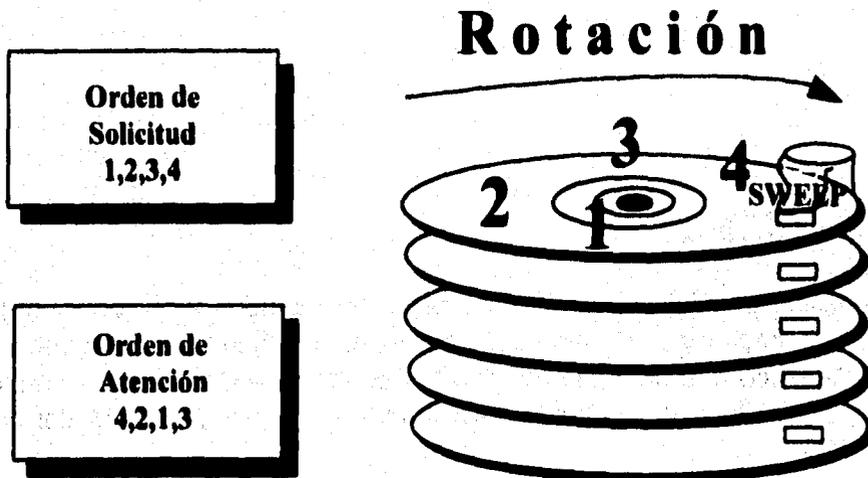


Figura 1.26

1.3.2.14 Capacidades del sistema de tolerancia a errores

El sistema de tolerancia a errores de NetWare 3.11 es de gran utilidad, dado que previene la pérdida de archivos y errores en los datos.

1.3.2.14.1 Proceso de verificación Read-After-Write

Esta característica asegura que los datos escritos al disco duro coincidan con los datos todavía en memoria. Los resultados del proceso de verificación se muestran en la figura 1.27.

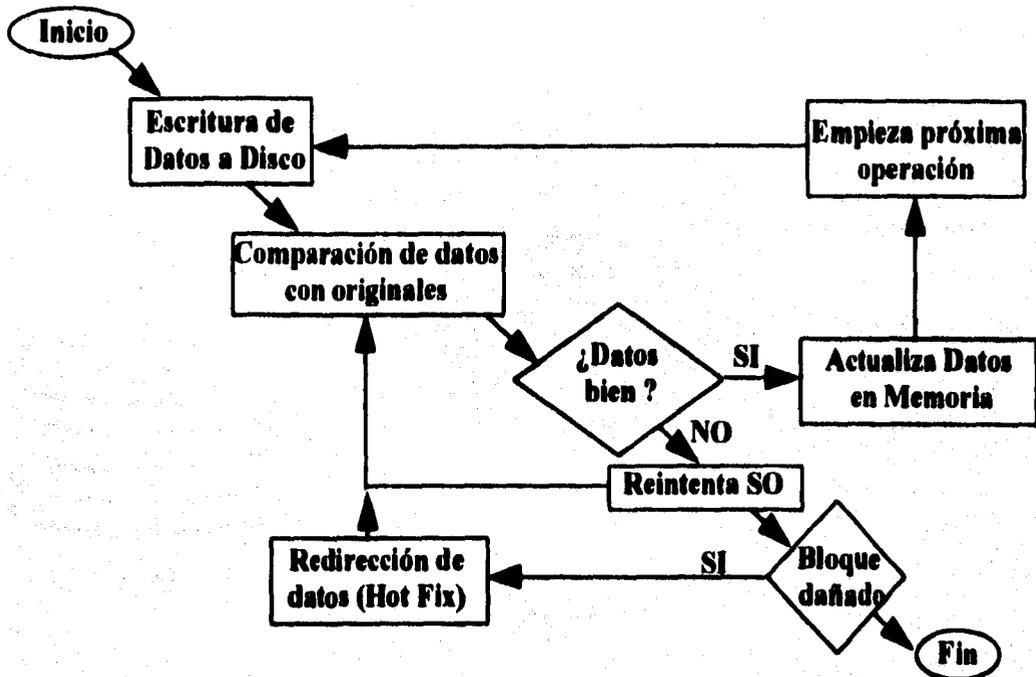


Figura 1.27

1.3.2.15 Duplicación de FATs y DETs

DET's y FAT's contienen las direcciones que el sistema operativo necesita para determinar dónde almacenar o extraer los datos. NetWare automáticamente duplica las tablas en áreas separadas del disco duro para reducir la posibilidad de perder acceso a alguna información almacenada en la red.

Re-mapeo dinámico de bloques dañados (Dynamic Bad Block Remapping (Hot Fix)).

Hot Fix proporciona detección y corrección de defectos de disco. Cuando un bloque dañado es detectado durante una operación de escritura, los datos son trasladados a un área segura del disco y el bloque dañado es marcado como inútil (figura 1.28).

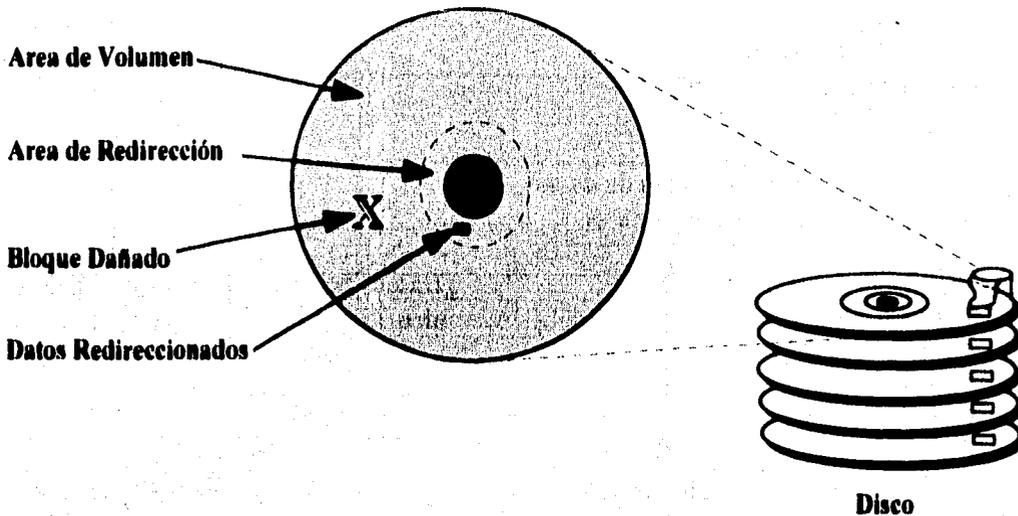


Figura 1.28

1.3.2.16 Disk Mirroring (Disco Espejo)

El disco espejo duplica un disco duro entero en otro disco duro, Si el disco duro original falla, el disco duplicado (espejo) automáticamente entra en acción evitando la pérdida de datos importantes (figura 1.29).

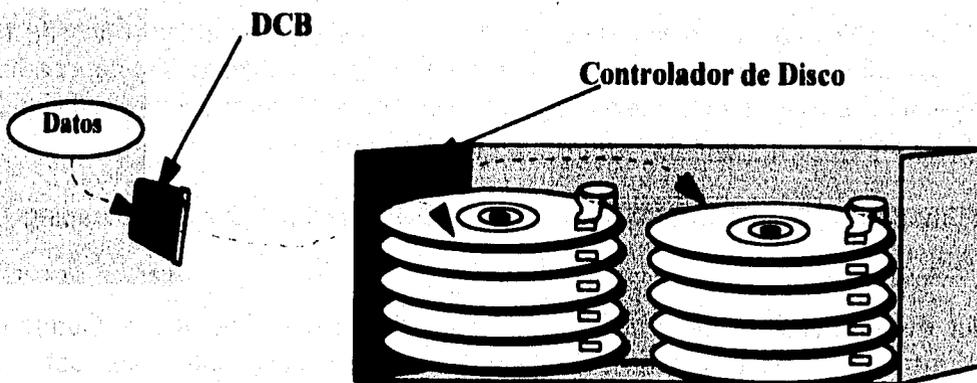


Figura 1.29

1.3.2.17 Disk Duplexing

Disk duplexing duplica la tarjeta coprocesadora de disco (DCB), unidad de cable y controladores; así también el disco duro. La pérdida de datos es prevenida desde el canal del servidor hasta el disk media (figura 1.30).

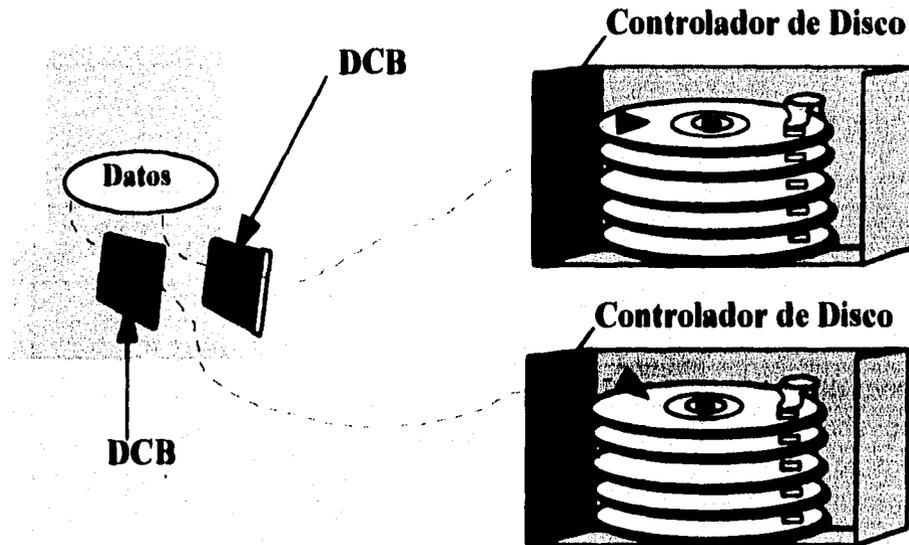


Figura 1.30

1.3.2.18 Transaction Tracking System (TTS)

El TTS es una facilidad para proteger bases de datos de la corrupción causada por actualizaciones incompletas a archivos relacionados. Cuando se combina con Hot Fix y Disk Mirroring o Disk Duplexing, TTS proporciona lo último en sistemas de tolerancia de errores para microcomputadoras.

TTS preserva la integridad de las bases de datos si una aplicación, una workstation o el servidor fallan antes de que una transacción esté completa. En caso de error, TTS automáticamente aborta los cambios a la base de datos al punto previo de consistencia.

1.3.2.19 Monitoreo UPS

Un suministrador de poder ininterrumpible proporciona una fuente de poder estable al servidor y se conecta a subsistemas de discos durante fluctuaciones de poder y cortes de electricidad. NetWare reconoce cuando el UPS activa y advierte a los usuarios el *log out*. NetWare "da de baja" el servidor para asegurar el cierre adecuado de todos los archivos abiertos.

1.3.2.20 Especificaciones de NetWare v3.11

DESCRIPCION	VALOR ACEPTADO EN v3.11
Conexiones lógicas soportadas por servidor	250
Archivos abiertos concurrentes por servidor	100,000
Transacciones concurrentes TTS	10,000
Volumen por servidor de archivos	64
Discos duros por volumen	32
Discos duros por servidor	2,048
Directorios por volumen	2,097,152
Tamaño máximo de archivo	4GB
Tamaño máximo de volumen	32TB
Máximo almacenamiento de disco direccionable	32TB
Máxima memoria RAM direccionable	4GB

Tabla 1.2

La tabla 1.2 detalla las especificaciones técnicas y máximos teóricos de NetWare v3.11.

NetWare v3.11 se ejecuta en cualquier Compaq 386, 486 o máquina compatible. El servidor de archivos NetWare v3.11 requiere como mínimo 4MB de memoria RAM.

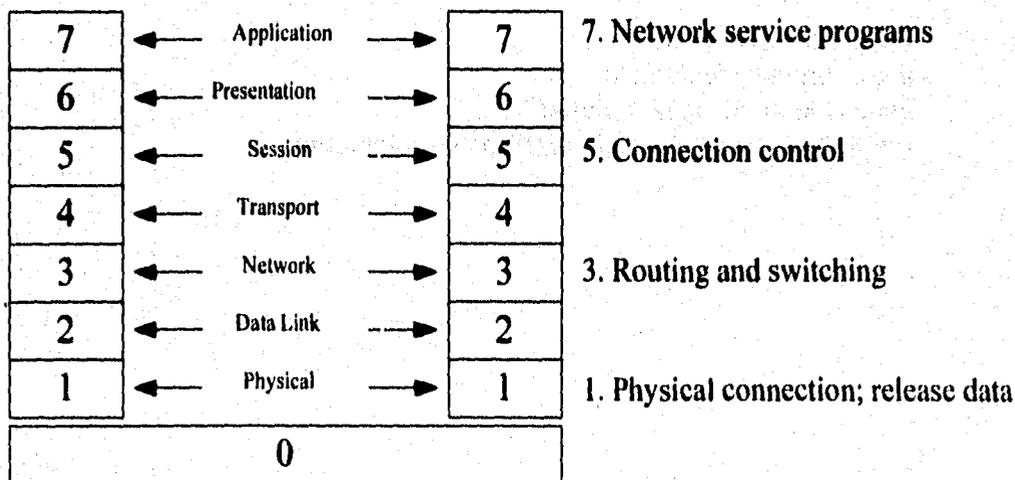
1.3.3 TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) es un compendio de protocolos. El Departamento de Defensa de EUA (DoD) desarrolló estos protocolos a los que posteriormente les llamó de Internet, los cuales se asocian más con sólo un par de ellos TCP/IP. TCP e IP son los protocolos más populares en el medio. TCP/IP fue diseñado para soportar comunicaciones entre hosts conectados por una red. Como sabemos las redes pueden estar conectadas por algunos de los siguientes métodos de comunicación en redes privadas o públicas:

- Transmisión por banda base
- Carriers públicos de transporte
- Redes satelitales
- Radiomóvil
- LAN

TCP/IP es una arquitectura que permite la transferencia de datos entre sistemas. Desde mediados de los 80's todas las arquitecturas han sido comparadas al Open Systems Interconnection (OSI) como modelo de referencia. Una examen de este modelo esencialmente para entender la relación del presente y futuro en la arquitectura de redes.

System A



Modelo OSI de interconectividad de sistemas heterogéneos.

Figura 1.31

TCP/IP es actualmente un conjunto de protocolos para la transferencia de datos entre sistemas heterogéneos. Las tareas específicas para las cuales los protocolos fueron desarrollados incluyen las siguientes:

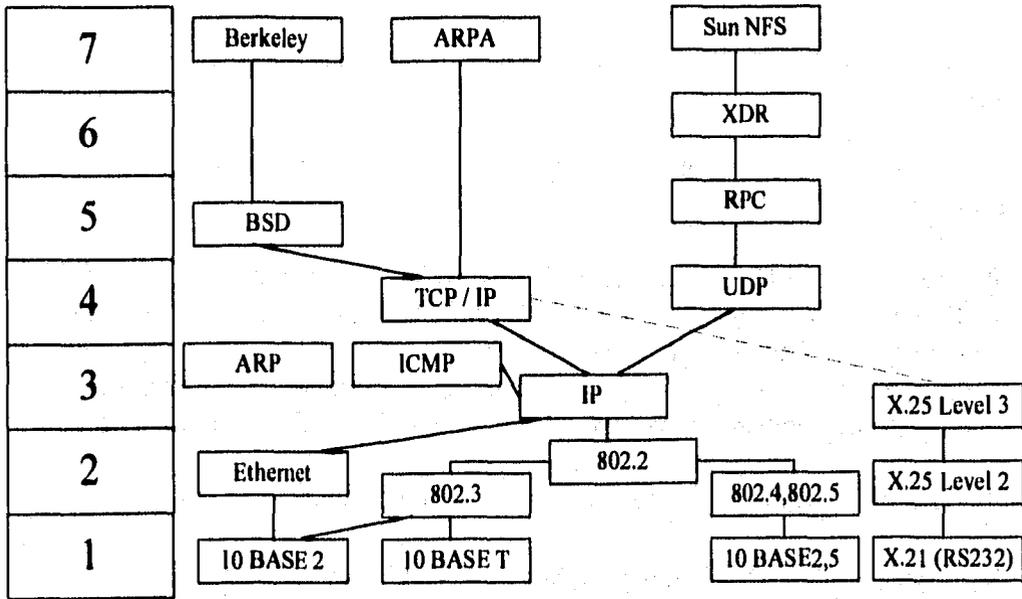
- Acceso al mecanismo de transporte
- Trazo de la(s) rutas para datos
- Reporte de errores asociados con el transporte de los datos
- La presentación de datos
- Acceso a los datos una vez que encuentra su destino

Ya tiene establecidas las capas del enlace y física, las cuales dan la seguridad de los datos y las conexiones físicas, backbone de la red está listo para el transporte de datos por medio de TCP/IP.

TCP fue diseñado para ofrecer el servicio en la capa de transporte, para asegurar la transferencia de datos entre procesos. IP fue diseñado para servir en la capa de red como un distribuidor de datos entre nodos. El Protocolo de Control de Mensajes en Internet (ICMP, Internet Control Message Protocol) es una implementación de IP para reportar errores y controlar los mensajes asociados con la ruta de los datos.

Los protocolos de aplicación fueron diseñados para asignar las funciones de las tres capas superiores, aplicación, presentación, sesión. Las necesidades más comunes se enfocaron a asignar un camino a:

- Conexiones remotas
- Iniciar una sesión remota
- Identificar archivos remotamente
- Controlar la transmisión de archivos remotamente



Protocolos Internet, según el Departamanto de Defensa (DoD) de EUA
 Figura 1.32

Estos se controlan por medio de protocolos algunos de los cuales se listan en la tabla 1.3:

7 Application	ftp telnet bootp tftp named gated	rcp rlogin rexec rwho ruptime sendmail	NFS NIS VHE	Services LAN Link
6 Presentation	SMTp		XDR	
5 Session		BSD IPC	RPC	
4 Transport	TCP	TCP	UDP	
3 Network	IP	IP	IP	
2 Data Link	Ethernet	Ethernet	Ethernet	
1 Physical	Ethernet/IEEE 802.3	Ethernet/IEEE 802.3	Ethernet/IEEE 802.3	

Tabla 1.3

Servicios ofrecidos por los protocolos y servicios basados en las especificaciones del DoD

Existen tres principales entidades que liderean los servicios de las capas superiores:

- **ARPA, sección del DoD encargada de desarrollar servicios basados en TCP/IP**
- **BSD (Berkeley Software Development), servicios desarrollados por la Universidad de Berkeley en base a TCP/IP.**
- **NFS (Network File System), servicios que permiten el intercambio de información completa a otras máquinas que es independiente del hardware.**

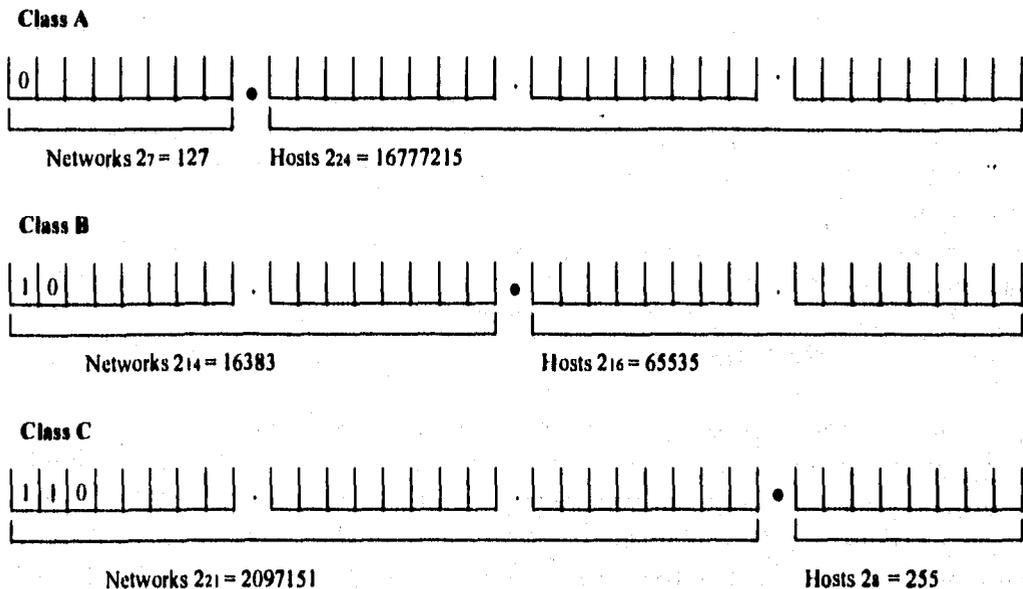
En la capa de transporte se aprecian dos tipos de protocolos:

- **UDP (User Datagram Protocol), que es un protocolo connection less.**
- **TCP (Transport Control Protocol), que es un protocolo connection oriented.**

Como sabemos, un protocolo connection less es aquél que no necesita reconocimiento de transmisión para poder seguir con la secuencia de tramas; es un protocolo mucho muy rápido pero no asegura, en esta capa, la seguridad de los datos.

Un protocolo connection oriented, es aquél que necesita reconocimiento de la transmisión para asegurar la integridad de los datos pero es un protocolo lento.

En la capa de red, observamos a IP junto a un par de protocolos que son el ARP y el ICMP. Como ya se mencionó, IP es un protocolo que permite la distribución de los paquetes para una mejor administración de la(s) red(es). IP se basa en direcciones las cuales se forman de dos partes, una que define el número de Red y otra que define el número de máquina. Estas direcciones son asignadas a través de cuatro octetos; para que su representación sea mucho más sencilla se diseño un método que implica cambiar el valor de los octetos a uno decimal separado cada uno por un punto. Existen varias clasificaciones según el número de redes y nodos que se quieran usar, según se muestra en la figura 1.33.



Asignación de direcciones IP y sus clases.

Figura 1.33

ARP (Address Resolution Protocol) El módulo IP finaliza con el datagram, éste pasó al protocolo de acceso a la red el cual está en el nivel de link. Si el protocolo es LAN entonces el mapeo de dirección es requerido. Nosotros sabemos que la dirección IP es de 32 bits, mientras una dirección LAN es de 48 bits. ARP diseñó la IP para traer la dirección de la LAN cuando ésta es conocida. ARP envía fuera un broadcast requiriendo la dirección Ethernet para dar una dirección IP.

ICMP (Internet Control Message Protocol) IP fue diseñado para proveer algunos significados de reportes de problemas de comunicación, y que deben ser implementados con IP. Los mensajes ICMP son generalmente enviados a reportes con un error cuando se está procesando un datagrama. Otros puntos que se incluyen cuando envía mensajes son:

- El destino inalcanzable
- Los recursos del gateway tienen insuficiente buffer
- El gateway puede identificar una ruta corta

A finales de los 60's la Agencia de Desarrollo de Proyectos Avanzados (ARPA, Advanced Resource Project Agency por sus siglas en inglés hoy DARPA) fue fundada para desarrollar ligas entre sistemas de cómputo heterogéneos. El resultado de esto incluye ARPANET, una red de paquetes conmutados, el protocolo de control de transmisión TCP, el protocolo de internet IP, el protocolo de transferencia de archivos FTP y otros. ARPANET fue el último logro por

Internet, una red masiva a nivel mundial con miles de computadoras y millones de usuarios.

Los protocolos de Internet son diseñados para facilitar procesos multiples sobre diferentes máquinas que se comunican unas con otras a través de una red. El único requisito es que las computadoras deben estar conectadas a través de una red de switcheo de paquetes. Ninguna suposición fue hecha a partir de la naturaleza de la capa baja del medio o para asegurar la entrega de paquetes. En el modelo, las computadoras son conectadas en y hacia varias redes, dentro de una área geográfica delimitada.

Los objetivos del grupo de protocolos de internet fue diferente a los del modelo OSI u otras arquitecturas de redes como SNA o DECnet. Estos protocolos fueron diseñados para ser usados en comunicaciones de computadoras militares, dichas redes y sistemas deben tener disponibilidad y seguridad especialmente durante tiempos de crisis. En resumen, estas redes deberán tener disponibilidad aún cuando halla congestión de paquetes.

Lo relevante de estos protocolos es la eficiencia y la interoperabilidad de sistemas de cómputos diversos residiendo en ambientes de red heterogénea. La guía de conexión es el protocolo de internet, el ahora familiar IP. Protocolos de capas superiores proveen servicios orientados a conexión, como es el caso de TCP, y orientados a no conexión.

Estos protocolos están organizados en cuatro capas que en términos del modelo OSI, pueden ser descritos como la capa de aplicación, transporte, red, enlace de datos y física, la descripción de estas capas es :

- Capa de Aplicación. Es la que contiene las aplicaciones de red; ejemplos de aplicaciones de red incluyen programas para la comunicación interpersonal tales como correo electrónico y bulletin board, emulaciones de terminal virtual (TELNET y Transferencia de Archivo), esta capa contrasta con la del modelo OSI la cual contiene elementos de servicios de aplicación que puede ser combinada con elementos específicos de aplicación para dar forma a un ambiente de aplicación (Aplicaciones de red).

- Capa de Transporte. La primera función de la capa es asegurar conexiones punto a punto; es en esta capa donde programas o procesos sobre diferentes computadoras se hablan directamente unos con otros. Los dos protocolos internet definidos en esta capa son el TCP (Transmission Control Protocol) y el UDP (User Datagram Protocol). TCP provee una conexión basado en el modelo de circuitos virtuales para comunicaciones de red; UDP presta un servicio basado en el modelo de no conexión que es el servicio de datagramas que el protocolo IP presta.

- **Capa de Red.** Habilita a múltiples redes la comunicación a una misma red, el protocolo definido en esta capa es el llamado IP (Internet Protocol). IP proporciona una conexión con servicios de datagramas para protocolos en capas superiores. Es un servicio poco seguro, siguiendo con esta capa, IP provee servicios de ruteo a computadoras y es el encargado de ligar redes y computadoras en la internet.
- **Capa de Acceso al Medio.** Provee el acceso al medio de comunicación con control de flujo opcional y detección de errores y corrección. Este grupo de protocolos puede hacer uso del protocolo que paquetes X.25 para redes de área amplia y especificaciones IEEE 802 como lo son (802.3 Ethernet y 802.5 Token Ring) para acceso a redes locales.

El direccionamiento usado por el grupo de protocolos TCP/IP son llamados direccionamiento Internet. Estos direccionamientos tienen valores de 32 bits que son divididos en números de red y en números de host. Los diseñadores de este tipo de direccionamiento crearon tres clases de direcciones. El direccionamiento clase A tiene el bit de mayor significancia puesto a cero, con los siguientes 7 bits identificando la red y los restantes 24 bits identificando el host. El direccionamiento clase B tiene los primeros 2 bits en 10, los siguientes 14 bits identifican la red y los restantes 16 identifican el host y en la clase C los primeros 3 bits son 110, los siguientes 21 bits identifican la red y los últimos 8 bits identifican el host.

Los diseñadores escogieron estas tres clases de direcciones porque sintieron que las diferentes configuraciones de red pueden ser mejor atendidas con una variedad en la estructura de direccionamiento. Creyeron que podría haber un número pequeño de redes con una gran cantidad de host, una cantidad razonable de redes con número moderado de host y un gran número de pequeñas redes.

1.3.3.1 Gráfica de direcciones

Una idea del flujo de datos es la siguiente. La aplicación del usuario pasa los datos a TCP a través de un API (Application Programm Interface). Es entonces cuando TCP crea una conexión, la conexión al proceso remoto y permite que el IP enrute y transfiera los paquetes de datos hacia la computadora remota. TCP hace esto al pasar los datos, direcciones destino y fuente además de información de control a IP hasta que se reciben los datos en el modo remoto IP le da estos datos a TCP en la computadora remota lugar en el que los datos son almacenados en un bufer. La aplicación remota lee estos datos desde la conexión y es cuando la transferencia está completa.

1.3.3.2 TCP.

Este protocolo asegura la conexión a través de un servicio de circuito virtual para procesos de aplicaciones en comunicaciones de host a host, es la norma para comunicar procesos. Las aplicaciones que requieran una seguridad en la conexión de una aplicación a otra, deberán usar este servicio. Las aplicaciones de red deben interactuar directamente con TCP a través de API's que es una implementación del protocolo, dependiendo del sistema operativo en el host, este API puede crear un componente íntegro del sistema operativo. Las aplicaciones usan llamadas comunes de entrada y salida como open, close, read, write y llamadas que presentan el estado de la conexión.

TCP, que usa un protocolo orientado a conexión requiere que la conexión esté establecida entre los dos procesos. Esto requiere cierto tiempo y esfuerzo para asegurar la transferencia de los datos. Durante el establecimiento de la conexión, parámetros fundamentales que deberán ser usados a lo largo de la conexión son establecidos incluyendo el socket usado la secuencia de números para datos y el tamaño de la ventana para control de flujo.

El punto final de una conexión TCP es llamado socket. Un socket es una combinación de direcciones de red, direcciones físicas y el número de puerto sobre el host local. Puerto es un concepto lógico que habilita a procesos de múltiples aplicaciones para usar el servicio de transporte de TCP sobre la misma máquina. El socket identifica el punto final de la conexión al mandar y recibir los datos anteriores; es por esto que un par de sockets diferentes identifican la conexión.

TCP ocupa tres tipos de handshake para el establecimiento de la conexión, los paquetes enviados tienen banderas de control que indican el proceso de entrega en particular las banderas de sincronía(synchronize SYN y el acuse de recibo(acknowledgment ACK) son usadas de la siguiente manera:

- 1) Computadora 1 envía un SYN con un número de secuencia a la computadora 2.
- 2) Computadora 2 envía un ACK y SYN (Ambos enviados en un sólo mensaje) a la computadora 1 con el número de secuencia.
- 3) Computadora 1 envía un ACK con el número de secuencia a la computadora 2.
- 4) La conexión está terminada al intercambiar segmentos con la bandera de control FIN.

1.3.3.3 Encabezado TCP

El segmento TCP está implícito en el datagrama de IP para transferencia sobre la red. Porque IP está interesado en obtener el paquete del destinatario en la red, esta dirección está contenida en el header de IP y no en el de TCP. De igual manera ya que el puerto es un concepto de TCP, los puertos fuente y destino son almacenados en el header de TCP, éstos tienen un valor de 16 bits.

El número de secuencia tiene un valor de 32 bits que contiene la secuencia del primer octeto de datos en el segmento. También tiene el efecto de ACK, todos los datos recibidos arriba del número de secuencia menos uno.

El campo de Data Offset es un delimitador al inicio del header para indicar el inicio de datos. Los siguientes 6 bits están reservados para un uso futuro y su valor debe ser 0.

El campo para las banderas de control tienen una longitud de 6 bits y su significado es el siguiente:

URG (Urgent) Indica que el apuntador de urgente contiene un valor significativo.

ACK Indica que el acuse de recibo contiene el número de secuencia esperado.

PSH (Pushed) Indica que los datos deben ser enviados inmediatamente y no almacenados antes de transferirlos.

RST (Reset) Informa a TCP que la conexión debe ser inicializada

SYN Bandera de control para establecer una conexión y sincronizar los números de secuencia.

FIN Indica que ya no existen más datos a transmitir y desea terminar la conexión.

La ventana es un campo de 16 bits que contiene el número de octetos que el receptor puede aceptar, después de un ACK.

1.3.3.4 UDP (User Datagram Protocol)

El UDP usa IP para proveer los procesos de aplicación con un protocolo de datagramas sin reglas en la capa de transporte, habilitando a las aplicaciones a comunicarse sin la sobrecarga de la conexión y desconexión. Como IP, UDP no garantiza la entrega de paquetes no provee secuencias de paquetes o supresión

de duplicación de los paquetes. Aplicaciones que requieran este tipo de servicios debe considerar a TCP.

UDP es útil para aplicaciones que pueden tener sus razones para implementar su propia secuencia de entrega de paquetes y confiabilidad. En estos casos los servicios que provee TCP pueden dejar de usarse esperando una considerable baja en la carga. El formato del header UDP es el siguiente:

1.3.3.4.1 UDP Header

Source Port an Destination Port. Especifica los puertos de proceso de la aplicación que envía y recibe respectivamente.

Length. La longitud del paquete UD incluyendo el header y los datos.

Checksum. Un cómputo de 16 bits que verifica que los datos fueron transferidos sin daño.

1.3.3.5 IP (Internet Protocol)

IP provee un servicio de datagramas inseguro orientado a no conexión para la conmutación de datos sobre una red de conmutación de paquetes. También provee facilidades para fragmentar grandes paquetes para la transmisión y el reensamble en las estaciones receptoras. IP no provee control de flujo, secuencia o supresión de duplicación alguna.

IP usa tanto TCP como UDP para rutear y entregar paquetes a través de la red. El segmento de TCP (header y datos) está localizado en la sección de datos del datagrama IP. IP debe ser implementado en cada host que esté conectado a la red y que sea capaz de rutear paquetes sobre la red local.

IP usa una estructura jerárquica de las direcciones internet y rutea cada datagrama independiente del otro.

1.3.3.5.1 Header del datagrama IP

Versión. Denota el formato del header IHL (Internet Header Length) es el inicio de los datos, el valor de este campo está multiplicado por 32 bits para indicar el valor del delimitador.

Type of Service. Campo de 8 bits que contiene el valor que indica la calidad del servicio a proveer en ciertas redes. Un ejemplo del tipo de servicios es *Precedence*, el cual asigna prioridad para asignar paquetes.

Total Length. Campo de 16 bits que contiene la longitud del header y los datos juntos. Este campo de 16 bits asigna un límite en el tamaño del datagrama de 65 535 octetos por lo general, las implementaciones en IP mantienen este campo en 576 octetos para asegurar que puedan pasar a través de cualquier ruteador en la red.

Identificación. Usada por la máquina que recibe para reensamblar datagramas fragmentados.

Flags. Campo de 3 bits que indica la fragmentación de datagramas.

Bit 0. Está reservado y siempre es 0.

Bit 1. Indica si el datagrama está o no fragmentado.

Bit 2. Indica si el paquete es el último fragmento o si existen más fragmentos.

Fragment Offset. Campo de 13 bits y que muestra la localización del fragmento en el datagrama. El valor de este campo está multiplicado por 8 octetos para determinar el octeto delimitador del fragmento en el datagrama. Un datagrama es fragmentado cuando quiere pasar a través de una red que tiene definido un tamaño de paquete más pequeño que el datagrama. El datagrama no será fragmentado si la bandera de no fragmentar (don't fragment) está indicada, en este caso el datagrama será descartado y un reporte será enviado al fuente a través del ICMP.

Time to live: Campo de 8 bits que especifica el tiempo máximo que un datagrama puede existir en la red antes de que sea atrapado en algún ciclo indefinido dentro de la red y sea destruido. La unidad de tiempo es el segundo; el campo es para intentar prevenir que un datagrama navegue indefinidamente por la red.

Protocol. Campo de 8 bits que especifica el protocolo que creó los datos y que el datagrama debe entregar al host remoto.

Checksum. Un cómputo de 16 bits que verifica que los datos fueron transferidos sin daño.

Source & Destination Address. Campos de 32 bits cada uno que contiene la dirección internet para el host local y remoto respectivamente.

Options. Campo de longitud variable que es opcional en el datagrama. Casi siempre los host y ruteadores que implementan IP deben soportarlo si está presente.

1.3.3.6 Internet Control Message Protocol (ICMP).

Este protocolo es usado para notificar de errores que ocurrieron en la entrega de datagramas a través de la red. Generalmente el host destino o un ruteador interno es quien origina este mensaje. Este dispositivo puede mencionar que el destino es inalcanzable o que el ruteador no tuvo los suficientes buffers para almacenar y pasar (Store & Forward) el datagrama. El mensaje puede contener información referente al transmisor y la ruta más corta a usar.

ICMP es un requisito para cada dispositivo que usa IP y es una parte esencial de IP. ICMP usa IP para entregar los mensajes de control esta relación de IP que crea con ICMP en si es insegura, lo que quiere decir que la entrega de mensajes de control no está garantizada. Por esta razón no existen mensajes de control relacionados con ICMP.

Los mensajes de ICMP se distinguen uno de otro por el primer octeto de la porción de datos en el paquete IP y ellos habilitan al modulo ICMP para interpretar y manejar estos mensajes.

Cuando el header de IP está construido, el ruteador o host lo usa como dirección fuente si un error se presenta. El destino es la dirección del mensaje inicio.

Echo replay. Respuesta si cualquier envío presenta el mensaje. El número de secuencia puede ser usado para determinar qué petición de echo se está respondiendo.

Destination Unreachable. Información concerniente a las siguientes condiciones: la red fue inalcanzable, el destino fue inalcanzable, el puerto destino fue inalcanzable o un paquete no se pudo fragmentar. Varios de los mensajes regresan al header de IP y los primeros 64 bits del campo de datos en el datagrama inician el mensaje ICMP.

Source Quench. Envía por un ruteador o el destino indica que los datagramas están llegando tan rápido que no tiene espacio en su memoria o poder de procesamiento para manejarlo. El mensaje a la estación transmisora es para reducir su tasa de paquetes enviados.

Redirect. Enviado por un ruteador cuando descubre una ruta más corta al destino en su propia tabla de ruteo. Este mensaje no es enviado si el datagrama está haciendo uso de la información fuente/ruteo.

Echo. Una petición para que el destino conteste con un mensaje echo replay. Esta respuesta es un acuse de recibo que el datagrama pudo llegar al destino.

Time Exceeded. Enviado por un ruteador si éste notifica que el campo time to live en el datagrama ha expirado. El ruteador usa este mensaje para informar al transmisor que se ha descargado el datagrama. Un host puede mandar este mensaje si es imposible reensamblar los fragmentos de un datagrama.

Parameter Problem. Enviado por un ruteador o host que fue forzado a descartar un datagrama porque encontró algo críticamente mal en el header del datagrama. El mensaje también contiene un apuntador indicando la localización del error en el header.

Timestamp. Información reunida acerca del tiempo requerido para alcanzar un destino. El transmisor llena en los 32 bits el tiempo que le toma (medido en milisegundos), usando UTC (Universal Time Coordinate) como referencia.

Timestamp replay. Respuesta a un mensaje timestamp; contiene un timestamp de cuando el datagrama fue recibido por el destino y un timestamp de cuando la respuesta fue enviada. La aplicación del cliente es libre para usar esta información de cualquier manera.

Information Request & Information Replay. Usada por el host para determinar el número de red a la que está conectada. Estos mensajes son definidos en la especificación del protocolo pero generalmente no son implementados.

1.3.3.7 Routing Information Protocol (RIP)

Como se mencionó antes, las redes basadas en IP fueron creadas para separar redes interconectadas a través de ruteadores. Estos ruteadores son los responsables de direccionar los mensajes entre redes cuando el nodo destino no está localizado en la misma red local. La tarea de los ruteadores es encontrar la ruta más corta hacia el destino.

Para hacer esto, los ruteadores contienen sus tablas de ruteo, el mantenimiento y uso de estas tablas es responsabilidad del RIP para asegurar el intercambio de información entre ruteadores.

El RIP de internet es muy similar al RIP de XNS(Xerox Network System). El RIP de XNS está basado en el gateway information protocol el cual fue un componente del grupo de protocolos PUP.

El protocolo RIP tiene la ventaja de intercambiar un mínimo de información para mantener al día las tablas de ruteo. RIP tiene la limitación de alojar sólo 15 saltos

como máximo para alcanzar una red. Para RIP 16 saltos representan al infinito. Otras limitaciones adicionales son que RIP no toma en cuenta las condiciones de la red en tiempo real como los son el congestionamiento u otros retrasos cuando se calcula la distancia entre redes.

Las redes que se quieren mantener ocultas deberán tener el valor de la distancia en 16 que significa infinito. Cada ente en la tabla de ruteo contiene la siguiente información:

IP Address. Dirección IP del destino.

Distance. Mide que tan lejos se encuentra el destino del host o del ruteador fuente, y mide el costo de enviar el datagrama hacia el destino. En muchas de las implementaciones, la distancia está medida en número de saltos (hops o ruteadores) que el datagrama debe atravesar para alcanzar el destino.

Next hop. La dirección IP del próximo ruteador al cual necesita llegar el datagrama para enviarlo lo más cerca de su destino final.

Change Flag. Bandera indicadora de que ha ocurrido alguna modificación en la información del ruteo para esa entrada.

Interface. Interface de red la cual debe ser usada para enviar el datagrama al próximo ruteador o host.

Timers. Usado para asignar tiempos a cada entrada en la tabla. Existen 2 timers para cada entrada. El primero indica el tiempo que le queda a la entrada antes de ser considerada sin uso y ser considerada para ser borrada. Generalmente este valor es de 180 segundos cuando la entrada es creada o actualizada. El segundo es un timer controlado que actúa cuando la ruta es removida de la tabla.

RIP hace uso de UDP para el intercambio de información. Ambos envían y reciben procesos usando el well-know port número 520. Algunos dispositivos como son host, pueden escoger un proceso que escuche ese puerto y crear una tabla de ruteo de la información que están escuchando.

RIP propaga la información de su tabla de ruteo a cada ruteador cada 30 segundos. En resumen responden a peticiones explícitas para información ruteada. Finalmente, cuando la distancia ha sido actualizada para cada entrada, RIP crea el cambio para mandarlo a los ruteadores conectados.

1.3.3.7.1 Estructura del paquete RIP

El paquete RIP puede contener más de 25 entradas de información ruteada. Usando el campo de comando en el paquete RIP un sistema puede pedir toda o parte de la tabla de ruteo para que se la transfieran y puede responder a peticiones de informaciones de ruteo al enviar parte o toda su tabla de ruteo.

El **Address Family Identifier (AFI)** especifica el protocolo a la que la información de ruteo se refiere. Esto habilita a RIP a usar protocolos que no se encuentran en el grupo de protocolos de internet.

La petición a un ruteador para mandar toda su tabla de ruteo como una respuesta, prepara al transmisor un paquete de RIP con una entrada para usar un AFI de 0 y especificar la métrica a 16.

1.4 Interconectividad de redes

Con el rápido crecimiento de las redes en los 80's viene la necesidad de conectarlas y enlazarlas para crear una infraestructura de cómputo sólida. Lo anterior es llamado internetworking, que da razón al crecimiento de las redes corporativas conectando minis y mainframe. Para crear estos bloques de redes empresariales existen dispositivos de interconectividad de redes como lo son bridge, switch, routers y gateway.

Hand-in hand con LANs juntos es la necesidad de organizar los resultados de redes dentro de unidades de jerarquía administrable. Los dispositivos internetworking son usados no sólo para ligar LANs sino para crear también estructuras de redes que proveen un nivel de performance y que puede ser administrado con razonable esfuerzo.

Primero internetworking tuvo la necesidad de ligar todas las computadoras usuarias en una organización, proporcionando comunicaciones del ancho de la organización. El correo electrónico es aún la aplicación primaria para redes corporativas. Porque el slogan del mercado "la red es la computadora" es lento pero seguro; como quiera, la importancia de construir una infraestructura de una red sana está creciendo. La industria de la computación observa que tiene que declarar que el futuro es la distribución de computadoras, con un estilo de computadora en la cual cada aplicación individual corra simultáneamente en más de un computador sobre la red.

Esto no es un conjunto de fórmulas para construir una red del ancho de la organización. Comienza con una instalación base de aplicaciones, sistemas operativos de redes, protocolos, computadoras, y cableando, mencionando que la

espera de la instalación base es en 5 años, y esto es una mezcla con el resultado de la instalación y el presupuesto.

Varios factores determinan los números y tipos de dispositivos. El factor principal es el tráfico de red.

Porque las organizaciones de redes encuentran diferentes protocolos y tipos de computadoras, teniendo un marco común de referencias que son importantes. El desarrollo de protocolos de redes TCP/IP, IBM, SNA, DEC, DECNET, y PC LAN tienen múltiples niveles que pueden ser mapeados por la séptima capa del modelo OSI.

1.4.1 Séptima capa del modelo OSI

1.4.1.1 Repetidores

El nivel más bajo del modelo de referencia OSI, la capa física cubre cableado y señal eléctrica. El dispositivo que opera en la capa física es llamado un *repetidor*. Cada repetidor recibe una transmisión en un segmento LAN y regenera la señal, son usados para levantar la transmisión débil, así que los segmentos LAN pueden ser grandes.

Una Ethernet puede consistir de 2 tipos de segmentos: segmentos coax y segmentos link. El segmento link utiliza repetidores (actualmente, half-repeater - ellos son usados en pares) para extender el rango de la red para conectar algunos segmentos coax. Una Ethernet sólo consiste de segmentos coax y link es un segmento lógico. Este puede ser considerado un solo Ethernet.

Los repetidores no son actualmente dispositivos internetworking porque ellos sólo extienden segmentos individuales. Pueden ser usados para piezas de conexión de cable. Ethernet soporta, teóricamente, un máximo de 1,024 nodos por segmento lógico, por ejemplo, y el número puede ser excedido sólo por usar más de un segmento. No importa cuántos repetidores son usados o que tan grande sea el segmento, el límite de nodos se sigue aplicando. Más importante aún, los repetidores no corren software alguno y no son parte significativa del tráfico en la red más allá de transmisión de señales eléctricas.

Los repetidores deben considerarse más como parte del sistema de cableado, que parte del plan de internetworking. Debe usar repetidores cuando se requiera que los nodos sean conectados a su red, ya sea dentro de los 500 m que ofrece un coaxial grueso o de los 100 m que ofrece el UTP. El retraso de los paquetes debido a los repetidores es una limitante del número de segmentos de cable que estén conectados a él. En el caso Ethernet no se pueden separar 2 nodos por más de 4 repetidores en el mismo segmento.

1.4.2 Internetworking en la capa de enlace de datos

El rol de internetworking inicia en la segunda capa del modelo OSI, la capa de enlace de datos. Esta capa cubre la comunicación entre dos nodos adyacentes porque cada dirección de enlace (dirección MAC, dirección física, dirección Ethernet, dirección de enlace, etc.) corresponde a la dirección de enlace de un nodo en particular de la red.

En la capa de enlace, los pulsos eléctricos que forman la cadena de bits es organizada en paquetes.

Los tres tipos de red más ocupados (Ethernet, Token Ring, FDDI) tienen definida en su mayoría las características de esta capa. Internetworking sobre esta capa tiene el objetivo de ligar redes del mismo tipo, aunque la generación más reciente para estos productos pueden conectar FDDI a Ethernet y a Token Ring.

Ethernet forma una red CSMA/CD (Carrier Sence Multiple Access / Collision Detection) es un medio donde se rolan los papeles en el cual todos los nodos escuchan cada transmisión en el cable. Un nodo listo a transmitir verifica el cable y si no hay transmisión ésta ocurre. Si dos o más nodos intentan transmitir al mismo tiempo, la transmisión se colisiona. El nodo que envía detecta la colisión y espera un intervalo de tiempo aleatorio antes de tratar de transmitir. Ethernet opera a 10 mbits por segundo.

Token Ring utiliza como medio un aro, en el cual un token es pasado de nodo a nodo. El nodo que esté listo a transmitir espera a que el token arribe. Sólo el nodo que tenga posición del token puede transmitir. El nodo receptor marca el paquete transmitido para indicarle que tiene una copia de la transmisión. Cuando el paquete regresa al nodo que lo envió con un acuse de recibo, este nodo lo remueve y regresa el token al anillo. Los paquetes deberán ser removidos del ciclo porque el primer bit del paquete retorna a la estación que lo envió antes de que el último bit del paquete halla sido transmitido. Hay dos versiones normalizadas de Token Ring: una opera a 4 Mbits y la otra 16 Mbits por segundo.

FDDI es una red de Token Passing. A diferencia de las redes de Token Ring instaladas en ambiente de PC'S, casi siempre opera a 100 Mbits por segundo y tiene dos anillos para redundancia. FDDI fue diseñado para operar sobre cables de fibra óptica dando oportunidad a que los nodos estén a distancias mayores a dos kilómetros.

El dispositivo internetworking usado en esta capa es el llamado bridge. Los bridges consisten en interfaces al medio, buffers, tablas de direcciones y uno o más procesadores; son dispositivos que almacenan y envían (store and forward).

Los paquetes recibidos se almacenan en su bufer, verifica la dirección del paquete en su tabla de direcciones y, dependiendo si el fuente o destino se encuentran en el mismo segmento, esté descartado para enviarlo a otro segmento de la red, aunque los bridges basados en conmutación tienen mayor performance y están disponibles ahora.

Los bridges pueden ser traducidos, encapsulados, transparentes o, en el caso de tener varios bridges de Token Ring, ruteo de fuente. Bridge, encapsulación y traducción son usados entre diferentes tipos de redes. Bridge de traducción convierte los paquetes de red de un tipo a otro. Bridge de encapsulamiento encapsulan paquetes o fragmentos de paquetes desde el nodo transmisor dentro de paquetes del nodo receptor.

La mayor ventaja de los bridges es segmentar una red y controlar tráfico entre grupos de trabajo y backbound de la red. Cuando la carga de tráfico sobre un segmento de la red comienza a causar problemas de rendimiento, la solución más fácil es reducir la carga. La mejor forma de reducir la carga es al reducir el número de nodos en el segmento de red.

Al segmentar las redes con bridges, esto es usando bridge para dividir la red en segmentos adicionales, comienza a aumentar necesariamente tanto más usuarios que queden en línea y como las aplicaciones que usen más recursos sobre la red. Antes de segmentar la red se deben mapear los patrones de tráfico para determinar quién genera a quién y qué usuarios ocupan más recursos.

La manera más recomendable para segmentos sobrepoblados es la llamada regla 80/20 la cual dice qué: "el 80% del tráfico en la red es propia de ésta y no cruza en bridge". Se debe verificar esta regla, si el tráfico debe cruzar enlaces de área amplia por cualquier punto porque los enlaces de este tipo son lentos y mucho más caros que el uso de LANs.

La segmentación es una operación táctica en la cual los bridges no tienen uso en relación al problema. Los bridges son por lo general de más ayuda como herramientas estratégicas cuando se planea una red o una extensión de una red.

1.4.3 Conmutadores LAN

Ha surgido una nueva clase de dispositivos de internetworking. Estos dispositivos tienen una tecnología de conmutación orientada a conexión, asociada con telecomunicaciones, contra el tradicional ambiente de datagramas orientados a no conexión de las LAN. Estos dispositivos tienen la misma aplicación que un bridge multipuerto, crean ligas virtuales entre nodos individuales en diferentes segmentos y permiten conexiones simultáneas múltiples.

Los conmutadores son dispositivos *cut-through* y no *store and forward* (ellos envían los paquetes sin almacenarlos). Ya que los conmutadores no almacenan paquetes provocan un retraso mínimo. La latencia (tiempo en que un paquete sale del dispositivo) de estos dispositivos es de microsegundos comparado con los bridges que pueden ser de milisegundos.

Una baja latencia es importante para protocolos o aplicaciones que tienen un tamaño de ventana muy pequeño. Ya que un tamaño de ventana pequeño implica que el acuse de recibo debe ser detectado en el emisor antes de que un paquete adicional sea enviado.

Ya que los conmutadores crean circuitos virtuales, crean un medio compartido de un incompartido. Al eliminar el problema de la competencia entre nodos para acceder a la red, los conmutadores crean más redes determinantes. Esto es necesario para aplicaciones que requieren una baja tasa de retraso, como lo es la video conferencia.

1.4.4 Enrutamiento en redes

El dispositivo de internetworking que corresponde a la capa de red es el ruteador. Las redes individuales pueden contener desde una cantidad manejable de nodos a miles de ellos. La mayoría de las redes basadas en ruteadores de medio a gran tamaño son jerárquicas, con alguna definición de ruteo de las fronteras entre zonas, niveles, dominios o grupo de redes.

Justo como un bridge maneja los protocolos en la capa de enlace, los ruteadores manejan protocolos específicos en la capa de red usados por los nodos para comunicar y comunicarse unos con otros. Algunos ruteadores son programados para manejar un solo protocolo de red, así como otros manejan más de una docena. Muchos protocolos en esta capa pueden existir, por lo menos uno para cada tipo de sistema operativo y varios si se trabaja con varios sistemas operativos. Ya que el ruteador examina cada paquete a nivel de red, éste opera independientemente de los protocolos de la capa de enlace como Ethernet o Token Ring.

El IP del grupo de protocolos de TCP/IP y los servicios de red orientados a no conexión (CLNS, Connection Less Network Services) y servicios de red orientados a conexión (CONS, Connection Oriented Network Services) del grupo de protocolos OSI envuelven al mundo de UNIX pero han sido extendidos a varios sistemas operativos. Muchos sistemas operativos de redes de PC's usan una adaptación del XNS. LAN Manager, Ungermman Bass y Net One usan XNS. Novell Netware, usa el Internet Packet Exchange (IPX), una derivación del protocolo XNS. Banyan Systems Virtual Network System (VINES) usa el VINES Internet Protocol (VIP), el

cual también usa una derivación del XNS. Otro grupo de protocolos importante de sistemas operativos propietarios incluyen a Appletalk y Decnet Phase 4.

Como dispositivos de capa de red, los ruteadores no conectan capas de enlace. Como resultado un ruteador puede conectar diferentes redes tan largas con las interfaces de más de un tipo de red. Usando ruteadores es muy simple conectar redes Token Ring y Ethernet.

La función básica de un ruteador es la de transmitir paquetes entre redes. Ya que las redes usualmente tienen más de un camino entre ellas, estos dispositivos deben encontrar la mejor ruta para enviar los paquetes. La mejor ruta está determinada por algoritmos de ruteo, una variedad de los cuales se han desarrollado en los últimos 30 años.

La mejor ruta, depende de un rango de criterios incluyendo entre ellos la distancia el *hop count*, ancho de banda y carga. La distancia determina el tiempo en que el paquete viajará a través del enlace, éste es llamado retraso de propagación. *Hop count*, determina el retraso provocado por cada dispositivo internetworking. El ancho de banda determina cuánto tráfico puede transmitir un enlace. Este criterio es conocido como el costo por ruta y la mejor ruta es conocida como la ruta de costo más bajo.

Los ruteadores originales fueron los mainframes o minicomputadoras corriendo software de ruteo como una de varias aplicaciones o como un ruteador dedicado. Ruteadores de este tipo involucran a Internet, en la cual una computadora universitaria fue conectada directamente a la red.

Así, el software utilizado en los ruteadores de hoy es diferente y considerablemente más complejo que el software usado en bridges; el hardware es muy similar. De hecho, muchos de los fabricantes de ruteadores han añadido el bridging a sus propios productos en los últimos 5 años. La combinación bridge/router, algunas veces conocida como *brouters*, han empezado a reglamentar esta relación, ruteando cualquier protocolo que soporte y ocupando el bridge para el resto. Rutear algunos protocolos y puentear otros es de gran utilidad para redes que trabajan con protocolos que no pueden ser ruteados como el Transporte de Area Local de DEC que es un protocolo de comunicación entre terminales y host.

De acuerdo a un estudio realizado por la Universidad de Harvard acerca del rendimiento entre bridge y router, no existe diferencia con configuraciones similares.

Los ruteadores son necesarios para crear redes muy grandes o para participar en una red mucho mayor como la Internet. Para crear una red organizada

jerárquicamente es mejor estratificar una, que necesitar los manejadores de tráfico mas sofisticados que los ruteadores proporcionen.

Se puede crear una red ocupando solamente ruteadores. Hoy día es mejor utilizar ruteadores para aislar grupos de trabajo del backbound, ya que los ruteadores no tienen una diferencia significativa con los bridges. Si se tiene un router por cada par de workstation la red no será complicada.

Si se desea no utilizar estos dispositivos y la red sólo tiene unos cuantos cientos de usuarios, se puede hacer. Pero si la red formará parte de una más grande, o su expectativa de crecimiento es muy significativa, deberá prepararse para el desarrollo de una red basada en ruteadores.

Determinar cómo interconectar sus redes depende de cuántas redes tenga, de qué tipo sean, dónde están localizadas, qué protocolos y qué tanto tráfico generan, así como la configuración en la estructura o el esquema de distribución de cables.

CAPITULO 2 FUNDAMENTOS DE ATM

En este capítulo se describen los elementos teóricos que conforman las especificaciones de ATM, se estudian modelos matemáticos y los esquemas de capas superiores. Se analizan también algunos aspectos de diseño de hardware en un conmutador ATM.

2.1 Fibra Óptica

2.1.1 Introducción

El desarrollo de redes que transmitan a gigabits (redes gigabit) está ligado a los desarrollos en fibras ópticas. En realidad, el advenimiento del equipo de señalización de fibra óptica capaz de transmitir a diferentes gigabits por segundo a grandes distancias con bajos rangos de error a través de fibra óptica (comunmente conocida con el nombre de "fibra") mostró que las redes gigabit eran factibles y sirvieron como motivación a los investigadores.

Dado que la fibra y sus propiedades juegan un papel importante en las redes gigabit, es importante tener al menos conocimientos básicos acerca de las propiedades de la comunicación por fibra óptica y cómo esas propiedades afectan el diseño de redes gigabit. Proporcionar una visión de las fibras ópticas es el propósito primario de este capítulo.

Otras tecnologías de transmisión están siendo perfeccionadas para que también sean capaces de transmitir y recibir información en rangos de gigabits. Aunque con menos desarrollo y con menos influencia que la fibra, estos medios son parte de las redes gigabit.

2.1.2 Lo esencial de las fibras ópticas

El campo de las fibras ópticas ha aumentado desde que los investigadores empezaron a examinar el potencial que representaban las pocas pérdidas en la transmisión usando luz en fibras.

2.1.2.1 Refracción y fibra

Es una interesante propiedad de la luz que consiste en que cuando se envía luz de una sustancia a otra, ocurren dos cosas: parte de la luz es reflejada y parte pasa a la nueva sustancia. Sin embargo, los rayos de luz que entran a la nueva sustancia, son usualmente modificados de su ángulo original (fenómeno conocido como refracción). Este comportamiento es ilustrado en la figura 2.1. La luz que llega (el rayo incidente) se muestra golpeando en el límite entre dos sustancias. Una parte de la luz es reflejada y otra es refractada.

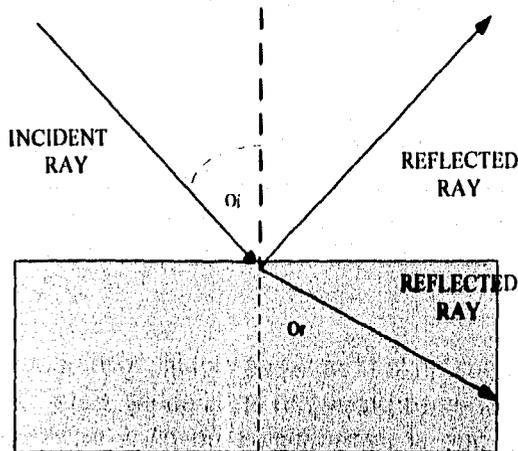


FIGURA 2.1: REFLECTION AND REFRACTION OF LIGHT

La cantidad que un rayo angula cuando refracta entre dos sustancias es determinada por el *índice de refracción* de cada una de las dos sustancias y la longitud de onda de la luz enviada. Diferentes longitudes de onda de luz angulan de diferentes maneras - el fenómeno explica cómo los prismas separan la luz en colores. El índice de reflexión mide cuánto angula la luz cuando entra a una sustancia. La relación de los índices de las dos sustancias determina cuanta angula la luz cuando se mueve de una sustancia a la siguiente. En particular, la relación de los senos del ángulo de incidencia, O_i , y el ángulo de refracción, O_r , son iguales a la relación de los índices de refracción de las dos sustancias.

La cantidad de luz reflejada y refractada varía, dependiendo de los índices de refracción de las dos sustancias a través de las cuales está pasando la luz y el ángulo en el cual la luz golpea el límite entre las dos sustancias. Si la luz incide perpendicularmente, la luz refractada pasa en forma recta. Si la luz incide en ángulo, parte de la luz es reflejada en el mismo ángulo y parte es refractada en un ángulo diferente. Sin embargo, si la luz incide en un ángulo mayor a cierta cantidad, llamado el *ángulo crítico*, entonces la luz es completamente reflejada. El ángulo crítico es el valor de O_i cuyo seno es igual a la relación del índice de refracción de la segunda sustancia dividida por el índice de refracción de la primera sustancia.

Utilizando las propiedades de refracción, es posible crear finos hilos de fibra de vidrio que pueden transmitir luz a través de largas distancias. Un hilo de vidrio, llamado *núcleo*, es envuelto con otra capa de vidrio ligeramente diferente, llamado

revestimiento. El núcleo y el revestimiento tienen diferentes índices de refracción, donde el del núcleo es mayor que el del revestimiento. Como resultado, la luz enviada en línea recta bajo el núcleo permanecerá en él, dado que si trata de escapar a través del revestimiento será reflejada al interior del núcleo. Gracias a la transmisión de luz a través del núcleo es posible enviar bits en forma de pulsos de luz.

El índice de refracción tiene otra parte significativa. El índice de refracción mide qué tan rápido los fotones viajan a través de la fibra. Para fibra óptica, el índice de refracción es de alrededor de 1.45, lo que significa que la velocidad de la luz en la fibra es aproximadamente 0.69 de la velocidad de la luz en el vacío o alrededor de 2.1×10^8 a 8 m/s .

Observe que la velocidad de la luz en la fibra no es significativamente diferente de la velocidad a la cual los electrones se propagan en el cobre. Esta observación es importante dado que significa que si transmitimos un bit a través de la misma longitud de fibra y cobre, al bit le tomará el mismo tiempo llegar a través de la fibra y del cobre. Lo que distingue a la fibra del cobre es la densidad de información o ancho de banda.

Para ver como el empaquetar más bits por unidad de cable puede afectar el diseño del protocolo, considere el problema de tratar llevar las reglas de transmisión de Ethernet a velocidades de gigabits.

En Ethernet cada nodo está siempre escuchando a la red y puede iniciar una transmisión sólo cuando la red está en silencio. La red es un medio de transmisión en el cual cada nodo puede escuchar la transmisión de cualquier otro nodo. Para prevenir situaciones en las cuales dos nodos empiecen a enviar al mismo tiempo, los nodos deben escuchar sus transmisiones, y si el dato que el nodo lee de la Ethernet no coincide con el dato que fue puesto en la misma, se dice que ha ocurrido una *colisión*. Cuando ocurre una colisión el nodo detiene el envío y espera un tiempo antes de tratar de enviar de nuevo.

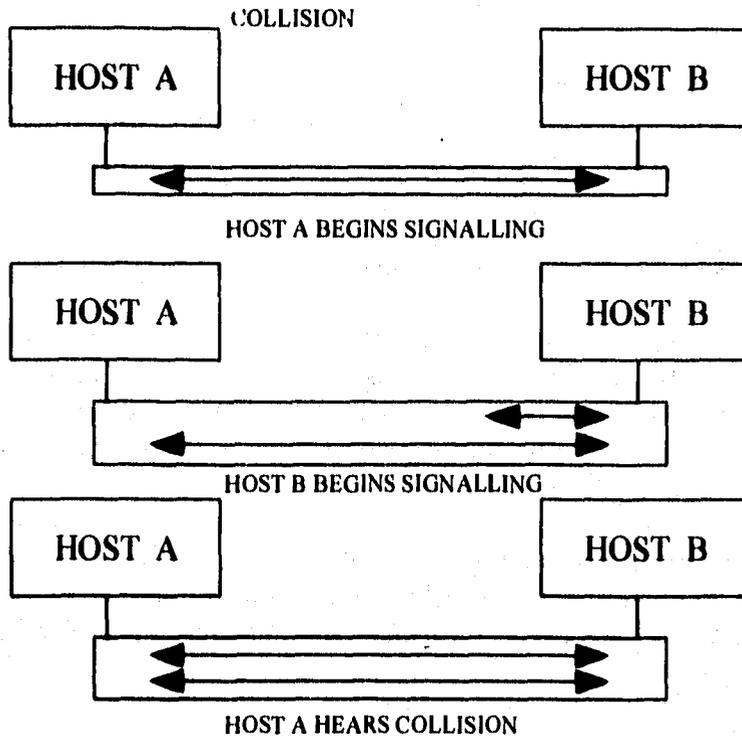


Figura 2.2

Como se ilustra la figura 2.2 para la detección de una colisión Ethernet y recobrar el esquema para trabajar adecuadamente, la red debe de tener un tamaño mínimo de paquete. Considere el ejemplo mostrado en la figura 2.2. El Host A, que se encuentra en un extremo del cable Ethernet empieza a transmitir un paquete. El Host B, es la terminal colocada en el otro extremo del cable. Justo antes del primer grupo de bits del Host A alcanza a Host B, el Host B empieza a enviar. Es importante guardar en mente que hasta que los bits de "A" alcancen al Host B, la red aparecerá en silencio para el Host B. Ahora, observe que el Host A, escuchará la colisión sólo después de que los primeros bits del paquete del Host B han atravesado el cable hasta llegar a Host A. Así, si queremos estar seguros de que el Host A escuchará una colisión antes de detener el envío necesitamos asegurar que el Host A transmitirá al menos el doble de la longitud del cable en bits. En una Ethernet a 10 megabits, el tamaño mínimo del paquete es de 64 bytes para 5 Km de cable. Pero en un Ethernet a 1 gigabit, el tamaño mínimo del paquete es de cerca de 6,400 bytes.

Desde una perspectiva arquitectónica, 6,400 bytes, está muy lejos del tamaño mínimo de paquete. Este requeriría de paquetes pequeños (ej. 40 a 60 bytes de largo); para incluir cientos de bytes como relleno para proteger contra colisiones y esto causará el uso ineficiente del ancho de banda de la fibra.

El punto de este ejemplo es que si tratamos de usar el gran ancho de banda de las fibras, seremos incapaces de usar algunos esquemas de transmisión existentes, como Ethernet. La lección particular es que el costo de asegurar la detección de colisiones en redes de alta velocidad es lo suficientemente grande, para que deba hacerse de otra manera.

2.1.2.2 Capacidad de ancho de banda de una fibra

El ancho de banda de una fibra está determinado por el total de luz que puede llevar. Debido al número de factores físicos, la luz pasa fácilmente a través de la fibra en sólo 3 partes del espectro óptico. Estas bandas son cada una, de cerca de 200 nanómetros (nm) de ancho y son centrados alrededor de la longitud de onda de 0.85, 1.3 y 1.5 micrones.

Cada una de las 3 bandas tiene cerca de 25 terahertz (THz) de capacidad. Los estándares de equipo de señalización pueden señalar entre 1 y 1.4 bits por Hz, entonces una sola fibra puede ser usada para transmitir entre 50 y 75 terabits por segundo.

En realidad, la tasa de capacidad del bit es un poco menos. Crear dispositivos de señalización rápidos es caro; es más efectivo crear diferentes dispositivos de señalización paralelos que transmitan en diferentes longitudes de onda en la misma fibra, práctica llamada multiplexado de la longitud de onda (Wave Length Division Multiplexing o WDM). WDM es análogo a la forma en que las ondas de radio son multiplexadas a través de varios canales. Y como en los canales de radio, algún hueco es dejado entre señalamientos de longitud de onda para asegurar que las señales no se interfieran mutuamente. Pero aun si uno deja espacios entre los canales, una sola fibra puede ser usada para transmitir decenas de terabits por segundo.

2.1.3 Un ejemplo de señales de fibra óptica: SONET

Después de ver como las fibras ópticas pueden ser usadas para señalización de bits, es ahora tiempo de demostrar como los componentes de fibra óptica pueden ser usadas para construir un red. Como ejemplo inicial, examinaremos la Synchronous Optical Network (SONET). Sonet es un ejemplo bastante trivial dado que es una manera primaria de reemplazar el alambre de cobre con fibra. El objetivo es aumentar los rangos de transmisión en líneas telefónicas, usando pocos cables (porque una fibra puede reemplazar varias líneas de cobre) y empleando un protocolo de señalización más flexible que el usado para cobre.

Pero Sonet, no sólo ilustra algunas de las transmisiones básicas usadas para fibra. Es también el protocolo de transmisión usado en fibra de compañías

telefónicas y como resultado, es uno de los más comunes protocolos de transmisión sobre fibras. Además, si uno renta fibra de alguna compañía telefónica, es probable que use frames Sonet. En verdad muchos investigadores creen que debido a que la comunidad de teléfonos proporcionará un gran mercado para chips de señalamiento Sonet, los chips de Sonet pueden estar disponibles para todos los que usan señalización Sonet para enlaces de fibra punto a punto.

2.1.4 SONET y SDH

Sonet es parte de una larga serie de estándares telefónicos conocidos como Synchronous Digital Hierarchy (SDH), estandarizado por (CCITT), el organismo mundial de estándares telefónicos.

El SHD fue desarrollado para soportar multiplexaje en enlaces de datos de cientos de megabits o más. El objetivo del SDH es desarrollar un solo grupo de estándares para enlaces de alta velocidad. Actualmente, hay 3 grupos de estándares para multiplexado telefónico en bajas velocidades: el estándar de U.S.A., el estándar Japonés, que es muy parecido al de USA y el de CCITT, el cual es usado casi en todo lugar menos en EUA y Japón. Por ejemplo, los EUA usan un estándar T1 para multiplicar juntos circuitos de voz de 2.464 Kb/s en enlaces a 1.5 Mb/s, donde el equivalente CCITT es un circuito E1, el cual multiplexa 32 circuitos de voces en 2 Mb/s. Debido a los estándares diferentes, la conexión internacional de redes telefónicas es algunas veces difícil. Por ejemplo, para conectar redes telefónicas a EUA, una compañía telefónica en Suecia tiene que rentar líneas en una ruta a través de Dinamarca, Países Bajos, Francia y Reino Unido para obtener fibra transatlántica a los EUA. Si distintas compañías de teléfonos tienen diferentes líneas de transmisión, entonces construir un circuito conectado se torna difícil porque cada salto tiene diferente tipo de señalamiento. Mediante el desarrollo de estándares consistentes de multiplexaje para altas velocidades, muchos de estos problemas pueden ser eliminados.

TABLA 2.1: SONET/TRANSMISSION RATES

Data Rate (Mb/s)	SONET STS/OC Designation	CCITT STM Designation
51.84	1	-
155.52	3	1
622.08	12	4
1,244.16	24	8
2,488.32	48	16

La tabla 2.1 muestra parte de las jerarquías de transmisiones Sonet/SDH. Porque Sonet empezó como un estándar de EUA y fue entonces incorporada en los estándares del CCITT para SDH, hay 3 diferentes formas de describir un rango de datos dado.

Bajo el estándar Sonet, el primer rango de datos en la jerarquía es 51.84 Mb/s, y es designada Synchronous Transport Signal Level 1 (STS-1) u Optical Carrier Level 1 (OC-1). Numerar bajo el esquema STS/OC indica cuántos circuitos STS/OC-1 pueden ser encapsulados en un rango dado. Por ejemplo STS-12, en 622.08 Mb/s equivale a 12 circuitos STS-1. De hecho, una línea STS-12 puede ser usada como 12 circuitos STS-1, cuatro circuitos STS-3, o como una línea a 622 Mb/s de un solo canal. Si el circuito está siendo usado por un solo canal, es llamado línea concatenada y designado mediante una *c* después del número; por ejemplo: OC-3c.

Los rangos de datos del CCITT empiezan con 155.52 Mb/s, el cual es Synchronous Transport Module Level 1 (STM-1). Como la numeración del esquema Sonet, el esquema CCITT cuenta en múltiplos: así una porción de datos STM-4 es igual a 4 veces la rango de datos STM-1 y es posible traducir entre valores STM y STS simplemente multiplicándolo por 3.

Si bien, todo el rango de velocidades de multiplexaje ha sido definido, de hecho sólo un grupo limitado será usado. Por ejemplo, los estándares completos de circuitos de multiplexaje telefónico a través de enlaces STM, existen sólo para rangos de datos OC-3, OC-12 y OC-48 (STM-1, STM-4, STM-16).

La razón de esta selección de estándares es que las diversas redes telefónicas no han sido planeadas para cambiar sus rangos de multiplexaje para bajas velocidades, y el multiplexado eficiente de circuitos de baja velocidad de EUA y CCITT es posible sólo en algunos rangos de datos.

El uso selectivo de rangos de datos OC es importante para la gente interesada en Sonet para comunicaciones de datos, tal como algunas de los rangos de datos no útiles para telefonía, son muy interesantes para la comunicación de datos. El ejemplo más obvio es OC-24, que tiene un rango de datos de 1.2 gigabits y es una rango lógico de datos usado como enlace entre LAN's a velocidades de gigabits. Diferentes LAN's a velocidades de gigabits propuestas tienen anchos de banda entre 800 megabits y 1 gigabit por segundo. Si se coloca una línea Sonet entre dos LAN's de 800 megabits, una línea OC-12 es claramente lenta, pero una línea OC-48 lo es mucho más. Sin soporte para OC-24 dentro de las redes telefónicas, no es claro que existirá un mercado para componentes OC-24. Si las redes telefónicas no soportan OC-24, entonces es obvio que no comprarán chips OC-24. Además, si las redes telefónicas no soportan OC-24, entonces los usuarios no podrán contratar líneas OC-24, por lo tanto, tampoco comprarán circuitos integrados OC-24 para sus computadoras.

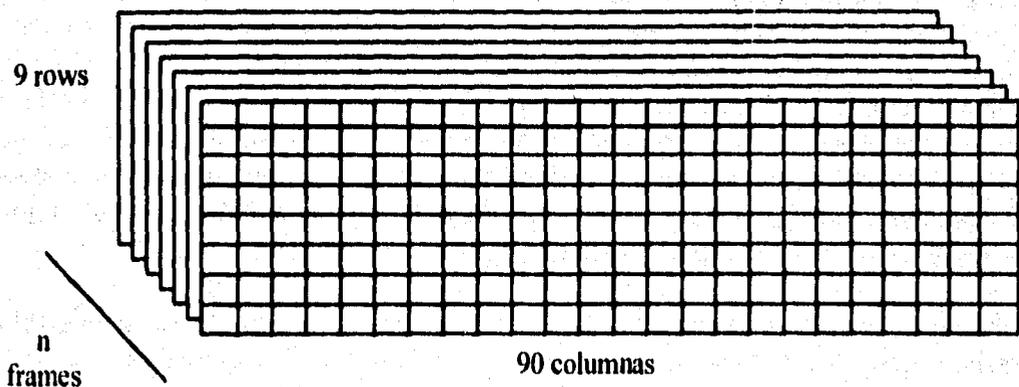


Figura 2.3

2.1.5 Como trabaja SONET

Sonet transmite datos en *frames*. Cada frame es pensada lógicamente como una parte bidimensional de bytes, con 90 columnas y 9 renglones (ver figura 2.3). Para un rango de datos OC-n dado, la unidad de transmisión es de "n" frames. Entonces OC-1 transmite datos frame por frame, pero OC-3 maneja transmisiones en grupos de 3 frames.

Las primeras 3 columnas (27 bytes por frame OC-1) están reservadas para transportar información. Las primeras tres filas son llamadas "sección regeneradora de gastos" (regenerator section overhead) y las últimas 5 filas son llamadas "The multiplexor section overhead". El regenerador de sobrecarga es procesado por cada repetidor Sonet. El multiplexor de sobrecarga es procesado por multiplexores Sonet. Los repetidores simplemente renuevan las señal Sonet en una fibra, pero los multiplexores combinan y extraen canales de datos individuales de dentro de las estructuras Sonet.

La cuarta fila del transporte contiene un indicador. El problema clave en multiplexión es que las líneas sujetas a un multiplexor comúnmente obtiene fuera de sincronización con cada una. Cada línea tiene su propio mecanismo de tiempo para manejar la transmisión y recepción de bits y por razones como la variación en la onda de la fibra antes mencionada, el reloj de diferentes líneas comúnmente varía. Ahora considerando el problema de tomar cuatro canales OC-3 de diferentes fibras y multiplicándolos dentro de un byte integrado canal OC-12. Esto puede ser claro que el tiempo relativo de cuando la estructura llegue de diversas fibras variarán sobre el tiempo. El indicador es usado para adaptarse a esas variaciones. Sonet permite a los datos el empezar a manejar bytes en una carga y el medidor indica en qué parte de la carga empiezan los datos.

En suma, una columna en cada 90 x 9 estructuras (frame) puede ser usada para colocar información múltiple dentro de datos (llamado path overhead). Si este path overhead aparece sólo en la primera estructura de 90 x 9, entonces el canal Sonet es concatenado.

Frame A1	Frame A2	Interleave C1
Party B1*	EOW E1*	User F1*
	Regenerator Data Comm D1 thru D3	
Pointer H1	Pointer H2	Pointer H3
Error Detect B2*	Protection K1*	Swiching K2*
Multiplex Data Comm D4 through D12*		
Zero Bytes		EOW-2 E2*

Figura 2.4

La estructura de 3 columnas de transporte de información general es mostrado en la figura 2.4 como definida OC-1. En altas estructuras, el byte del principio aparece sólo en la primera estructura 90 x 9; los otros bytes pueden ser repartidos en estructuras posteriores.

La mayoría de los campos sirven para funciones obvias. Los bytes A1 y A2 de una estructura alineada en palabra, usada para sincronizar el comienzo de cada bloque de 90 x 9. El byte C1 es usado para interfolear estructuras STS (una porción mucho mejor que OC-3).

El byte B1 y B2 son errores de chequeo en la sección de regeneración y la sección multiplexor overhead respectivamente. Los bytes E1 y E2 son usados para proveer un canal de voz 64 Kb/s para atender en cada una de las secciones de regeneración y la sección multiplexor. El F1 byte es un canal de alarma de 64 Kb/s. Bytes D1 a través de D3, y D4 a través de D12 proveen canales de comunicación de datos para manejo de redes entre regeneradoras y multiplexores.

Los canales de comunicación de datos son de interés porque son usados para señalar el equipo Sonet. Usando estos canales un usuario puede dar instrucciones a los multiplexores para cambiar la rutina de los canales Sonet, haciendo posible construir una red interruptor Sonet en la cual las conexiones entre nodos diferentes de redes Sonet estén bajo el control del usuario.

Debe ser claro que Sonet está diseñado cuidadosamente para conocer los requerimientos de pase telefónico de datos en largas distancias. Por ejemplo, la

presencia de canales con voz para mantener canales personales y de alarmas son, innecesarios si Sonet es para ser usado como el protocolo estructural entre dos comunicaciones de datos cercanos en un edificio de oficinas. La mayor ventaja de una especificación es que debe hacer lo posible para construir fácil (y presumiblemente menos caro) el señalamiento de hardware Sonet.

2.2 Modelo de referencia de protocolo B-ISDN.

La figura 2.5 muestra el modelo de referencia de B-ISDN, el cual consiste en tres planos :

- Plano de usuario
- Plano de control
- Plano de supervisión

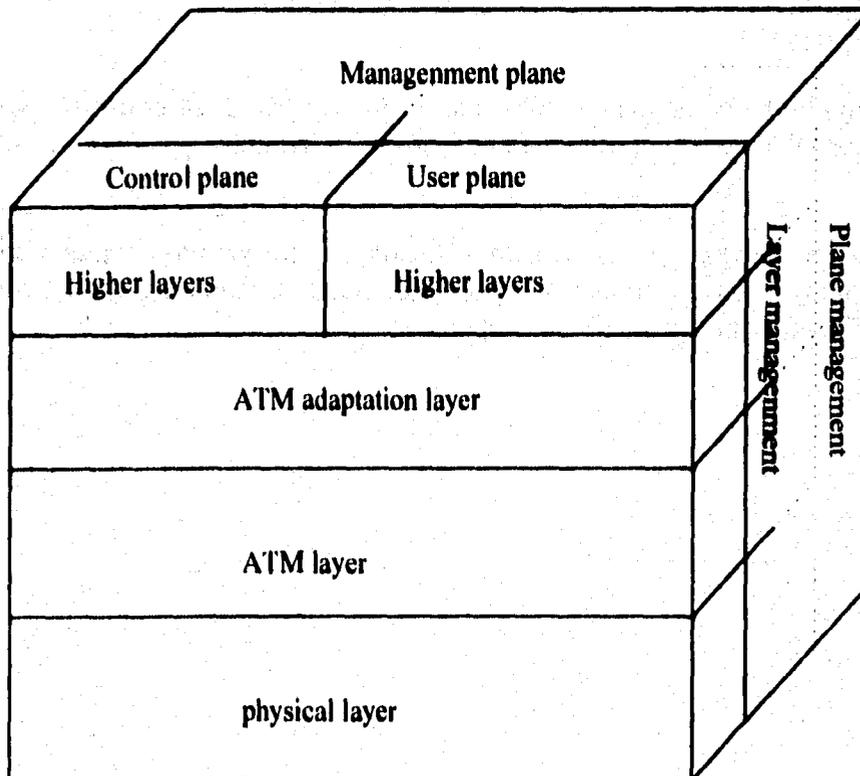


Figura 2.5

El plano de supervisión incluye dos tipos de función: las funciones de supervisión de las capas y las funciones de supervisión del plano. Todas las funciones de supervisión relacionadas con todo el sistema están localizadas en un plano de supervisión, que es el responsable de proveer la coordinación entre todos los planos. No se utiliza ninguna estructura de niveles en este plano.

La supervisión de las capas tiene una estructura de niveles. Esta ejecuta las funciones de supervisión relacionadas a los recursos y a los parámetros que residen en sus entidades de protocolo. Para realizar esta tarea la supervisión de niveles utiliza las especificaciones del flujo de información OAM (Operación, Administración y Mantenimiento) en cada uno de los niveles.

El plano de usuario realiza la transferencia de información. Todos los mecanismos asociados, como control de flujo y recuperación de errores están incluidos en este plano.

Una estructura en niveles es también utilizada dentro del **plano de control**. Este plano es responsable de las funciones de control de las llamadas y control de las conexiones.

Las funciones del nivel físico y del nivel de ATM son las mismas para el plano de control y el plano de usuario. Funciones diferentes pueden ocurrir en el nivel de adaptación ATM así como en los niveles superiores.

2.2.1. Funciones de las capa

La figura 2.6 presenta los niveles inferiores de ATM y sus principales funciones. Las funciones del nivel físico, del nivel de ATM y del nivel de adaptación de ATM son descritas a continuación:

L a y e r	Higher layer functions	Higher layer	
		convergence	C
	segmentation and reassembly	S	A
		A	L
	Generic flow control		
	Cell header generation/ extration	A	
	Cell VPI/CI translation	T	
	Cell multiplex and demultiplex	M	
	Cell rate decoupling		
	HEC sequence generation/ verification		
	Cell delineation	T	P
	Transmission frame adaptation	C	h
	Transmission frama generation/ recovery	y	
		s	
	Bit timing	i	
		c	
		a	
		l	
	Physical medium	P	l
		a	
		y	
		e	
		r	

AAI. ATM ADAPTATION LAYER
 ATM ASYNCHRONUOS TRANSFER MODE
 CS CONVERGENCE SUBLAYER
 HEC PHYSICAL MEDIUM

SAR SEGMENTATION AND REASSEMBLY
 TC TRANSMISSION CONVERGENCE
 CVI VIRTUAL CHANNEL IDENTIFIER
 VPI VIRTUAL PATH IDENTIFIER

Figura 2.6

2.2.2 Capa Física

La capa física está dividida en dos subniveles: el subnivel de medio físico (PM) y el subnivel de convergencia de transmisión (TC), como se describe en la figura 2.6.

2.2.2.1 El subnivel del medio físico (PM).

El nivel del medio físico (PM) es el nivel más bajo e incluye sólo las funciones dependientes del medio físico. Este provee las capacidades de transmisión de bits a través del medio físico correspondiente, además realiza operaciones como la alineación de bits (cuando es necesario), conversión eléctrica/óptica y transferencia de la cadena de bits recuperados a la capa de convergencia de transmisión (TC).

Aunque en muchos casos el medio físico será fibra óptica, otros medios como cable coaxial y par trenzado también pueden ser utilizados. Las funciones de transmisión son específicas del medio.

2.2.2.2 Funciones del subnivel del medio físico (PM).

Ajuste de tiempo para los bits y Código de Interface

En operación normal, el ajuste del tiempo de transmisión está determinado principalmente por la regulación recibida a través de la interface, aunque éste puede ser provisto alternativamente por el reloj local del equipo del usuario, en condiciones de falla la opción de interface basada en celdas proveerá localmente la regulación del tiempo, para este caso la interface funciona en modo de reloj de dirección libre.

La Inversión de marca Codificada (CMI) como se describe en la recomendación ITU-T G.703 ha sido escogida como la interface eléctrica para 155.520 Mbit/s. El CMI tiene varias ventajas:

- Una implementación simple (e. g. , Extracción fácil de reloj).
- Corriente directa a cero (DC) y un contenido de baja frecuencia.
- Transiciones de señal garantizadas: El número de transiciones en la secuencia de datos codificados, es independiente de la secuencia de datos aplicados.
- No se multiplican los errores de bits.
- La habilidad para rastrear errores de bit a través de violaciones de código.

Sin embargo, el CMI tiene la desventaja de doblar la tasa de transmisión de la señal codificada (Baud Rate = 2 x bit rate). Esto no es crítico en el caso de la interface a 155.520 Mbit/s pero es claramente desventajosa para la interface a 622.080 Mbit/s.

Debido a esta circunstancia el código de línea más usado será no-regreso-a-cero (NRZ) para las interfaces ópticas en 155.520 Mbit/s y 622.080 Mbit/s. La convención usada para la lógica los niveles ópticos es:

- Emisión de luz para uno binario
- No emisión de luz para cero binario.

2.2.2.3 Medios físicos

En este subnivel se proveen los relojes para la transmisión de bits sobre los medios físicos. Hay tres cuerpos de estándares que han definido el nivel físico para el soporte de ATM:

- ANSI
- CCITT/ITU-T
- Foro ATM

Resumimos cada una de las interfaces estandarizadas, en términos de la velocidad del reloj de la interface y el medio físico, además de describir cómo se integran las interfaces basadas en celdas.

2.2.2.3.1 Estándares ANSI

El estándar de ANSI T1.624 actualmente define tres modos ópticos simples para interfaces de ATM basadas en SONET:

- STS-1 a la velocidad de 51.84 mbps.
- STS-3c a la velocidad de 155.52 mbps.
- STS-12c a la velocidad de 622.08 mbps.

La T1.624 también define la operación del rango de S3 a 44.736 Mbps, utilizando un protocolo de convergencia de nivel físico extraído del estándar 802.6

2.2.2.3.2 CCITT/ITU-T

La recomendación I.432 define dos interfaces ópticas síncronas con jerarquía digital para ATM las cuales corresponden a los rangos de ANSI antes mencionados. Estos son:

- STM-1 a 155.520 Mbps.
- STM-4 a 622.08 Mbps.

Ya que los rangos de transporte de SDH corresponden a los de SONET la interconectividad debe ser simplificada. La ITU-T estandariza rangos eléctricos y físicos para los siguientes tipos y velocidades:

- DS1 a 1.544 Mbps.
- E1 a 2.048 Mbps.
- DS2 a 6.312 Mbps.
- E3 a 34.368 Mbps.
- DS3 a 44.736 Mbps usando PLCP.
- E4 a 139.264 Mbps.

2.2.2.3.3 Foro ATM

El Foro ATM ha definido cuatro rangos para interfaces de nivel físico. Dos de esos rangos de interface están destinados a redes públicas y son los estandarizados por ANSI e ITU-T. Las interfaces SONET STS-3c son soportadas en OCs-3, ya sea en fibra multimodo o unimodo.

Las siguientes tres interfaces y medios son para aplicaciones de redes privadas:

- FDDI- basado a 100 Mbps.
- Canal de fibra basado a 155.52 Mbps.
- Par trenzado blindado a 155.52 Mbps.

2.2.2.4 Interfaces basadas en celdas

Estas interfaces (a 155.520 Mbit/s y 622.080 Mbit/s) consisten de una secuencia continua de celdas, cada una contiene 53 octetos (conjuntos de ocho bits).

La secuencia máxima entre celdas sucesivas de nivel físico es de 26 celdas de ATM. Después de 26 celdas continuas de ATM, se inserta una celda de la capa física a fin de adaptar la capacidad de transferencia a la velocidad de la interface. (La razón es de 26:27, es decir de 149.760 Mbit/s para 155.520 Mbit/s y 599.040 Mbit/s para 622, 080 Mbit/s). Cuando no hay celdas de ATM, se insertan celdas de la capa física.

2.2.2.5 Funciones del subnivel de convergencia de transmisión (TC)

La subcapa de convergencia de transmisión (TC) hace la conversión entre la cadena de bits y celdas de ATM adaptándolas en un factor de tiempo del medio físico. En la transmisión, el TC básicamente mapea las celdas ATM en formatos de frame para multiplexaje por división de tiempo (TDM). En la recepción, debe delinear las celdas individuales con la cadena de bits recibidos ya sea de un frame TDM directamente, o vía el verificador de errores del encabezado (HEC) en celdas ATM. Generar el HEC en la transmisión y usarlo para corregir y detectar errores en la recepción son también funciones importantes para este subnivel. Otra función importante que el TC realiza es la "adaptación de la velocidad de celdas" esto lo realiza a través del envío al medio físico de celdas ociosas cuando el nivel de ATM no provee celda alguna. Esta función crítica permite que el nivel de ATM opere con un rango muy amplio de diferentes velocidades para las distintas interfaces físicas.

- Ejemplo de mapeo del TC

En esta sección presentaremos un ejemplo de mapeo directo para Sonet STS-3c.

El mapeo para Sonet se realiza en forma directa en una envoltura síncrona de información de carga (SPE) del Sonet STS-3c (155.52 Mbps). La celda de ATM se acomoda en la información de carga del frame STS-3c en forma continua y como no cabe un número exacto de celdas (porque utilizan 53 octetos) se utiliza el HEC para delinear las celdas del frame de Sonet.

Las celdas de la capa física que son insertadas en el lado de transmisión pueden ser celdas ociosas o celdas OAM de capa física, dependiendo de los requerimientos de operación y mantenimiento.

La información OAM de la capa física es llevada en celdas específicas de la capa física, las cuales son identificadas por patrones únicos de bits reservados exclusivamente para estos tipos de celdas. Esto significa que la capa ATM no usará estas combinaciones de bits para los campos del encabezado de las celdas correspondientes.

2.2.2.6 Acoplamiento de la velocidad de celdas

Sin importar si existen o no celdas ATM disponibles para su transmisión, una celda ociosa será insertada para adaptar la cadena de celdas a la velocidad de transmisión del medio físico. Cualquier celda ociosa será desechada en el lado receptor. La inserción y el descarte de celdas ociosas es llamado acoplamiento de velocidad de celdas.

Las celdas ociosas están identificadas por un patrón estandarizado del encabezado. Este es usado a través de la red ATM para identificar celdas ociosas. Cada octeto del campo de información de una celda ociosa se llena con 01101010.

2.2.2.7 Control de error del encabezado (HEC)

De acuerdo al modelo de referencia de protocolo B-ISDN el control de error en el encabezado de la celda es una función de capa física y se describe en la recomendación ITU-T I.432.

Debe remarcarse que el método HEC (Header Error Control), estandarizado para la interface usuario-red (UNI), puede ser empleado universalmente en una Red ATM. El algoritmo de generación del HEC se describe a continuación:

Cada emisor de celdas ATM calcula el valor del HEC con los primeros 4 octetos del encabezado de la celda e inserta el resultado en el quinto (campo del HEC). El valor del HEC está definido como el resultado de la división (módulo 2) por el generador polinomial $x^8 + x^2 + x + 1$ del producto x^8 multiplicado por el contenido del encabezado excluyendo el campo del HEC (los equipos emisores calculan este residuo poniendo en su registro todos los bits a cero antes de efectuar la división), para los patrones fijos '01010101' se debe añadir módulo 2.

Este código de HEC es capaz de:

- * corregir los errores de un solo bit
- * detectar errores múltiples de bit

Se utilizarán las capacidades de procesamiento de error por el equipo receptor de las celdas según la figura 2.7

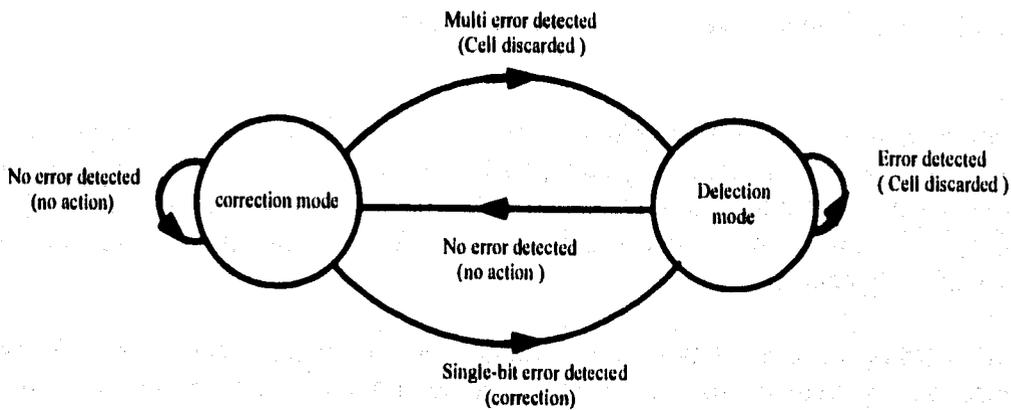


Figura 2.7

2.2.2.8 La Delineación de las Celdas

De acuerdo a la recomendación de la ITU-T 1.432 la delineación de celda es el proceso con el cual se permite la identificación de los límites de la celda. El método recomendado por la ITU-T para la delineación de la celda se basa en la correlación entre los bits del encabezado que son protegidos (los primeros 4 octetos del encabezado de la celda) y los bits de control relevantes (primer octeto del campo HEC). En la figura 2.8 se exhibe el diagrama de estados para la delineación de celdas basado en el análisis del HEC.

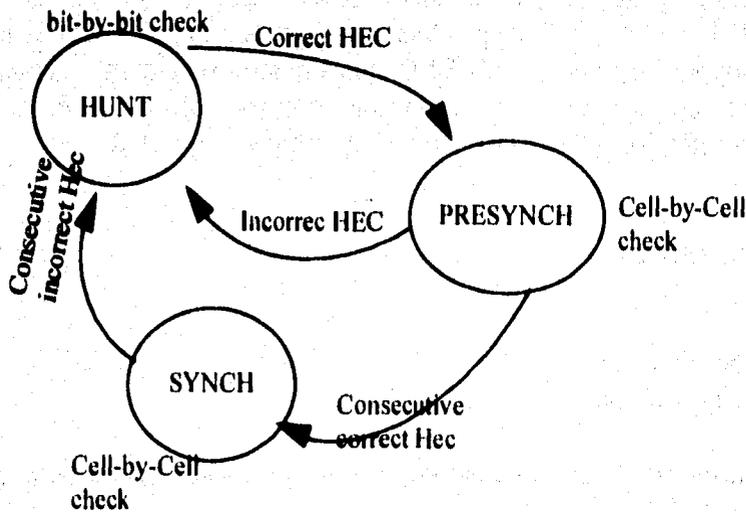


Figura 2.8

Como se muestra en la figura 2.8, los estados que se recorren en la delineación de las celdas son:

Estado de CAZA (HUNT), en éste se realiza una validación bit-por-bit del supuesto encabezado. Cuando hay más información disponible (por ejemplo, en los límites del octeto), este estado es opcional. Cuando la codificación del HEC es respetada, esto es, el residuo igual a cero, se asume que un encabezado ha sido hallado y se va al estado de PRESINCRONIZACION (PRESYNCH). Ahora la validación de la correlación del HEC es ejecutada celda por celda.

Si se encuentra un delta de HECs correctos consecutivo, el estado de SINCRONIZACIÓN (SYNCH) entra nuevamente al estado de CAZA. El sistema pasa del estado de SINCRONIZACION al estado de CAZA si se identifica un número gama de HECs incorrectos consecutivos.

Los valores para delta y gama obviamente influyen en el desempeño del proceso de delineación de la celda. La confiabilidad contra las malas alineaciones producidas por errores de bits, dependen de gama. Los siguientes valores son sugeridos :

delta = 7 , gama=6 para interfaces SDH

delta = 7 , gama=8 para interfaces basadas en celdas

2.2.3 Capa ATM

La Recomendación ITU-T 1.150 incluye las características funcionales de la capa ATM; sus especificaciones están dadas en la recomendación I.361.

2.2.3.1 La estructura de la celda

La celda es el elemento básico de la capa de ATM. El término "celda" es usado también en la capa física. Una celda consiste de un encabezado de 5 octetos y un campo de información de 48 octetos.

Las siguientes convenciones de numeración están definidas en la recomendación ITU-T I.361:

- Los octetos son enviados en orden creciente comenzando con el Octeto 1. Por lo tanto, el encabezado de la celda será enviado primero, seguido por el campo de información.
- Los bits dentro de un octeto están enviados en orden decreciente comenzando del bit 8.
- Para todos los campos, el primer bit enviado es el bit más significativo (MSB).

2.2.3.2 El encabezado de la celda

El encabezado de la celda en la especificación UNI B-ISDN difiere con el que se tiene en el encabezado para NNI B-ISDN en el uso de los bits 5- 8 del octeto 1.

El B-ISDN NNI es la interface entre nodos de red. En el B-ISDN NNI estos bits forman parte del VPI, mientras que en el B-ISDN UNI ellos constituyen una unidad independiente, el GFC.

Los diferentes campos definidos dentro del encabezado de la celda no tienen ningún significado para las celdas de la capa física. Su significado está restringido a las celdas de ATM.

2.2.3.3 Valores pre-asignados del encabezado

A fin de diferenciar las celdas para el uso de la capa ATM de las celdas usadas solamente en la capa física, así como para identificar celdas asignadas y no asignadas, se usan los valores pre-asignados del encabezado.

La diferencia entre las celdas de la capa física y las celdas no asignadas está basada en el uso del bit menos significativo (LSB) del octeto 4 del encabezado de la celda. Este bit no es usado para la indicación de prioridad de pérdida de la celda como en el caso de celdas asignadas.

Varios tipos de celdas físicas ya han sido definidos por los valores del encabezado preasignados. Otros valores del encabezado de la celda están preasignados para señalización OAM y futuras funciones.

2.2.3.4 Control de flujo genérico

El campo de control de flujo genérico (GFC) consiste de 4 bits. Su valor por omisión es 0000 siempre y cuando la función del GFC no sea usada. La información del GFC es llevada ya sea en celdas asignadas o no asignadas. La descripción funcional del GFC está incluida en la recomendación ITU-T 1.150. El mecanismo del GFC ayuda a controlar el flujo del tráfico de ATM en conexiones de B-ISDN UNI. Este es usado para aliviar a corto plazo las condiciones de sobrecarga las cuales ocurren frecuentemente en las redes de los clientes.

El mecanismo del GFC soporta las configuraciones punto-a-punto así como las configuraciones punto-multipunto. El GFC es usado globalmente como un control de acceso al medio.

2.2.3.5 Identificador de la ruta virtual (VPI)

El campo del identificador de la ruta virtual (VPI) en B-ISDN UNI consiste de 8 bits y es usado para encaminar la celda. El VPI en NNI comprende los primeros 12 bits del encabezado de la celda. Esto provee más capacidad de dirección. Los valores preasignados de VPI son usados para algunos propósitos generales. Todos los bits del campo VPI están en cero para las celdas no asignadas.

2.2.3.6 Identificador del canal virtual (VCI)

Junto con el campo de VPI, el campo identificador de canal virtual constituye el campo de enrutamiento de una celda. Un campo de 16 bits es usado para el VCI en B-ISDN UNI, así como en NNI. También hay valores preasignados. Con esta asignación en mente es evidente que el VCI cero no está disponible para la identificación del Canal Virtual (VC).

2.2.3.7 Tipos de carga de pago

Tres bits en el encabezado son usados para el identificador del tipo de carga de pago (PT).

La carga de pago de las celdas de información del usuario contienen información de usuario, así como funciones de adaptación de servicio. En las celdas de información de red, la carga de pago es usada para llevar información que le sirve a la red para su operación y mantenimiento.

El bit de indicación de congestión (CI) dentro del PTI, en las celdas de usuario puede ser modificado por cualquier elemento de la red, que esté congestionado, para informar al usuario final acerca de su estado.

2.2.3.8 Prioridad de pérdida de celda

El campo de la prioridad de pérdida de celda (CLP) consiste de un bit, el cual es usado explícitamente para indicar la prioridad de pérdida de celda. Si el valor del bit CLP es 1, la celda está sujeta a ser desechada, dependiendo de las condiciones de la red. Sin embargo, los parámetros de la calidad de servicio convenida (QOS) no serán violados. En el otro caso (CLP= 0), la celda tiene prioridad alta y por lo tanto, recursos suficientes de la red deben de ser asignados.

2.2.3.9 El Control de error del encabezado

Este campo forma parte del encabezado de la celda pero no es usado por la capa ATM. Este contiene la secuencia del control de error del encabezado (HEC), la cual es procesada por la capa física.

2.2.4 Capa de adaptación de ATM (AAL)

La capa de adaptación de ATM (AAL) está dividida en dos subniveles :

Segmentación y reensamble (SAR)
Subnivel de convergencia (CS)

Las funciones del AAL están descritas en la recomendación ITU-T I.362

El AAL es un nivel entre la capa de ATM y los niveles superiores. Esta función es la ampliación de los servicios que provee la capa de ATM para los requerimientos de las capas superiores. Los PDUs que provienen de las capas superiores son mapeados en los campos de información de una celda ATM. Las entidades de AAL intercambian información con sus entidades AAL iguales para soportar las funciones AAL.

Las funciones AAL están organizadas en dos subcapas. Las funciones esenciales de la subcapa de SAR son, en el lado transmisor, segmentar las PDUs de los niveles superiores en un tamaño adaptable para el campo de información de la celda ATM (48 octetos) y, en el lado receptor, reensamblar los campos de información particular en PDUs de capas superiores. El servicio de CS depende y provee el servicio de AAL para AAL-SAP

Ningún SAP ha sido definido entre estas dos subcapas. SAPs de diferentes capas superiores pueden ser entregados usando diferentes combinaciones de SAR y CS. Para algunas aplicaciones no se necesita CS ni SAR, para estos casos estarán vacíos.

Para minimizar el número de protocolos AAL, la ITU-T propuso un servicio de clasificación el cual es específico para cada AAL. Esta clasificación está hecha con respecto a los siguientes parámetros :

- Relación de ajuste de tiempo
- Bit rate (velocidad de bits)
- Modo de conexión.

Varios tipos de protocolos AAL han sido definidos. Cada uno consiste de una capa de SAR y CS específica, la figura 2.9 muestra las diferentes clases definidas.

	class A	class B	class C	class D
Timing relation between source and destination	Required		Not required	
Bit rate	Constant		Variable	
connection mode	Connection oriented			connectionless

Figura 2.9

2.2.4.1 AAL tipo 0

Aunque el AAL tipo cero no es un término oficialmente usado puede ser considerado como importante, ya que es un AAL con un SAR y CS vacíos. Esto significa que la funcionalidad de AAL no es requerida y el contenido del campo de información de la celda es directa y transparentemente transferido a las capas superiores. Sin embargo una descripción de este servicio no está disponible en los estándares de la ITU-T.

2.2.4.2 AAL tipo 1

Normalmente los servicios CBR (Clase A) utilizan AAL tipo 1 porque reciben y entregan SDUs con un bit rate constante. La sincronización de la información también es transferida entre fuente y destino. Si se necesita la información acerca de la estructura de los datos también es transportada. Una indicación de pérdida o de información con error es enviada a las capas superiores si estas fallas no pueden ser recuperadas dentro del AAL.

Las funciones que realiza AAL son las siguientes:

- Segmentación y reensamble de la información de usuario
- Manejo de la variación del retraso de la celda
- Manejo del retraso del ensamble de la información de carga de la celda
- Recuperación de la frecuencia del reloj fuente en el receptor
- Monitoreo de los errores de bit así como manejar estos errores.

En caso de una emulación de circuito, un monitoreo de la calidad de servicio QOS es necesario.

2.2.4.2.1 Subcapa de segmentación y reensamblaje.

LAS PDU-SAR se forman con 48 octetos. El primer octeto incluye el campo PCI, el resto de los octetos están disponibles para la información pago de carga en las SAR-PDU. El PCI está subdividido en un número de secuencia de 4 bits (SN) y un número de protección de secuencia (SNP). El SN consiste de un bit indicador de convergencia (CSI) y un campo de secuencia de 3 bits. El SNP contiene un CRC de 3 bits el cual protege el campo de SN.

El campo de secuencia permite detectar falta de celdas o celdas mal insertadas. Para sistemas con un alto promedio de falla este método no es muy robusto ya que 3 bits para el campo de secuencia es poco.

El bit CSI es usado para enviar la información de sincronización y/o de estructura de datos.

El SNP provee capacidades de detección y corrección de errores en el SN con ayuda del campo de CRL de 3 bits y con el bit de paridad.

* El SN está protegido con base al polinomio $G(X) = X^3 + X + 1$

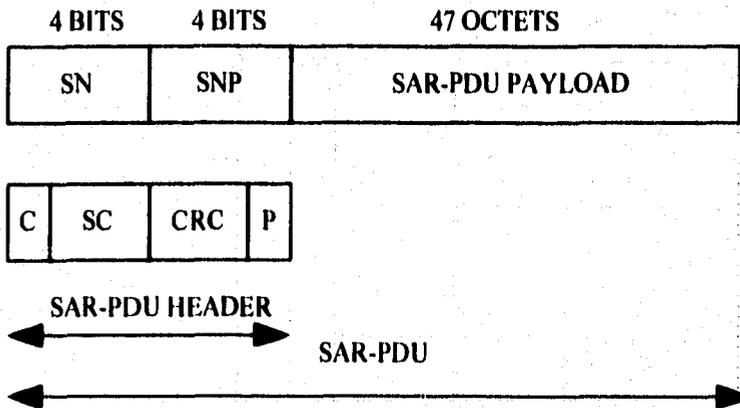
* El resultado del séptimo bit está protegido por una validación de paridad non.

2.2.4.2.2 Subcapa de convergencia

Las funciones del CS dependen fuertemente del servicio que se esté soportando. Algunas de estas funciones se muestran a continuación :

- Manejo de la variación de los retrasos. Un buffer es usado para soportar esta función.
- Recuperación de la frecuencia del reloj fuente, utilizando un método de estampa de tiempo residual (SRTS). Una estampa de tiempo residual (RTS) es usada para medir y calcular las diferencias entre relojes de referencia comunes.
- Transferir la estructura de la información entre la fuente y el destino
- Corrección de error adelantado (FEC) ésta puede ser utilizada para asegurar una alta calidad para algunas aplicaciones de voz y video.

FORMATOS PARA SAR-ADU AAL TIPO I



C Convergence sublayer indication	SAR segmentation and ressembly
CRC cyclic redundancy check	SC sequence count
P Even parity bit	SN Sequence number
PDU Protocol data unit	SNP Sequence number protection

Figura 2.10

2.2.4.3 AAL Tipo 2

AAL tipo 2 está diseñado para servicios VBR con una relación variable de tiempos entre fuente y destino. Este tipo no está bien definido aún y sólo podemos anticipar las siguientes funciones y servicios :

Servicios :

- Información de ajuste de tiempos entre fuente y destino
- Si se necesita, las capas superiores pueden ser informadas acerca de los errores

Como se muestra en la figura 2.11, las funciones son:

- Segmentación y reensamble de la información del usuario.
- Manejo de la variación del retardo de las celdas
- Manejo de pérdida o daño de las celdas
- Recuperación del reloj fuente en el receptor
- Monitoreo del campo de información del usuario para errores y posible acciones correctivas.

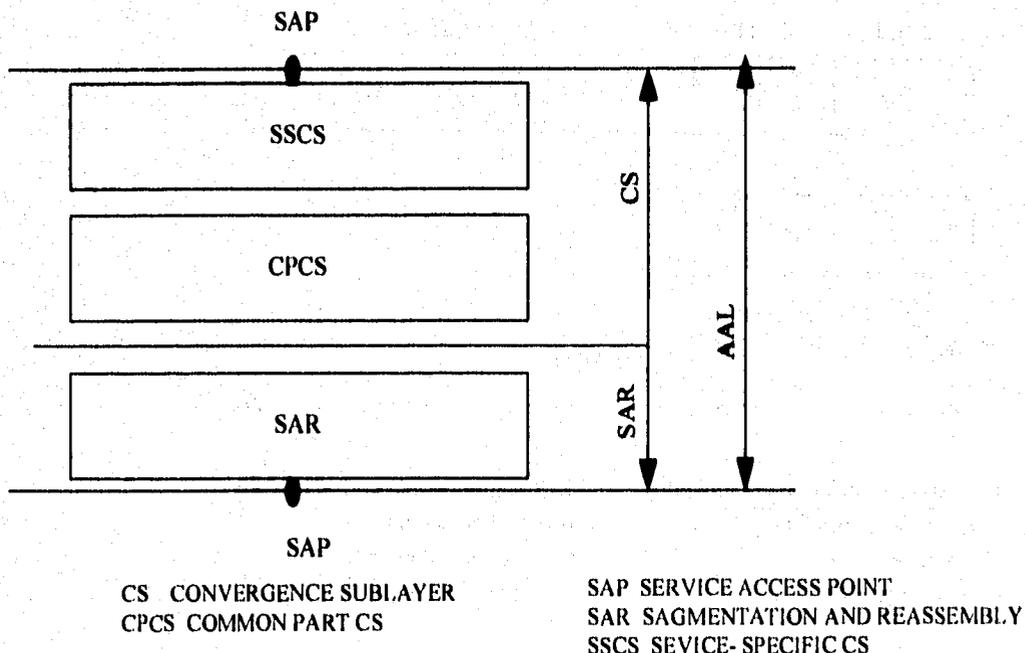


Figura 2.11

2.2.4.4 AAL Tipo 3 / 4

El nombre de este tipo de AAL refleja su desarrollo, así como se definieron diferentes clases de servicio diferentes, AALs fueron alojados para las clases de servicio C y D, llamados AAL tipo 3 y AAL tipo 4, pero fueron integrados para tener un soporte común en ambas clases.

Dos modos de servicio están definidos para el AAL tipo 3/4:

- Servicio en modo mensaje. Este puede ser usado para transferencias de frames de datos (por ejemplo, frames de control de la capa de enlace).
- Servicio en modo cadena. Este puede ajustarse para transferencias de datos a bajas velocidades con requerimientos de poco retraso.

En el servicio en modo de mensaje transporta una sola AAL-SDU (Unidad de Datos de Servicio) en una sola Cs-PDU (opcionalmente en más), la cual puede estar construida de una o varias SAR-PUDs (Unidades de Datos de Protocolo).

En el servicio en modo de cadena una AAL-SDUs (de tamaño fijo) son transportadas en una CS-PDU.

La AAL-SDU puede resultar tan pequeña como un octeto y siempre es entregada como una unidad.

Dos procedimientos de operación se ofrecen en ambos servicios:

- Operación asegurada. La operación asegurada retransmite AAL-SDUs dañadas o faltantes pero el control de flujo es una característica obligatoria,
- Operación no asegurada. En la operación no asegurada las AAL-SDU dañadas o faltantes no son corregidas con retransmisiones.

2.2.4.4.1 Subcapa de segmentación y reensamble

En general las CS-PDU son de longitud variable. Cuando se acepta como un PDU el subnivel SAR genera una SAR-PDU que contiene hasta 44 octetos de datos de CS-PDU. La CS-PDU es conservada por el subnivel SAR. Esto requiere un indicador de tipo de segmento (ST) y un indicador de relleno de la información de carga del SAR.

El identificador ST permite identificar si la SAR-PDU es:

- Inicio de mensaje (BOM)
- Continuación de mensaje (COM)
- Fin del mensaje (EOM)
- Mensaje de segmento simple (SSM)

El indicador del relleno de la información de pago de carga representó el número de octetos CS-PDU.

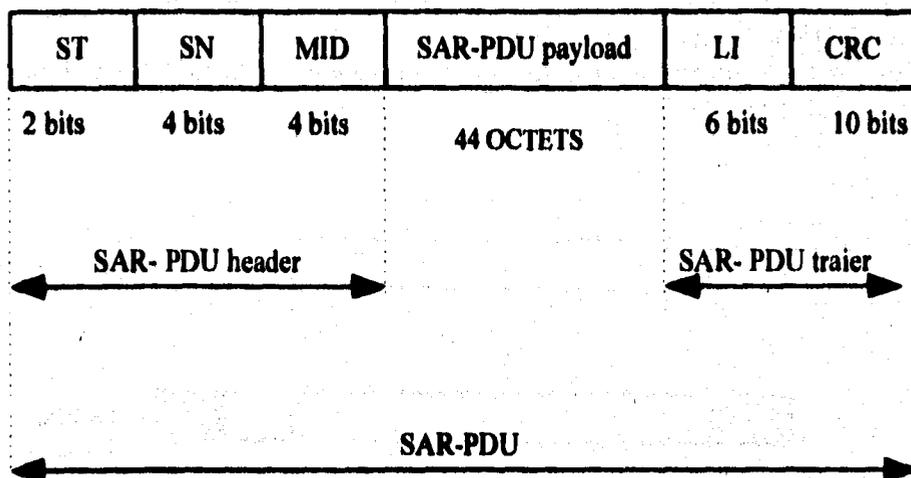
El campo identificador de multiplexaje permite identificar las SAR-PDUs, esta función se utiliza cuando múltiples conexiones trabajan con la misma conexión de ATM.

El campo indicador de longitud consta de 6 bits y contiene el número de octetos (codificado en forma binaria) de CS-PDUs que está contenida en la carga de información de la SAR-PDU.

El campo de CRL contiene el cálculo del CRL para el encabezado, la información de carga y el campo LI. El polinomio generador es:

$$G(X) = X^{10} + X^9 + X^5 + X^4 + X + 1$$

La clasificación de los indicadores es la primera función de este subnivel. La detección de errores es la segunda función del subnivel SAR, esta función incluye la detección de los errores de bit en las PDU-SAR así como la detección de celdas perdidas. La tercera función del subnivel de SAR es el multiplexaje/demultiplexaje para múltiples conexiones AAL sobre la misma conexión en la capa de ATM. (Figura 2.12).



CRC cyclic redundancy check
 LI length indicator
 MID multiplexing identifier
 PDU protocol data unit

SAR segmentation and reassembly
 SN sequence number
 ST segment type

Figura 2.12

2.2.4.4.2 Subcapa de convergencia

Esta subcapa está dividida en dos:

- Parte común (CPCS)
- Parte de servicio específico (SSCS)

El CPCS transfiere frames de datos de usuario con una longitud de 1 a 65535 octetos.

Las funciones CPCS requieren un encabezado de 4 octetos y un trailer de 4 octetos. Además un campo (PAD) se utiliza para alinear los bits. El indicador de la parte común (CPJ) se utiliza para interpretar los campos faltantes en el encabezado y trailer.

Los campos etiqueta de inicio (BTAG) y etiqueta de fin (ETAG) permiten la relación apropiada en el encabezado y trailer de la CPCS-PDU. El mismo valor numérico es configurado en ambos campos.

El campo BASIEE identifica al receptor y los requerimientos máximos de almacenamiento para recibir la CPCS-SDU.

El campo PAD asegura que la carga de información de la CPCS-PDU es un múltiplo entero de 4 octetos.

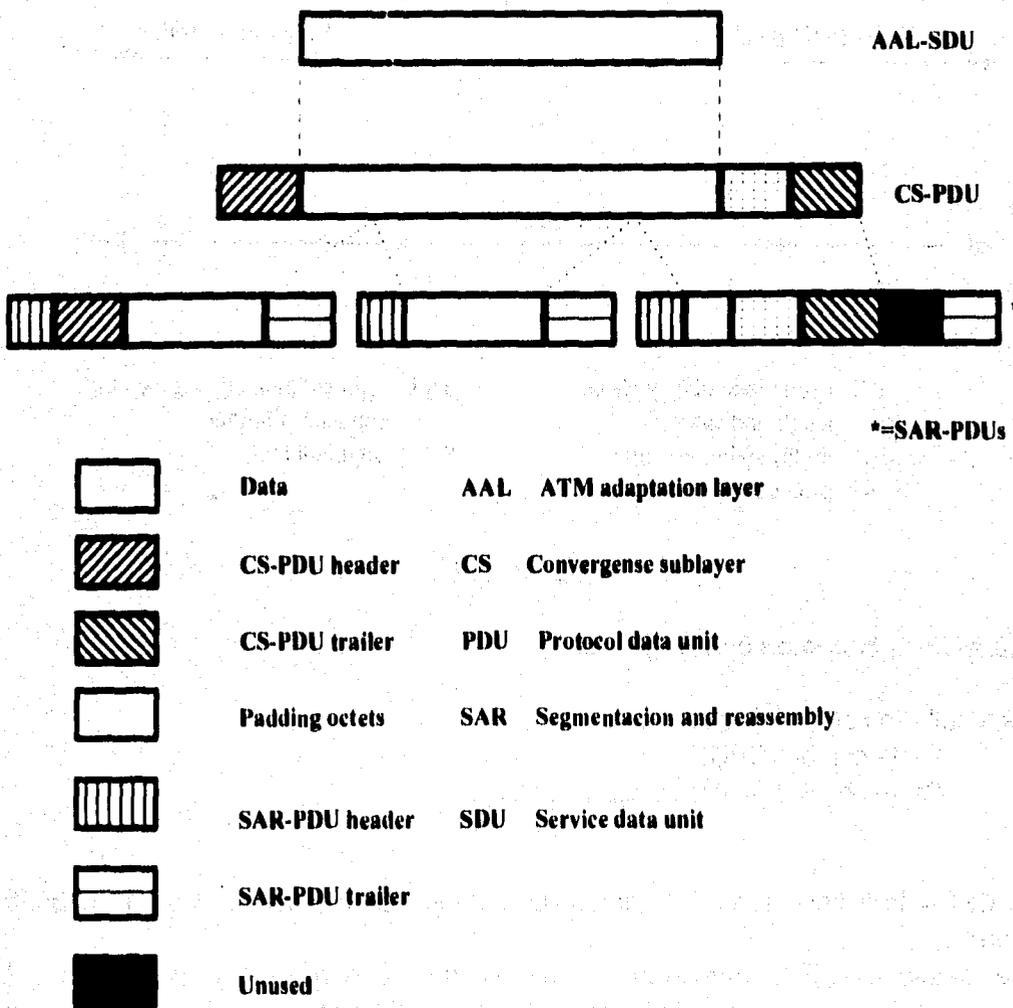


Figura 2.13

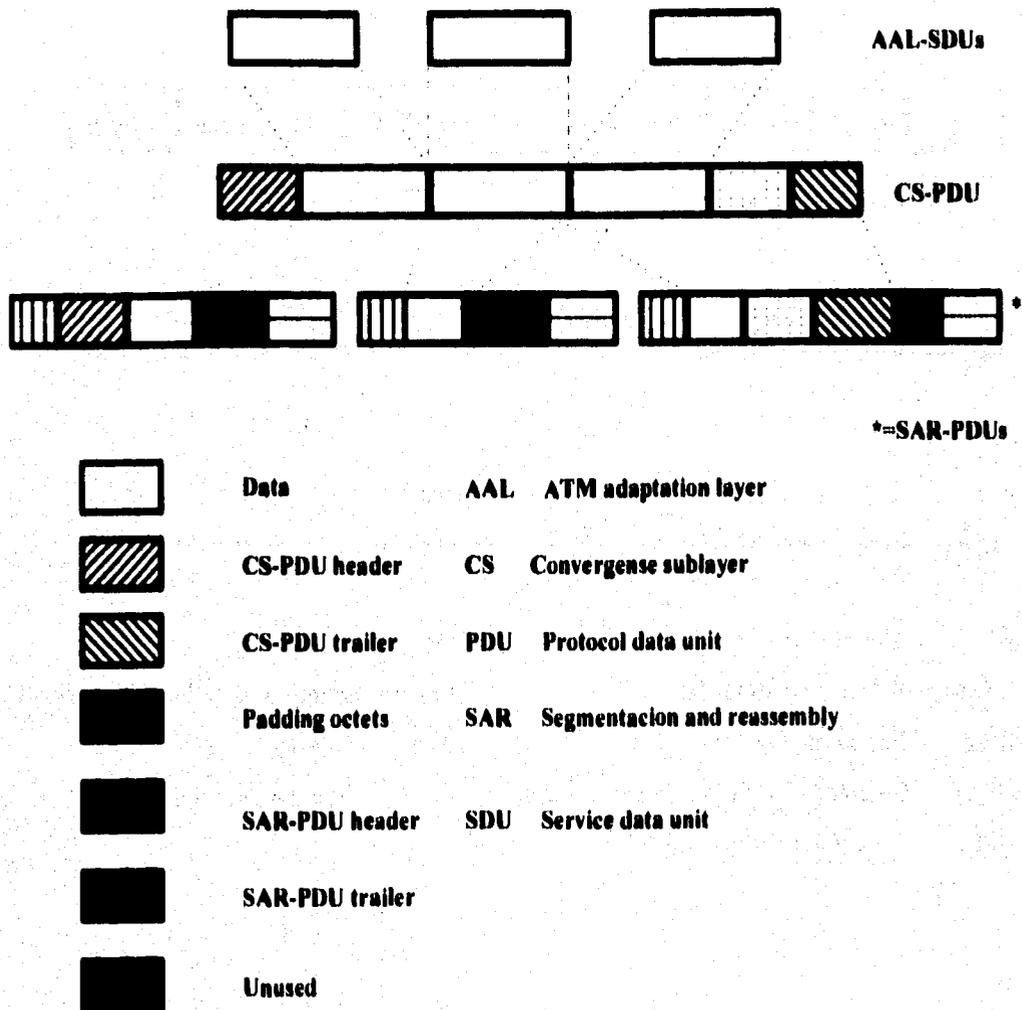
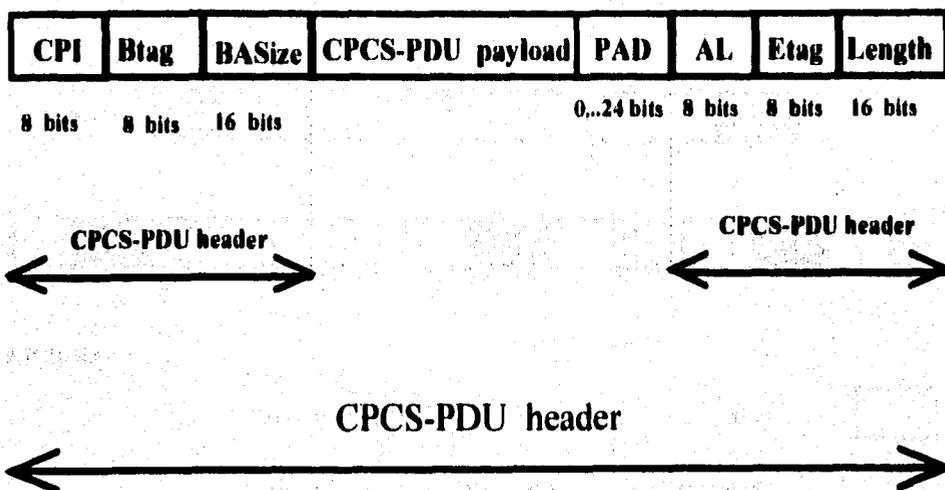


Figura 2.14



- | | |
|--|--|
| <p>AL Alignment</p> <p>BASize Buffer allocation size</p> <p>Btag Beginning tag</p> <p>CPCS Common part convergence sublayer</p> <p>CPI Common part indicator</p> | <p>Etag Ending tag</p> <p>Length Length of CPCS-PDU payload</p> <p>PAD Padding</p> <p>PDU Protocol data unit</p> |
|--|--|

Figura 2.15

2.2.4.5 AAL Tipo 5

El AAL Tipo 5 se usa con dispositivos de velocidad variable de bits sin necesidad de sincronización entre la fuente y el destino. Este provee servicios similares a AAL 3/4 y es usado principalmente para aplicaciones de datos. La razón de definir este AAL adicional es la de reducir sobrecarga ('es un AAL simple y eficiente'). Sus modos de servicio son idénticos que para AAL Tipo 3/4. Sin embargo este AAL no soporta las funciones de multiplejaje por lo tanto no hay campo de MID. El AAL Tipo 5 está diseñado principalmente para señalización y frame relay sobre ATM. Las subcapas de SAR y CS son idénticas que para AAL Tipo 3/4 sólo cambia el encabezado en la subcapa de SAR. Ver figura 2.16

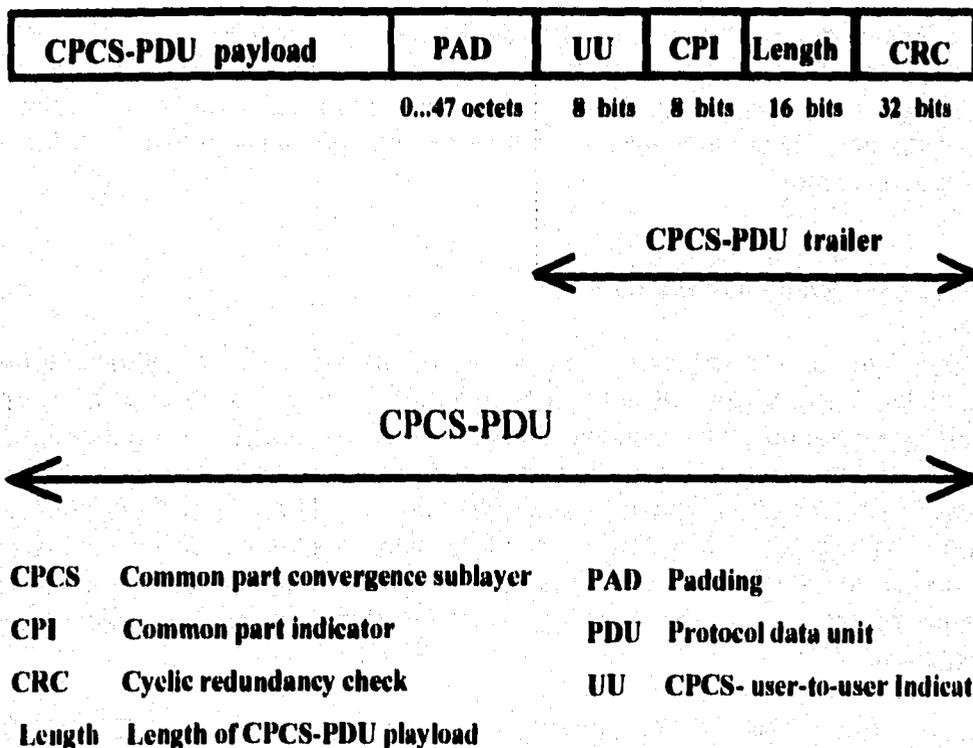


Figura 2.16

2.3 Conmutación ATM

Existen dos funciones principales que pueden encontrarse en el conmutador ATM o nodo de conexión por cruce:

- 1.- Traducción VPI/VCI.
- 2.- Transporte de celda de su entrada a su salida.

La estructura del conmutador necesita establecer una conexión entre un par arbitrario de entradas y salidas. En un principio, la electrónica del conmutador se puede implementar como un sencillo elemento de conmutación. Puesto que un solo elemento no podría satisfacer los requerimientos de un nodo de conmutación ATM de tamaño normal, se utilizan estructuras más grandes de conmutador para crecer el número de elementos de conmutación.

El "throughput" de un nodo de conmutación estará en el rango de Gbit/s, el retardo de nodos de cruce y pérdida de celdas deben mantenerse muy bajas. De tal forma, que un control central no puede ser usado para conmutar celdas. Solamente estructuras electrónicas con arquitecturas paralelas pueden satisfacer estos requerimientos.

2.3.1 Elementos de conmutación

Un "elemento de conmutación" es la unidad básica de una estructura de conmutador. En el puerto de entrada la información de ruteo de una celda de entrada es analizada y direccionada al puerto de salida correcto. En general, un elemento de conmutación consiste de una red de interconexión, un controlador de entrada (IC) para cada línea entrante y un controlador de salida (OC) para cada línea de salida (figura 2.17). Para prevenir la pérdida excesiva de celdas en el caso de colisiones internas (dos o más celdas compitiendo por la misma salida simultáneamente), los buffers tienen que ser suministrados sin el elemento de conmutación.

Las celdas que llegan estarán sincronizadas al reloj interno por el IC. El OC transporta las celdas que han sido recibidas de la red de interconexión hacia su destino. Los ICs y OCs son acoplados por la red de interconexión.

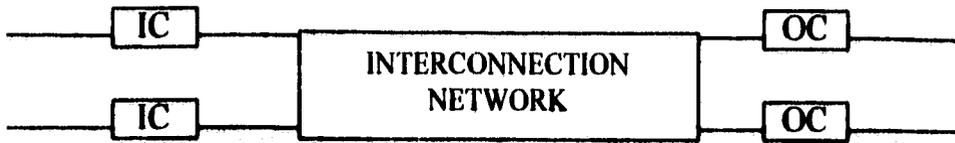


Figura 2.17

2.3.1.1 Elementos de conmutación tipo matriz

Internamente los elementos de conmutación de no bloqueo pueden ser contruidos usando una matriz rectangular de puntos de cruce para la red de interconexión (figura 2.18). Siempre es posible conectar algún par de entrada/salida desocupado. De cualquier forma un punto de cruce conecta una entrada a una salida dependiendo de la información de ruteo de la celda, así como la ocurrencia de colisiones.

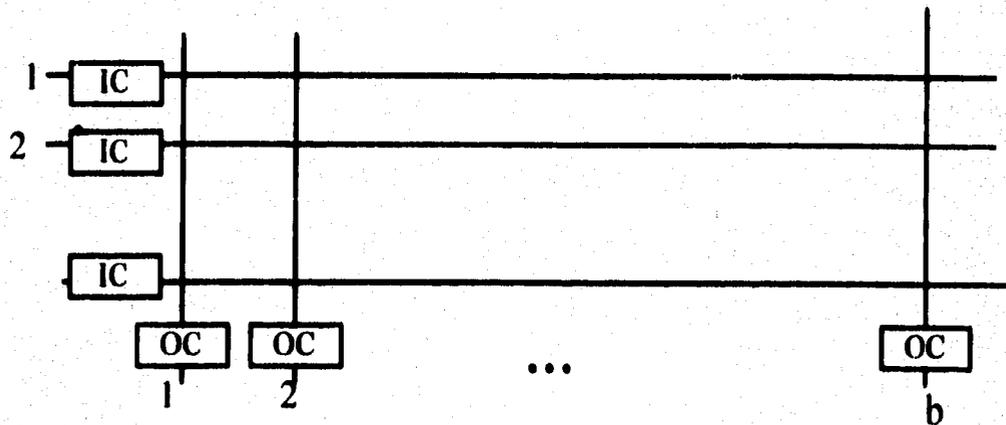


Figura 2.18

Varias localidades buffer son posibles en el elemento de conmutación:

- En los controladores de entrada
- En los controladores de salida
- En los puntos de cruce

2.3.1.1.1 Buffers de entrada

Los buffers de celda están localizados en el controlador de entrada (figura 2.19). Cuando usamos el buffer "primero en entrar primero en salir" (FIFO), ocurre una colisión si dos o más celdas líderes de la cola compiten simultáneamente por la misma salida. Entonces todas, excepto una de las celdas son bloqueadas. Las celdas siguientes a la celda líder de la cola bloqueada son bloqueadas también, aun cuando estén destinadas para otra salida disponible.

Para combatir esta desventaja, los buffers FIFO pueden ser reemplazados por memorias de acceso aleatorio (RAM). Si la primera celda del buffer es bloqueada, la siguiente celda destinada para una salida desocupada, será seleccionada para transmisión. No obstante, este modo de operación requiere control del buffer más complejo para encontrar una celda destinada a una salida desocupada, y garantizar la secuencia correcta de celdas destinadas a la misma salida. La capacidad total del buffer lógicamente estará subdividida de una manera dependiente de la carga dentro de FIFOs sencillos (un FIFO para cada salida).

Estas mejoras pueden lograrse si más de una celda puede ser transferida simultáneamente de un buffer a salidas diferentes. Esto requiere un buffer con múltiples salidas o un buffer con tiempo de acceso reducido.

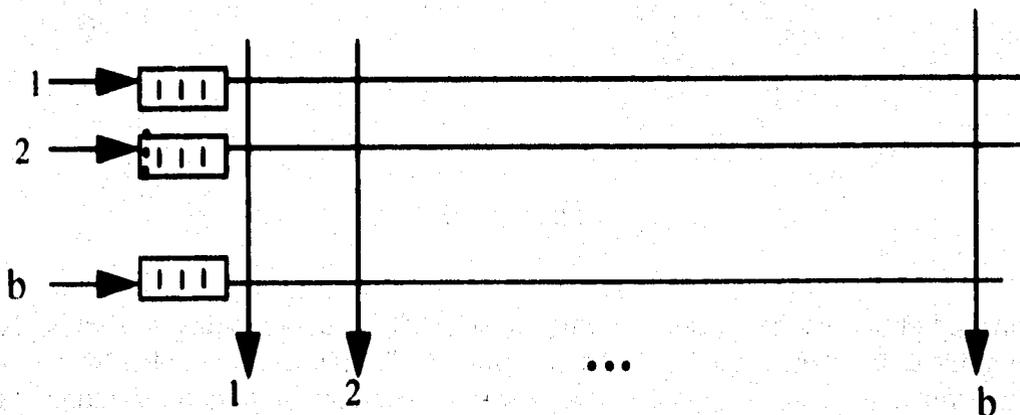


Figura 2.19

5.1.1.2 Buffers de salida

La figura 2.20 muestra un elemento de conmutación constituido de una matriz con buffers de salida. Solamente si la matriz opera a la misma velocidad que las líneas de entrada podrían ocurrir colisiones (varias celdas son destinadas simultáneamente a la misma salida). Esta desventaja puede ser compensada reduciendo el tiempo de acceso del buffer y aumentando la velocidad de la matriz de conmutación. Estos factores pueden conducir a limitaciones tecnológicas en el tamaño del elemento de conmutación.

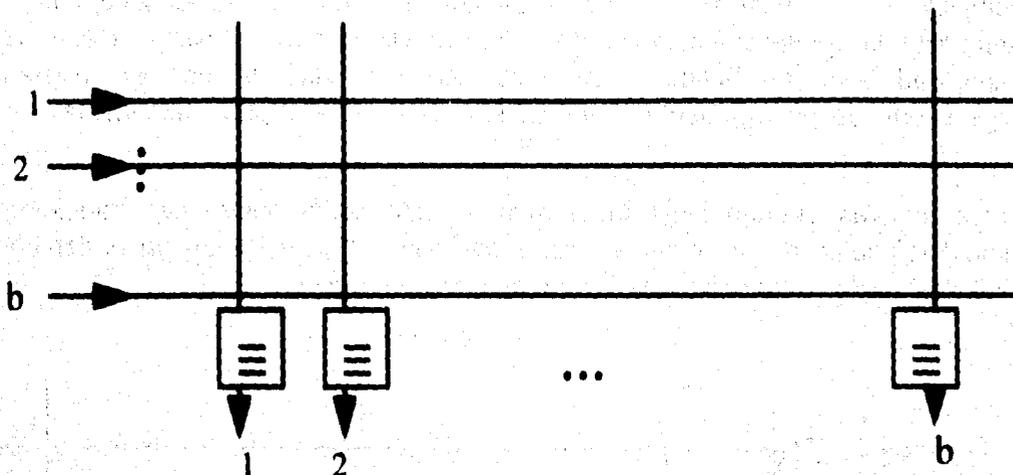


Figura 2.20

Un elemento de conmutación con buffers de salida no será bloqueado solamente si el factor aumento de velocidad de la matriz es "b" (es decir, la celda "b" cruce simultáneamente la misma salida que pueda ser conmutada) para un elemento de conmutación de "bxb". En todos los demás casos, son necesarios buffers adicionales en la entrada para evitar la pérdida de celdas causada por bloqueo interno.

2.3.1.1.3 Buffers de punto de cruce.

Los buffers pueden estar localizados en los puntos individuales de cruce de la matriz (figura 2.21). Y se denominan elementos de conmutación "mariposa". Esto previene que las celdas que están destinadas a diferentes salidas afecten alguna otra. Si hay paquetes en más de un buffer pertenecientes a la misma salida, la lógica de control tiene que elegir cuál buffer será atendido primero.

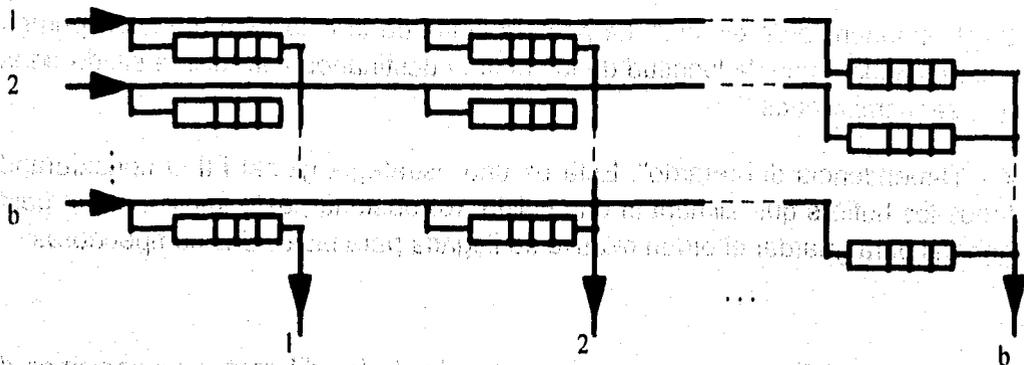


Figura 2.21

2.3.1.1.4 Estrategias de arbitraje

Si varias celdas compiten simultáneamente por la misma salida, solamente una podrá ser transferida y todas las demás estarán retardadas. Es requerida una estrategia de arbitraje para determinar cuál celda es la "ganadora". Los objetivos para este mecanismo pueden ser:

Minimización de pérdida de celdas y minimización en el retardo de celdas.

Se pueden aplicar las siguientes estrategias:

- 1.- "Aleatoria": La línea que será atendida primero se elige aleatoriamente de todas las líneas que compiten por la misma salida. Esta estrategia requiere sólo un mínimo gasto de implementación.
- 2.- "Cíclico": Los buffers son atendidos en orden cíclico. Esta aproximación también requiere solamente un mínimo gasto de implementación.
- 3.- "Dependencia de estado": La primera celda de la cola será atendida primero. Para este algoritmo, la longitud de los buffers destinados a la misma salida tienen que ser comparados.
- 4.- "Dependencia del retardo": Esta es una estrategia global FIFO considerando todos los buffers que alimentan una salida. No obstante, esto implica algún gasto general para guardar el orden relativo de llegada para las celdas competidoras.

En la figura 2.22 se muestra una comparación de los diferentes mecanismos de arbitraje.

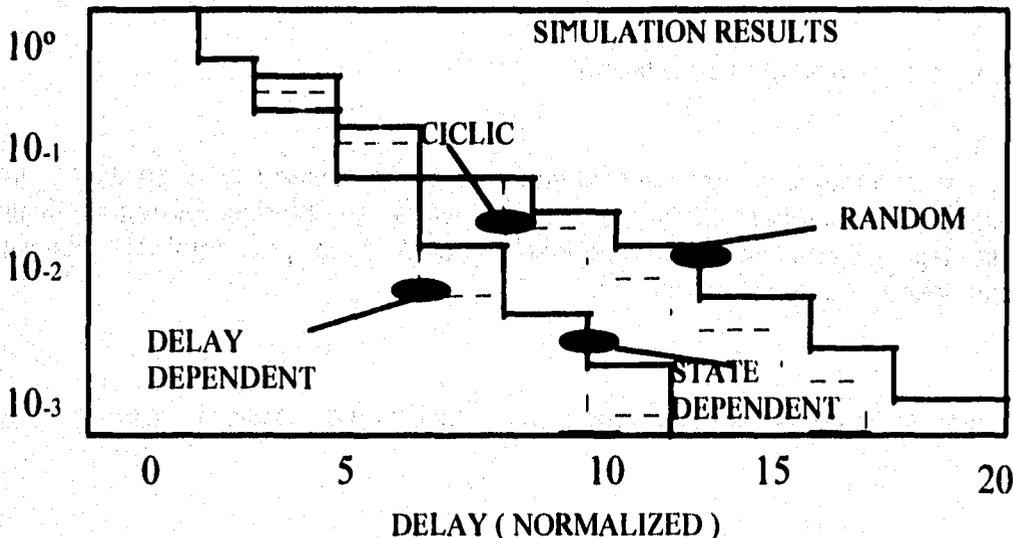


Figura 2.22

La estrategia aleatoria tiene las más altas variaciones de retardo. Un perfeccionamiento mínimo se puede realizar para usar la estrategia cíclica. La estrategia óptima con respecto a la variación del retardo de celdas es la "estrategia de dependencia de retardo". Se puede lograr la minimización de pérdida de celdas implementando el algoritmo de dependencia de estado. El desempeño con respecto a los requerimientos de retardo de esta estrategia es ligeramente malo, pero sin embargo aceptable.

2.3.1.2 Elemento de conmutación de memoria central

El principio de un elemento de conmutación de memoria central se muestra en la figura 2.23. Todos los controles de entradas y salidas son conectados directamente a una memoria común, la cual puede ser grabada por todos los controladores de entrada y leída por todos los controladores de salida.

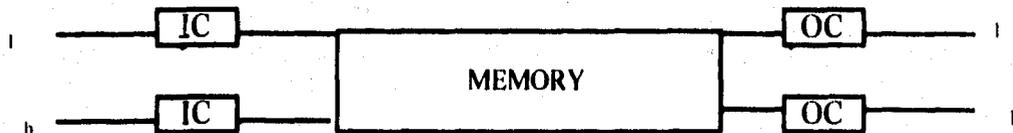


Figura 2.23

El primer ejemplo de tal elemento de conmutación se utilizó en el experimento de PRELUDE. La memoria común podrá estar organizada para proporcionar buffers de entrada lógica así como en buffers de salida lógica. El proyecto 1012 de Investigación y Desarrollo en Comunicaciones Avanzadas de Europa (RACE), denominado "Tecnología de redes locales de banda ancha" está usando el conmutador "Sigma", el cual se basa en una estructura de memoria común con buffers de salida lógicos.

Partiendo de que todos los buffers de elementos de conmutación comparten una memoria común, se puede lograr una reducción importante en el total de los requerimientos de memoria, en comparación con los buffers separados físicamente. Por otro lado, se necesita un alto grado de paralelismo interno para mantener la frecuencia de acceso a memoria en un rango realizable.

2.3.1.3 Elemento de conmutación tipo bus

La red de interconexión puede realizarse por medio de un bus de multiplexaje por división de tiempo de alta velocidad (TDM). (Figura 2.24). Una transmisión libre de conflicto puede garantizarse solamente si la capacidad total del bus es menor que la suma de capacidades de todas las ligas de entrada. La transmisión de datos de bit paralelo (por ejemplo 16 ó 32) es necesario en el sistema de bus para lograr esta alta capacidad.

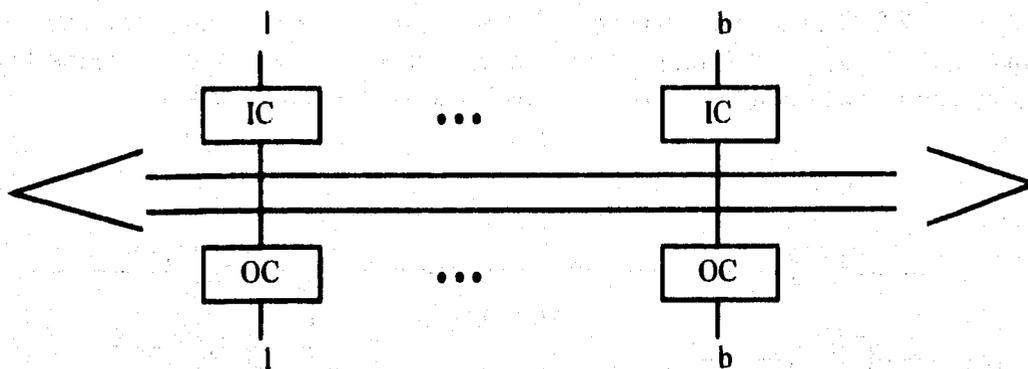


Figura 2.24

Normalmente, un algoritmo de acceso de bus se aplica para asignar el bus para los controladores de entrada individual en intervalos constantes. Cada controlador de entrada es capaz de transmitir su celda hacia el destino antes que se complete la llegada de la siguiente celda. No se necesitan buffers en los controladores de entrada. No obstante, varias celdas pueden llegar al mismo controlador de salida, mientras que solamente una de ellas puede abandonar el controlador. Por lo tanto, se necesitan buffers para el controlador de salida. Este elemento de conmutación funciona igual que el elemento de conmutación tipo matriz con buffers de salida.

2.3.1.4 Elemento de conmutación tipo anillo.

El elemento de conmutación tipo anillo se muestra en la figura 2.25. Todos los controladores de entrada y de salida están interconectados mediante una red tipo anillo la cual debería ser operada en forma de ranuras para minimizar el gasto general. En un principio, se puede utilizar un esquema de alojamiento por ranuras de tiempo, pero esto requiere una capacidad de anillo, la cual es la suma de todas las capacidades de todas las ligas eslabones de entrada. Si la capacidad de anillo es menor que la capacidad total de entrada, se necesitará un esquema de asignación flexible, lo cual resulta un gasto adicional.

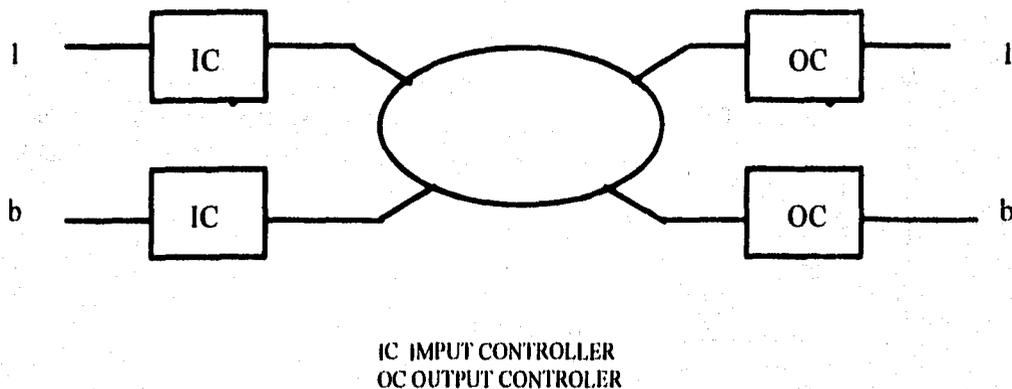


Figura 2.25

La estructura de anillo tiene la ventaja sobre la estructura de bus en que las ranuras de tiempo se pueden usar varias veces con una rotación. No obstante, requiere que el controlador de salida "vacíe" una ranura de tiempo recibida. Cuando se usa este mecanismo de liberación de destino, se puede lograr una utilización efectiva de más del 100%. Esta ventaja está compensada en contraste con el gasto adicional del mecanismo de liberación de destino y el mecanismo flexible de asignación por ranura de tiempo.

El anillo ORWELL es una aproximación de la implementación de un elemento de conmutación tipo anillo.

2.3.1.5 Aspectos del rendimiento

Muchas publicaciones ofrecen comparaciones del funcionamiento de diferentes estrategias de buferización. La figura 2.26 muestra un mal retardo de celda de un elemento de conmutación de 16x16 con diferentes localidades y modos de operación de buffer.

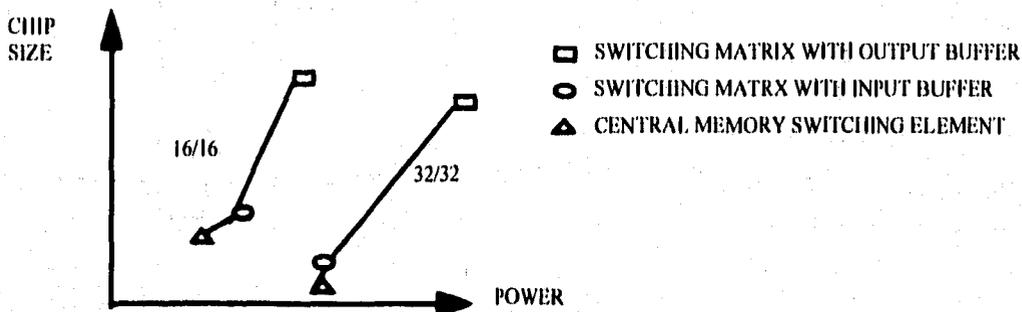


Figura 2.26

Los resultados para el elemento de conmutación con un buffer simple de entrada FIFO corresponde a la curva de velocidad ascendente con factor 1. Un factor "i" de velocidad ascendente significa que el tiempo de acceso al buffer está reducido por el factor i, o las celdas i de un buffer pueden ser transferidas simultáneamente. El máximo throughput de este elemento está limitado a aproximadamente el 58% del total de la capacidad total. El mejoramiento del funcionamiento será logrado usando un factor de velocidad ascendente de 2. Los mejores resultados son obtenidos por elementos de conmutación con un factor de velocidad ascendente de 16.

En este caso el comportamiento es idéntico a un elemento de conmutación con buffers de salida. No obstante, el throughput ideal puede casi obtenerse, aún con un factor de 4 de velocidad ascendente. Esto puede simplificar significativamente la implementación.

2.3.1.6 Aspectos tecnológicos

Los resultados del rendimiento se muestran en la figura 2.27 y son válidos para tamaños infinitos de buffer. No obstante, solamente son posibles tamaños finitos de buffer. La tabla 5.1 presenta tamaños de buffer (en celdas) para elementos de conmutación de diferentes tamaños y localidades de buffer, asumiendo una carga promedio del 85 % en cada entrada y una probabilidad de pérdida de celdas de 10^{-9} .

TYPE	SIZE	
	16 X 16	32 X 32
CENTRAL MEMORY	113	199
INPUT BUFFER	320	640
OUTPUT BUFFER	896	1824

Figura 2.27

El elemento de conmutación de memoria central requiere la capacidad de memoria mínima como resultado de la compartición de buffer. La capacidad de memoria requerida para un elemento de conmutación con buffers de entrada es baja comparada con el elemento de conmutación con buffers de salida. Esto puede ser atribuido al hecho de que en un elemento de conmutación con buffers de entrada solamente una celda puede grabar dentro del buffer y varias celdas pueden ser leídas del buffer, mientras que en el elemento de conmutación con buffers de salida, varias celdas pueden llegar simultáneamente pero solamente una celda puede salir. En la siguiente discusión se asume que un elemento de conmutación de 16x16 ó 32x32 puede implementarse en un solo circuito integrado con tecnología complementaria semiconductor metal-oxido (CMOS) o Bipolar CMOS (BICMOS). El área del chip puede ser subdividida en la parte de memoria y la parte lógica aleatoria (por ejemplo, un convertidor serie-a-paralelo). El área de memoria es más pequeña en el elemento de conmutación central, mientras que la requerida por el área lógica aleatoria será, sin ninguna duda, más grande que para los otros dos tipos.

La figura 2.27 muestra la relación entre el tamaño del chip y la disipación de potencia para los tres tipos de elementos de conmutación (matriz de conmutación con buffer de salida, matriz de conmutación con buffer de entrada y elemento de conmutación de memoria central). Se debe señalar qué principio específico de implementación y qué tipo de tecnología CMOS se utilizó.

La disipación de potencia de las memorias CMOS es muy pequeña. Por otro lado la lógica aleatoria de alta velocidad consume una cantidad relativamente alta de potencia. De esto resulta una relación no-lineal entre el tamaño del chip y la disipación de potencia de los elementos de conmutación considerados. De todo esto, es evidente que, en cuanto al tamaño del chip y la disipación de potencia, el elemento de conmutación de memoria central tiene ventajas claras, mientras que el elemento de conmutación con buffers de salida es la menos favorable.

2.3.2 Redes de conmutación

Esta sección tratará la clasificación general de redes de conmutación. La figura 2.28 da un vistazo a las redes presentadas.

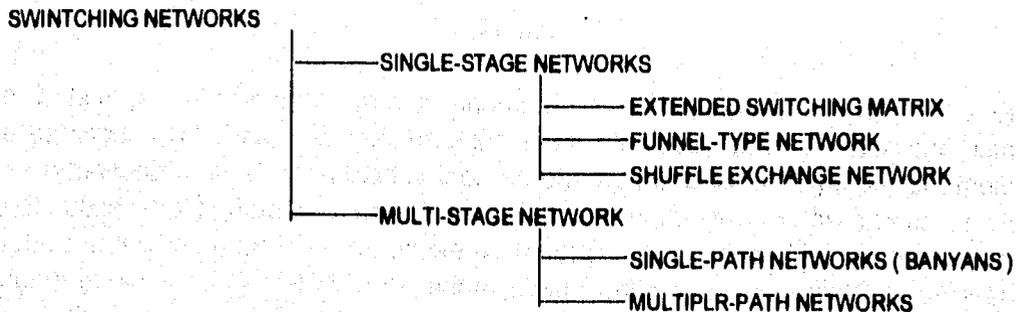


Figura 2.28

2.3.2.1 Redes de una etapa

Una red de una etapa se caracteriza por una sola etapa de elementos de conmutación los cuales están conectados a las entradas y salidas de una red de conmutación.

2.3.2.1 Matriz de conmutación extendida

La figura 2.29 muestra un ejemplo de matriz de conmutación extendido la cual está formada por elementos de conmutación de $b \times b$. Básicamente, cualquier tamaño de red de conmutación puede implementarse con esta configuración.

Para formar una matriz de conmutación extendida los elementos de conmutación descritos anteriormente, tienen que ser extendidos agregando entradas "b" y salidas "b". Las señales de entrada son relevadas a la siguiente columna de la matriz por medio de salidas adicionales. Las entradas adicionales se conectan a las salidas normales del elemento de conmutación en la misma columna pero en el renglón superior.

La ventaja del elemento de conmutación extendido es el pequeño retardo de cruce dado que las celdas solamente son bufereadas una vez cuando cruzan la red. De esto se observa que el retardo de cruce es dependiente de la localidad de entrada. El hecho de que el número de elementos de conmutación aumente con el número de entradas requeridas limita el tamaño de una matriz de conmutación extendida. Es posible formar una red de una sola etapa de 64×64 ó 128×128 , pero una red mult- etapa será preferible para sistemas más grandes.

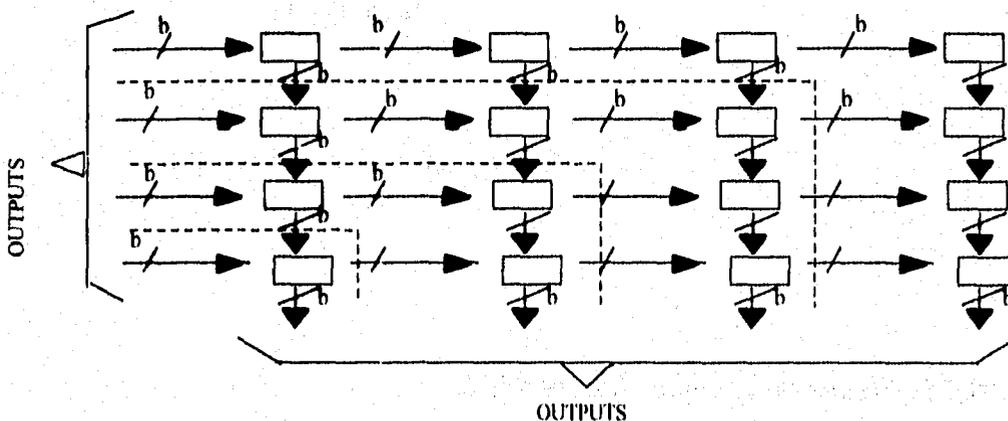


Figura 2.29

2.3.2.1.2 Red tipo embudo

En la red de conmutación de no-bloqueo de $N \times N$ mostrada en la figura 2.30, los elementos de conmutación están interconectados a una estructura tipo embudo. Todos los elementos de conmutación consisten de " $2b$ " entradas y " b " salidas. Cada embudo representa una matriz de $N \times b$, de la cual hay N/b en paralelo.

Con la tecnología actual es posible realizar elementos de conmutación de 32×16 . Una red de conmutación de 128×128 de una etapa puede implementarse con estos elementos. La aproximación multi-etapa puede ser la mejor solución para redes grandes.

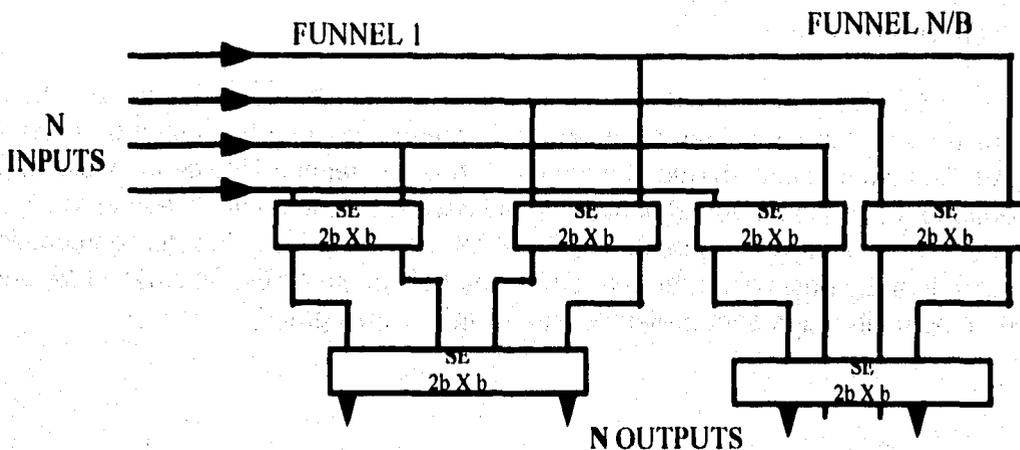


Figura 2.30

2.3.2.1.3 Redes de conmutación mezclada

Las redes de "conmutación mezclada" pertenecen a la clase de redes de una etapa. Se basan en una "conmutación mezclada" perfecta la cual está conectada a una etapa de elementos de conmutación (figura 2.31). Un mecanismo de realimentación es necesario para lograr una salida arbitraria de una entrada dada (este mecanismo está dibujado con líneas punteadas en la figura 2.31).

Es evidente que una celda puede pasar a través de la red varias veces antes de alcanzar su propio destino. Por lo tanto, también se le denomina red de

"recirculación". En la salida de un elemento de conmutación, éste tiene que decidir entre si la celda puede dejar la red o tiene que reglamentar la entrada.

Este tipo de red requiere solamente un número pequeño de elementos de conmutación, pero el rendimiento no es muy bueno. El retardo de cruce depende del número de elementos de conmutación que tienen que atravesar.

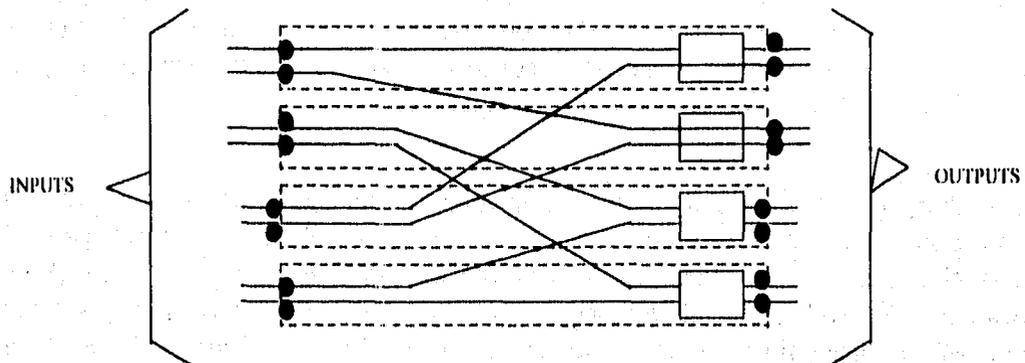


Figura 2.31

2.3.2.2 Redes multi- etapas.

Las redes multi- etapa se pueden usar para evitar las desventajas de las redes de una etapa. Se construyen de varias etapas, las cuales están interconectadas por una cierta liga modelo. Según el número de rutas que están disponibles para llegar a la salida destino de una entrada dada, estas redes se pueden subdividir en dos grupos denominados redes de "una ruta" y "multi-ruta".

2.3.2.2.1 Redes de una ruta

En las redes de una ruta, hay solamente una ruta al destino de una entrada dada. Estas redes también son llamadas redes "Banyan". Debido a que solamente existe una ruta para la salida, el ruteo es muy simple. Las redes Banyan tienen la desventaja de que puede ocurrir el bloqueo interno. Esto resulta de la propiedad de que una liga interna puede ser utilizado por diferentes entradas simultáneamente. Las redes Banyan pueden clasificarse en subgrupos.

En las redes Banyan nivel-(L), solamente están conectados los elementos de conmutación de etapas adyacentes. Cada ruta atraviesa la red pasando a través

de exactamente "L" etapas. Además, esta clase está subdividida en Banyan "regular" e "irregular". Las Banyans regulares se construyen de elementos de conmutación idénticos, mientras que las Banyans irregulares pueden usar diferentes tipos de elementos de conmutación. La red delta generalizada pertenece a la clase Banyans irregulares.

Las Banyans regulares tiene la ventaja de que se pueden implementar económicamente debido a que están construidas por elementos de conmutación idénticos. A continuación, solamente serán considerados los Banyans-SW, los cuales son una subclase de los Banyans regulares.

Los Banyans-SW se construyen recursivamente del elemento de conmutación básico con eslabones de entrada "F" y eslabones de salida "S". La Banyan-SW más simple es con un elemento de conmutación (llamado Banyan nivel-(1)). Un Banyan-SW nivel-(L) se obtiene conectando varios Banyan-SW nivel-(L-1) con una etapa adicional de elementos de conmutación de (FxS). Estos elementos de conmutación extra se conectan de manera regular a las Banyan-SWs

Las "Redes delta" son una implementación especial de Banyan-SWs. Las redes nivel-L que están construidas por elementos de conmutación de (FxS) tienen salidas "S" a la "L". Cada salida puede identificarse por una dirección de destino única, la cual es un número de base "S" con dígitos "L". Cada dígito especifica la salida destinada del elemento de conmutación en una etapa específica. Esto permite un ruteo simple de celdas a través de la red delta, lo cual se denomina "auto ruteo".

En las redes "delta rectangulares" los elementos de conmutación tienen el mismo número de entradas y salidas ($S=L$). En consecuencia, el número de entradas de la red es igual al número de salidas de la red. Estas redes también se denominan "redes delta-s". La figura 2.32 muestra una red delta-2 con cuatro etapas la cual tiene topología de una red línea-base. La línea gruesa indica la ruta de la entrada 5 a la salida 13 (dirección destino binaria 1101).

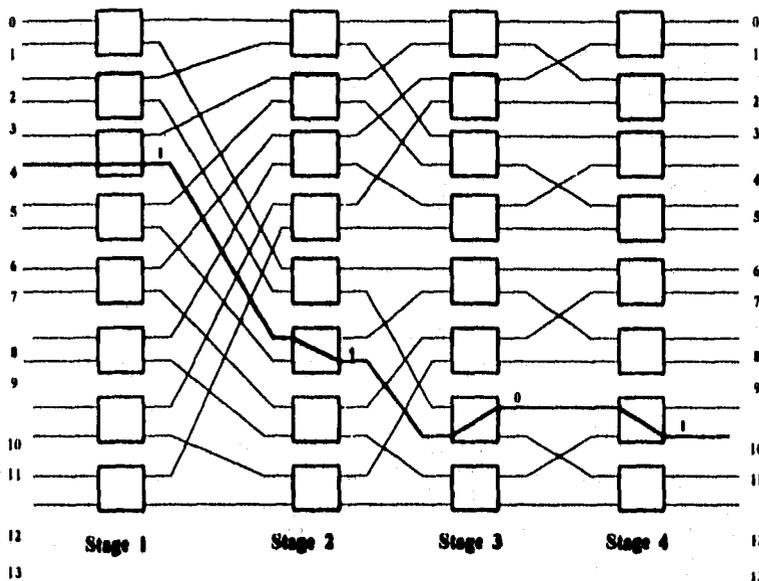


Figura 2.32

Las redes "bidelta" son una clase especial de redes delta; aun cuando las entradas son interpretadas como salidas y viceversa. Todas las redes delta son topológicamente equivalentes y pueden transformarse en otra de ellas renombrando los elementos de conmutación y las ligas.

2.3.2.2 Redes multi-ruta

En las redes multi-ruta, existen múltiples alternativas para la salida destinada de una entrada dada. Esta propiedad tiene la ventaja de que el bloqueo interno puede reducirse o casi evitarse.

En la mayoría de las redes multi-etapa la ruta interna será determinada durante la fase de conexión. Todas las celdas de la conexión usarán la misma ruta interna. Si se tienen FIFOs en los elementos de conmutación individual, la integridad de la secuencia de la celda puede garantizarse y no será necesario re-secuenciar.

En esta clasificación, las redes multi-ruta se pueden subdividir en redes dobladas y desdobladas.

La figura 2.33 muestra una red doblada de tres etapas. En las redes dobladas, todas las entradas y salidas se localizan en el mismo lado de la red de conmutación y las ligas internas de la red se operan de manera bidireccional (cada eslabón en la figura 2.33 representa las líneas físicas para ambas direcciones).

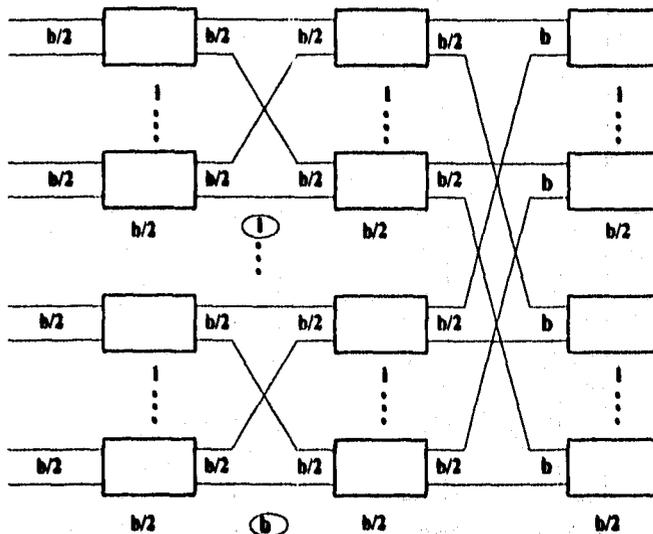


Figura 2.33

Las redes dobladas tienen la ventaja de que se pueden utilizar las rutas cortas. Por ejemplo, si la línea de entrada y las líneas de salida están conectadas al mismo elemento de conmutación, pueden ser reflejadas en el elemento de conmutación y necesitan no pasar a la última etapa. El número de elementos de conmutación que las celdas de una conexión tienen que atravesar depende de la localización de las líneas de entrada y salida.

La capacidad del puerto de una red doblada con tres etapas constituida de elementos de conmutación de $b \times b$ es $(b/2)(b/2)b$. Con la tecnología actual, los elementos de conmutación de tamaño 16×16 y 32×32 se pueden implementar dirigiendo redes de tres etapas con puertos de 1024 y 8192 respectivamente.

En una red doblada, las entradas están en un lado y las salidas en el lado opuesto de la red. Los estabones internos son unidireccionales y todas las celdas tienen que atravesar el mismo número de elementos de conmutación.

La estructura de las redes dobladas multi-ruta se basa en una estructura de red de una ruta. Además, la base de estas redes son elementos de conmutación de $b \times b$. Para simplificar, solamente se presentarán elementos de conmutación de 2×2 en las figuras.

Se describe una red de conmutación, la cual consiste de una red Banyan bufereada y una red de distribución anterior (figura 2.34). La red de distribución

tiene el propósito de distribuir tan uniformemente como sea posible sobre todas las entradas de la red Banyan. Esta aproximación puede reducir el bloqueo interno. No obstante, no se puede mantener la integridad de la secuencia de la celda de una conexión, por lo tanto se requiere un mecanismo adicional de re-secuenciamiento en la salida.

Otra de estas redes es la combinación de una red de sorteo y una red de trampa enfrente de una red Banyan (figura 2.35). La red de sorteo dispone la llegada de las celdas en una secuencia monótona dependiendo de la dirección de destino interna de la red.

Las celdas con direcciones iguales son detectadas por la red de trampa y una de todas las celdas es retroalimentada a la entrada de la red de sorteo. Las celdas que tienen que atravesar la red de sorteo serán asignadas nuevamente a una prioridad alta en la lista para mantener la integridad de la secuencia de la celda. Las celdas que entran a la red Banyan pueden ser transportadas a sus destinos sin ningún bloqueo interno.

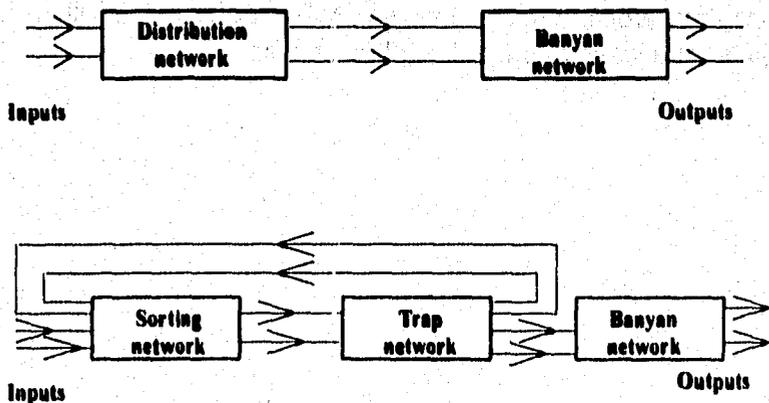


Figura 2.34 y 2.35

Las redes de ruta múltiple pueden también implementarse usando varios planos de redes Banyan en paralelo. Esto se denomina apilamiento vertical.

Todas las celdas pertenecen a la misma conexión atraviesan el mismo plano. Este estará determinado durante la fase de inicio de conexión. Una celda entrante será conmutada a su plano apropiado por la unidad de distribución, la cual se localiza en cada línea de entrada. En la salida de conmutador, un multiplexor estadístico colecta celdas de todos los planos. En este se demuestra que con dos planos en paralelo se puede lograr una estructura de conmutación no bloqueada virtualmente.

Agregando un número de etapas a una red Banyan dada se obtiene un apilamiento horizontal. Una red de interconexión multi-ruta (MIN) se construye agregando una red de línea base con topología invertida a una red de línea base existente. (Figura 2.36).

Asumiendo elementos de conmutación de $b \times b$ la red de $N \times N$ tiene etapas de $2 \log$ base b de N . En una red de $N \times N$, las rutas internas N están disponibles a una salida dada de una entrada arbitraria. Para una entrada particular, la ruta interna puede ser seleccionada arbitrariamente hasta la salida de la red de línea base. Entonces la forma de atravesar la red de línea base es fija.

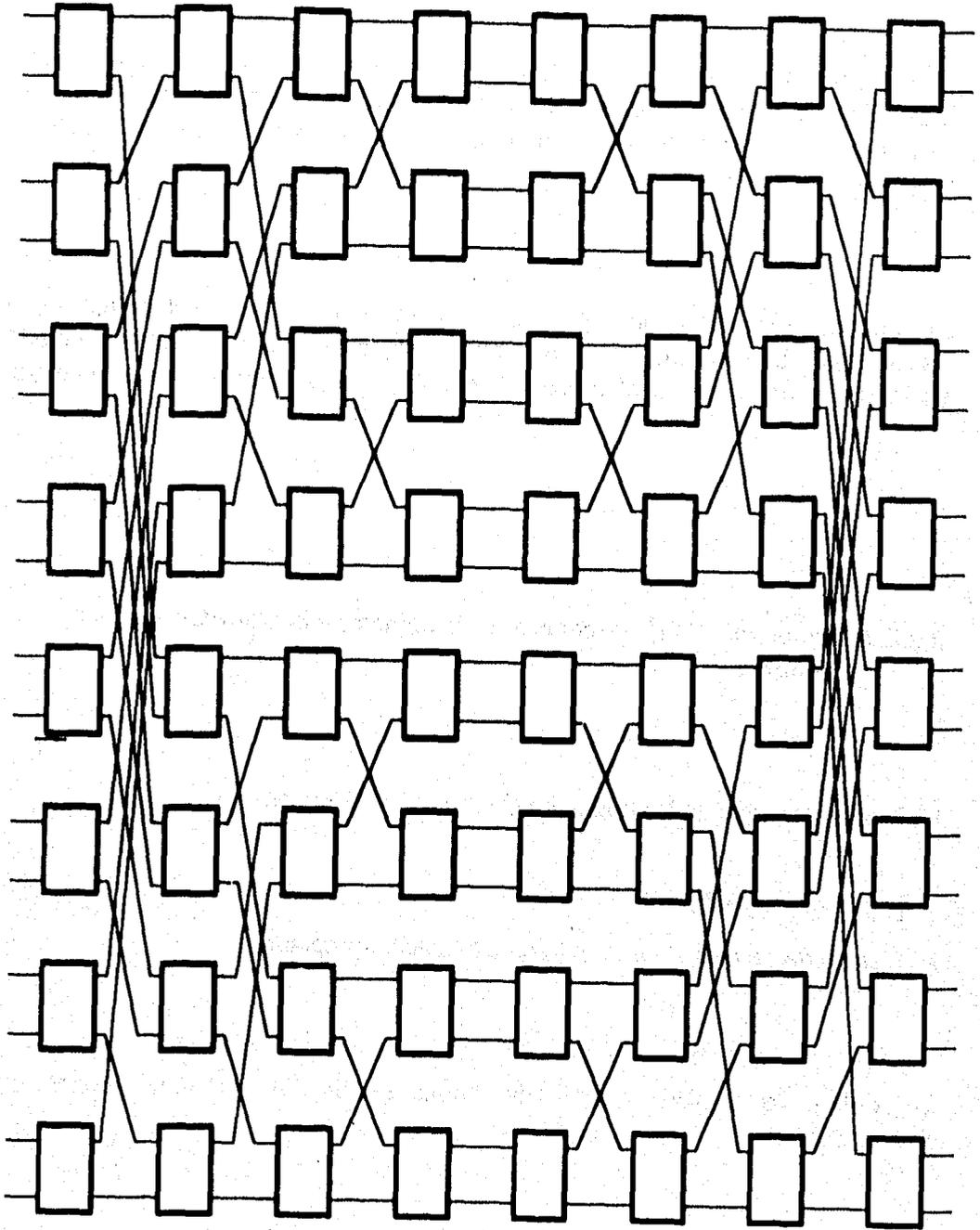


Figura 2.36

Una red Benes es muy similar a la MIN. La diferencia es que la última etapa de las redes de línea base coincide con la primera etapa de la red de línea base invertida. No obstante, el número de etapas está reducido a uno comparado con la MIN.

De nuevo, asumiendo elementos de conmutación de bxb, solamente están disponibles rutas alternativas de N/b para cualquier salida de cualquier entrada. Cada ruta es única para el elemento de conmutación que pasó en la etapa central.

2.3.2.3 Procesamiento de encabezado de celdas en la manufactura del conmutador.

La función principal de los nodos de conmutación ATM son:

1. Traducción VPI/VC1
2. Transporte de celdas de la entrada a la salida apropiada.

En orden de implementación de estas tareas, se pueden aplicar dos aproximaciones:

- Principio de auto-ruteo
- Principio de tabla de control

2.3.2.3.1 Elementos de conmutación de auto-ruteo

Cuando usamos los elementos de conmutación de auto-ruteo, la traducción VPI/VCI será desempeñada solamente en la entrada de la red de conmutación. Después de la traducción la celda es extendida por un header interno de la red de conmutación. Este header precede la celda header. La extensión de celda header requiere un incremento interno de velocidad de red.

En una red de k etapas el header interno es subdividido en k subcampos. el subcampo l contiene el número de salida destino del elemento de conmutación en la etapa l .

2.4 Señalización

2.4.1 Introducción

Por un lado las redes ATM deberán estar disponibles tan pronto como sea posible, y por otro lado una variedad de servicios (tanto simples como muy sofisticados) estarán integrados en una sola red. Es obvio que estos dos logros no pueden darse en un solo paso.

Considerando este problema se desarrolló un "itinerario" de red B-ISDN. Este concepto comprende tres aspectos: release 1, 2 y 3. La característica principal es la influencia de la señalización, la cual está resumida en la tabla 1.

Release 1: Contiene servicios de switcheo con tasa bit constante e interactúa con el existente ISDN de 64 Kbit/s, nótese que mientras los servicios de tasa bit variable pueden ser transportados, una tasa bit máxima deberá estar alojada. Dos configuraciones de acceso de señalización se pueden usar, una de las cuales requiere una meta-señalización.

Release 2: Proporciona servicios más sofisticados con tasa bit variable (asumiendo que es posible tomar ventaja del multiplexaje estadístico); soporta conexiones punto-a-multipunto y multi-conexiones. Con el release 2, **call** y **connection control** estarán separados, esto es, las direcciones estarán atrapadas (set up) y liberadas durante una llamada.

Finalmente, el release 3 proporciona rangos completos de servicios, incluyendo multimedia y servicios distribuidos.

Se asume que la influencia del "itinerario" no es tan fuerte en los protocolos de transferencia de la señalización. De esta manera, los protocolos deberán ser aplicables para todas las versiones (tal vez con alguna extensión y/o modificación).

Tabla 2.2 "Itinerario" para señalización B-ISDN

Release 1	Release 2	Release 3
Tasa bit constante Servicio orientado a conexión con temporización end-to-end	Tasa bit variable Servicio orientado a conexión Calidad de indicación de servicio por el usuario	Servicio multimedia y distribuido Calidad de negociación
Conexiones punto-a-punto (uni- y bidireccional, simétrico y asimétrico) Conexión simple, establecimiento simultáneo	Conexiones punto-a-multipunto Multiconexión, establecimiento con retardo Uso de prioridad de pérdida de celdas	Conexiones de transmisión
Indicación de ancho de banda máximo Alojamiento de tasa máxima	Negociación y renegociación de ancho de banda Alojamiento de ancho de banda en base a características de tráfico	
Interoperación con ISDN de 64 Kbit/s Accesos de señalización punto-a-punto y punto-a-multipunto. Servicios suplementarios limitados de señalización-meta	Servicios suplementarios	

2.4.2 Arquitectura de protocolo para el Relase 1

La ITU-T diferencia entre dos configuraciones de acceso para señalización UNI:

- 1.- Configuración de acceso de señalización punto-a-punto.
- 2.- Configuración de acceso de señalización punto-a-multipunto.

En el caso de configuración de acceso de señalización punto-a-punto hay solamente un punto final de la señalización en el lado del usuario. Esta podría ser una terminal simple o una B-NT2 inteligente, por ejemplo va PBX, dependiendo la configuración de red del vendedor. En esta configuración sólo se necesitará un SVC punto-a-punto permanentemente establecido. Este canal se usa para ofrecer llamadas, establecer llamadas y liberarlas.

También se pueden tener varios puntos finales de señalización localizados del lado del usuario por ejemplo, configuración de terminal punto-a-multipunto, en las configuraciones de acceso de señalización punto-a-multipunto. Para el caso de señalización meta es necesario manejar otra relación de señalización.

El protocolo para estas dos configuraciones de acceso de señalización se muestra en el lado izquierdo de la figura 2.37.

En la NNI, existe ya un sistema de señalización No. 7 (SS7) de canal común STM o una red ATM que pueda ser usada para transportar mensajes de señalización. Para ambos casos se necesita un protocolo de aplicación apropiado, el cual será descrito más adelante.

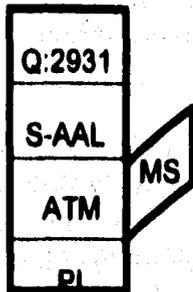
Es evidente que el uso del SS7 permite la rápida introducción del B-ISDN. Sin embargo una red de transporte de señalización puede también tomar ventaja de la tecnología ATM, y así en un futuro una red de transporte de señalización ATM podrá ser la mejor solución. En el caso de transferencia de señalización ATM, los CVCs entre los dos switches estarán administrados por protocolos OAM y entonces la meta-señalización no será necesaria en la UNI:

Interface usuario-red

acceso de señalización punto-a-punto

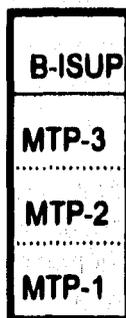


acceso de señalización punto-a-multipunto

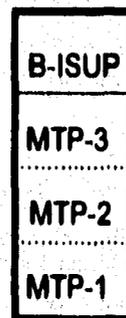


Interface red-nodo

red de señalización STM



red de señalización ATM



- ATM Modo de transferencia asíncrona
- B-ISUP Parte de usuario ancho de banda ISDN
- MS Señalización meta
- MTP Parte de transferencia de mensaje

- PL Nivel físico
- Q.2931 Protocolo Q.2931
- S-AAL ATM Capa de adaptación para la señalización
- STM Modo de transferencia Síncrona

Figura 2.37 Arquitectura del protocolo para la señalización B-ISDN

2.4.3 Meta-Señalización

2.4.3.1 General

La recomendación Q.2120 de la ITU-T describe el protocolo de meta-señalización que será usado para el establecimiento, mantenimiento y traslado de conexiones de señalización usuario-red en la UNI.

El protocolo de meta-señalización solamente opera sobre el MSVC. Actualmente es el único protocolo que usa ese canal. El MSVC está definido por VCI=1 en todos los VP y por default la tasa de celda máxima es 42 celdas/s. En un principio, el protocolo de meta-señalización puede operar en cada VP activo. Sin embargo, esto es suficiente para usarlo solamente en un VP entre el usuario y un intercambio local. Esto reduce el esfuerzo de implementación.

El protocolo de meta-señalización es una parte de las capas de ATM. Está localizado en el plan de administración de capas y bajo el control de un plan administrativo. Comúnmente, el Foro ATM no apoya la meta-señalización porque solamente considera configuraciones de señalización punto-a-punto.

2.4.3.2 Aplicación y Alcance

Los protocolos de meta-señalización proporcionan los procedimientos para:

- Asignar y trasladar SVCs punto-a-punto (PSVCs) y sus asociados BSVCs.
- Verificación del status de estos dos tipos de canal.

Con estos procedimientos es posible:

- Asociar un extremo de la señalización con PSVC y un PSVC.
- Alojarse la tasa de celda a SVCs.
- Resolver posibles problemas de contención para SVCs.

Los procedimientos de asignación, verificación y traslado son independientes entre sí. La relación necesaria entre ellos se realiza administrativamente.

Normalmente, el protocolo de meta-señalización es usado entre el usuario y la red. Sin embargo, dos usuarios que están conectados vía un VPC también pueden usar este protocolo para administrar el PSVCs y BSVCs. En este caso deberá usarse el valor de VCI predefinido.

Como se mencionó en la sección anterior, el protocolo de meta-señalización solamente se usa en configuraciones de acceso de señalización punto-a-multipunto. Como una opción de red también se puede aplicar en configuraciones de acceso de señalización dinámica. En este caso el usuario puede usar la meta-señalización para informar a la red si la configuración de acceso de señalización es punto-a-punto o punto-a-multipunto.

2.4.3.3 Resultado de los protocolos

En esta sección nos enfocaremos a los siguientes detalles del protocolo de señalización:

- Formateo de mensajes
- Procedimientos

2.4.3.3.1 Formateo de mensajes.

El formato del mensaje para mensajes de meta-señalización está representado en la figura 2.38, y es independiente del tipo de mensaje, puesto que cada mensaje consiste de la misma estructura. Los campos que no están usados por el mensaje se codifican con un valor "null".

El primer campo es llamado **protocol discriminator (PD)**. Identifica mensajes en el canal de meta-señalización, tales como mensajes de meta-señalización o mensajes pertenecientes a otro protocolo. Actualmente protocolo de meta-señalización es el único protocolo usado en el canal de meta-señalización.

El campo **versión del protocolo (Protocol Version, PV)**, encuentra la diferencia entre las versiones individuales del protocolo de meta-señalización e identifica el formato del mensaje general a usarse. El formato descrito en esta sección es válido para el release 1.

Los nombres de los mensajes están identificados por el campo **tipo de mensaje (Message Type, MT)**. Este también se usa para determinar la función exacta y el formato de detalle de cada mensaje.

Los seis mensajes siguientes son usados por el protocolo de meta-señalización:

1. **ASSIGN REQUEST**
2. **ASSIGNED**
3. **DENIED**
4. **CHECK REQUEST**
5. **CHECK RESPONSE**
6. **REMOVED**

Bit								Octet number
8	7	6	5	4	3	2	1	
Discriminador de protocolo								1
Versión del protocolo								2
Tipo de mensaje								3
Identificador de referencia								4...5
Identificador de canal A virtual de señalización								6..7
Identificador de canal B virtual de señalización								8..9
Tasa celda punto-a-punto								10
Causa								11
Identificador de perfil de servicio								12...22
Campo-nulo								23...46
								47
Verificación de redundancia cíclica								48

Figura. 2.38 Formato de mensajes meta-señalización

El campo **identificador de referencia** (Reference Identifier, RI), se usa para diferenciar entre un número de procedimientos asignados simultáneos. El valor es generado aleatoriamente por cada mensaje "ASSIGN REQUEST" por la terminal individual. La respuesta asociada es identificada por el mismo valor del identificador de referencia.

El contenido de los campos A y B de los "identificadores de canal virtual de señalización" (SVCI A y SVCI B) dependen del procedimiento que se esté usando. Los contenidos pueden ser:

- Un identificador de canal virtual de señalización punto-a-punto (PSVCI).
- Un identificador de canal virtual de señalización de transmisión (BSVCI).
- Un identificador de canal virtual de señalización global.

Un PSVC está identificado por el PSVCI. El PSVC transfiere todas las llamadas punto-a-punto y/o señalización de control portadora a un extremo de la señalización dado. El BSVCI indica el valor de un BSVC. Un BSVC siempre es un canal unidireccional y se usa en la dirección de la red al usuario para el ofrecimiento de la llamada. Este canal puede ser el BSVC general o el BSVC selectivo. Mientras que el BSVC general está identificado por un valor VCI definido durante la fase de asignación. El BSVC selectivo tiene una relación estrecha con el identificador de perfil de servicio, el GSVCI indica todos los canales de señalización excepto el canal de señalización mismo. Es un identificador único y está identificado por VCI=1. Se usa para una verificación global (por ejemplo), esto es, todos los extremos de señalización activos tienen un mensaje de "CHECK RESPONSE" después de recibir un mensaje de "CHECK REQUEST" del GSVCI.

El campo **tasa celda punto-a-punto de SVC** (point-to-point SVC cell rate, PCR) indica la tasa de la celda requerida/alojada para el canal virtual de señalización punto-a-punto. Comúnmente, sólo se usa alojar la tasa máxima de la celda. Posteriormente, cuando es posible tomar ventaja del multiplexaje estático, la codificación de este campo se puede extender para cubrir esta nueva característica. Los siguientes valores están definidos: 42, 84, 168, 336, 672, 1344, 2688 celdas/s. Note que 42 celdas/s son aproximadamente 16 Kbit/s y 2688 celdas/s son aproximadamente 1024 Kbits/s.

El campo **cause** (CAU) proporciona al usuario información más detallada, esto indica la razón para mandar el mensaje (por ejemplo; por qué la red manda el mensaje "DENIED").

El campo **service profile identifier** (SPID) es usado por el usuario para hacer un requerimiento básico o un nivel específico de servicio. El SPID apunta al perfil de servicio, el cual es un conjunto de información administrada por la red para proporcionar el fundamento o algún servicio específico al extremo de señalización. Cuando ambos, la red y el usuario sostienen el concepto de perfil de servicio, las llamadas pueden ofrecerse vía BSVC selectivo. En este caso, solamente un subconjunto de todos estos extremos de señalización localizados del lado del usuario, reciben la llamada ofrecida y de esta forma se simplifica el procedimiento de ofrecimiento de llamada.

Todos los bits del campo null-fill están codificados con '0'.

El último campo en el mensaje meta-señalización es el campo CRC, el cual es usado para detectar errores en mensajes de meta-señalización. Se usa un polinomio generador, el cual es el mismo que para AAL tipo 3/4.

	Mensajes					
	REQUERIMIENTO DE ASIGNACION	ASIGNADO	DENEGADO	REQUERIMIENTO VERIFICACION	RESPUESTA VERIFIC.	TRASLADO
PD	M	M	M	M	M	M
PV	M	M	M	M	M	M
MT	M	M	M	M	M	M
RI	M	M	M	-	-	-
SVCI A	- *	M	-	M	M	M
SVCI B	-	M	-	-	M	-
PCR	M	M	-	-	-	-
CAU	-	M	M	-	-	-
SPID	M	M	-	-	M	-
CRC	M	M	M	M	M	M
Dirección	U --- N	N --- U	N --- U	N --- U	U --- N	U --- N ó N --- U

- * Codificado normalmente con valor nulo
- M valor válido que debe estar presente
- codificado con valor nulo
- N --- U dirección red a usuario
- U --- N dirección usuario a red

Tabla 2.3 Mensajes meta-señalización y parámetros asociados

2.4.3.3.2 Procedimientos

Los siguientes procedimientos son utilizados por el protocolo de meta-señalización:

- Asignación
- Verificación
- Traslado

El procedimiento de asignación es invocado por el usuario para enviar un mensaje de "ASSIGN REQUEST" a la red, preguntando por un PSVCI y BSVCI. La red, dependiendo de la condición, enviará un mensaje "ASSIGNED" indicando el par PSVCI/BSVCI o enviará un mensaje "DENIED" con la razón apropiada. Este procedimiento es supervisado por un temporizador del lado del usuario para la recuperación de mensajes.

El procedimiento de verificación es iniciado por la red enviando un mensaje "CHECK REQUEST" y esperar por el mensaje "CHECK RESPONSE". La verificación más simple consiste de un par PSVCI/BSVCI, mientras que la verificación más general consiste de todos los canales de señalización. Este procedimiento también es supervisado por un temporizador del lado de la red.

El procedimiento de traslación puede ser inicializado ya sea por la red o por el usuario, en contraste con los otros dos procedimientos. El lado iniciador manda solamente el mensaje "REMOVED" seguido, después de un intervalo aleatorio, por un segundo mensaje "REMOVED". Este mecanismo es muy simple y previene los errores que puedan ocurrir si un mensaje "REMOVED" se pierde.

Del lado del usuario cada mensaje se retarda por algún tiempo aleatorio antes de ser transmitido a la red. Este es igual para todos los mensajes, si no es éste siempre necesario. No obstante, este mecanismo simple impide ciertas condiciones de sobrecarga (overload) de la red, que de otra manera ocurrirían (p.e., cuando la red inicia un verificación global en todas las terminales contestaría casi simultáneamente).

2.4.4 Capa de adaptación ATM para la señalización

Se requiere un nivel de adaptación ATM para la señalización (S-AAL), adecuada para adaptar los protocolos de aplicación de la señalización para la UNI y la Nni a los servicios proporcionados por la capa ATM fundamental. La S-AAL está subdividida en las siguientes partes:

- Parte común (CP)
- Parte de servicio específico (SSP)

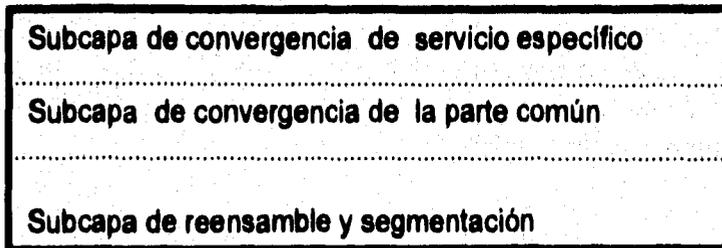


Figura 2.39 Capa de adaptación ATM para señalización

2.4.4.1 Parte común

En un principio ambos, la AAL tipo 3/4 y la AAL tipo 5 son adecuados para la CP. La ITU-T decidió usar la AAL tipo 5 porque es un protocolo simple con solamente un overhead pequeño.

La AAL tipo 5 tiene un mejor desempeño (p.e. más alta eficiencia, throughput, más bajo tiempo de transferencia promedio) para mensajes largos. Por otro lado, para mensajes cortos (1 a 3 celdas) y una alta probabilidad de pérdida de celdas, la AAL tipo 3/4 tiene un mejor desempeño. Esto es porque la última celda de un AAL-PDU está pérdida, y el error no puede ser detectado inmediatamente por una AAL tipo 5. El error será detectado después de recibir la PDU adyacente. No obstante, el receptor no puede indicar cual AAL-PDU está erróneo y entonces descarta ambas PDUs.

2.5.4.2 Parte de servicio específico

La ITU-T decidió utilizar un protocolo común para la UNI y la NNI, el cual se describe en las Recomendaciones Q.2100, Q.2110, Q.2130 y Q.2140 de la ITU-T, para la SSP. La relación entre la UNI y la NNI proporciona los siguientes beneficios:

- Reducción de la complejidad en los nodos de la red.
- Tiempo de especificación corto.
- Flexibilidad en operación y configuración de la red.
- Eficiente operación y mantenimiento de la red.
- Reducción de costos de operación y fabricación.

Nótese que la relación entre la UNI y la NNI no es posible; esto es porque hay diferentes protocolos sobre la S-AAL en la UNI y la NNI. Para cumplir con los requerimientos de los diferentes protocolos de la S-AAL, en la figura 2.40 se muestra la arquitectura seleccionada.

El protocolo de conexión-orientada para servicio específico (SSCOP), proporciona mecanismos para el establecimiento y liberación de conexiones y el oportuno intercambio de información de señalización entre entidades de señalización. Las funciones de coordinación de servicio-específico (SSCFs) mapean los requerimientos de la capa sobre los requerimientos de la siguiente capa inferior.

Para el caso del SSCOP podría usarse un protocolo de capa de liga de datos de servicios del portador de modo libre, con algunas modificaciones y mejoras. La aplicación de un protocolo existente podría tener el mismo enfoque tal como los protocolos de aplicación de la señalización para el release 1, proporcionando las mismas ventajas (p.e. procesos de especificación cortos). No obstante, la ITU-T decidió especificar un nuevo protocolo para la SSCOP, el cual será simple y eficiente.

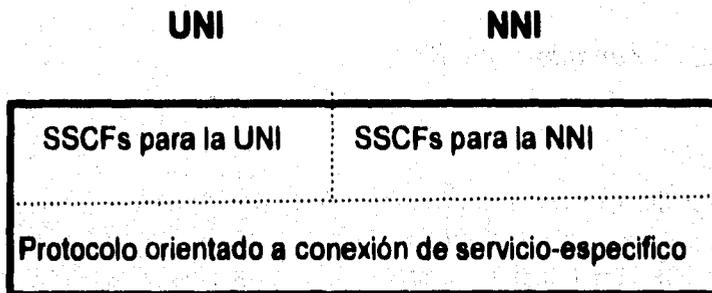


Figura 2.40 Parte específica de servicio de S-AAL

El nuevo SSCOP desempeña las siguientes funciones:

- **Integridad de secuencia:** Conserva el orden de los SSCOP-SDUs.
- **Corrección de error por retransmisión:** Los SSCOP-SDUs que faltan son detectados por el receptor usando un mecanismo de secuencia. El SSCOP corrige entonces el error por retransmisión selectiva.
- **Control de Flujo:** El receptor controla la tasa de mensajes que está asociada con el correspondiente transmisor que envía el mensaje por medio de un mecanismo de ventana dinámica.
- **Reporte de error al administrador de capas:** La ocurrencia de errores es indicada al administrador de capas.
- **Actividad retenida (Keep alive):** Dos entidades parejas (peer) permanecerán en conexión en el evento de una ausencia prolongada de transferencia de datos.
- **Recuperación de datos locales:** Los SDUs pueden recuperarse cuando aún no han sido liberados o reconocidos (esto es, que no han sido aprobados, en todo caso esta función es parte del SSCOP o SSCF).
- **Administración de enlace:** Esta función establece, libera y resetea conexiones de SSCOP.
- **Transferencia de datos:** Esta función desempeña la transferencia de mensajes entre dos entidades par-a-par. El SSCOP proporciona la seguridad y la inseguridad (assured, unassured) en el modo de transferencia de datos.
- **Detección de error de PCI:** Los errores en PCI son detectados.
- **Reporteo de status:** El SSCOP transmisor y receptor puede intercambiar información del status usando esta función.

Para lograr un protocolo de velocidad alta, las máquinas de estado receptora y transmisora están desacoplados, debido a que la retransmisión selectiva y el mecanismo de ventana dinámica para el control de flujo, son las mayores características comparadas con los protocolos de capas de enlaces de datos existentes. Para más detalle la lista de protocolos, mensajes utilizados y operación de protocolos se encuentran en la recomendación Q.2110 de la ITU-T.

Como se muestra en la figura 2.40, los diferentes SSCFs son necesarios, uno para la UNI y otro para la NNI. El SSCF mapea las primitivas de servicio entre el SSCOP y la capa 3 del protocolo de la UNI. En la NNI, el SSCF desempeña el mapeo de primitivas entre SSCOP y la parte de transferencia de mensaje nivel 3 (MTP 3) y alguna función local tal como la recuperación local.

2.4.5 Protocolos de señalización para Release 1.

Como se mencionó en la primera sección, el "itinerario" propuesto tiene una fuerte influencia en los protocolos de aplicación de la señalización. Los protocolos del release 1 fueron terminados en 1994. Debido a que estos protocolos no cubren todos los detalles sofisticados del B-ISDN, la mejor solución es utilizar los protocolos existentes con algunas modificaciones. La existencia del protocolo de capa 3 para el ISDN de 64 Kbit/s concuerda con la Recomendación Q.931 de la ITU-T y servirá como base para la UNI, mientras que el protocolo para la NNI está basado en la parte usuaria del ISDN.

El enfoque básico para la especificación de estos protocolos es utilizar los protocolos existentes tanto como sea posible, y mantener las modificaciones lo más simple posibles. No obstante, para asegurar una transmisión uniforme de las implementaciones del release 1 son preparar la separación de llamadas y control del portador. Esta extensión es básica para garantizar el uso de los protocolos del release 1 en nuevas versiones.

2.4.5.1 Interface usuario-red para la señalización

La capa 3 del protocolo de señalización para B-ISDN se describe en la Recomendación Q.2931 de la ITU-T. Este reside directamente sobre el S-AAL. El Q.2931 contiene especificaciones de mensajes de señalización, elementos de información y procedimientos finales de la señalización para la UNI de B-ISDN.

Debido a que la Q.2931 está basada en la especificación de la señalización para 64 Kbit/s, el cual proporciona las mismas funciones de B-ISDN tales como disponibilidad de 64 Kbit/s ISDN. No obstante, el Q.2931 es independiente del protocolo Q.931; éste se realiza utilizando un nuevo discriminador de protocolo para señalización de banda ancha. La estructura del Q.2931 corresponde a la estructura bien conocida de la Q.931. La mayoría de los procedimientos del Q.931 han sido transferidos al Q.2931 con algunas modificaciones simples, en particular los procedimientos de liberación y establecimiento de llamadas.

Hay dos razones que justifican las modificaciones hechas al Q.2931:

- Adaptación al nuevo modo de transferencia ATM.
- Modificaciones adicionales con las cuales se permiten una transición uniforme del protocolo de señalización release 1 a los protocolos release 2 y 3.

La adaptación de un nuevo sistema de transmisión B-ISDN principalmente se refiere a la descripción de los servicios portadores del B-ISDN. En resumen, la tasa de celda ATM describe el eficiencia (throughput) de una conexión ATM. Para el release 1 el valor de la tasa celda ATM se puede seleccionar, pero solamente una tasa de celda máximo resultante de la eficiencia (throughput).

El usuario puede seleccionar entre varias clases diferentes de AAL y sus correspondientes protocolos para sus necesidades de comunicación.

Un identificador de canal antiguo del Q.931 es obsoleto y fue reemplazado por un nuevo elemento de información del identificador de conexión. Este elemento de información consiste de un identificador de conexión de ruta virtual (VPCI) y el VCI existente. El VPCI identifica un VPC, mientras que un VPI solamente identifica una liga a un VP. El uso de un VPCI en un elemento de información de identificador de conexión es necesario puesto que el usuario puede conectarse vía red VP conexión cruzada al intercambio local (figura 2.41). La red VP está controlada por un administrador y no por la señalización. Un extremo de señalización solamente conoce acerca de su propio VPI y no el VPI de un extremo de señalización asociado. De esta forma vemos la necesidad de introducir un identificador único entre el usuario y el intercambio local.

Las modificaciones descritas fueron hechas a la parte principal. Sin embargo, algunas partes de mensajes y procedimientos también necesitaron modificarse un poco. En resumen, la interacción entre los protocolos Q.931 y Q.2931 está especificada en el Q.2931

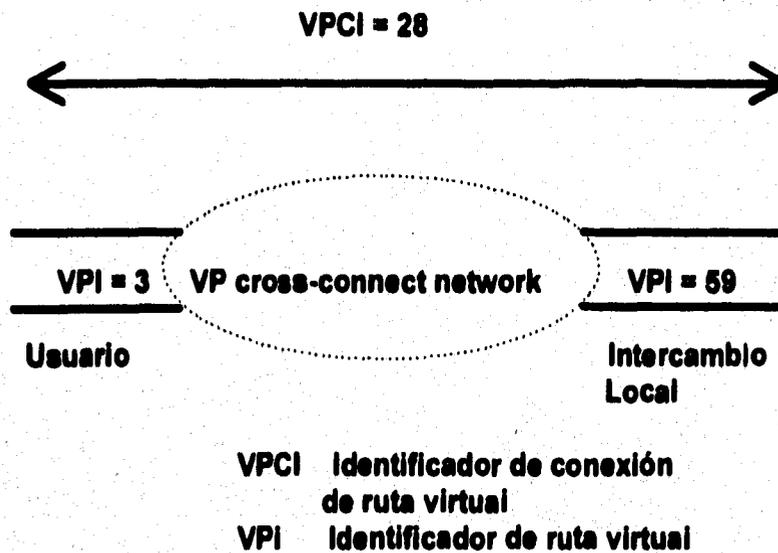


Figura 2.41 Ejemplo de uso de conexión de ruta virtual en la UNI de B-ISDN

Cambios al protocolo	
Elementos de información nuevos/modificados	Capacidad del portador de ancho de banda La tasa celda de ATM Elemento de información del parámetro de AAL Identificador de conexión
Reglas de codificación nuevas/modificadas	Indicación de la longitud del mensaje Formato variable común para elementos de información Ordenamiento libre de elementos de información en mensajes de señalización excepto para el header del mensaje Incluir información compatible
Procedimientos modificados	Verificación de compatibilidad called-side Alojamiento/selección de VPCI/VC1

Tabla 2.4 Resumen de los principales cambios en la recomendación Q.2931 de la ITU-T comparada con la recomendación Q.931.

2.4.5.2 Interface red-nodo de la señalización

Los protocolos de aplicación de la señalización para la NNI se describe en las Recomendaciones Q.2761 a la Q.2764 de la ITU-T. Estas recomendaciones se basan en la descripción y definición de una versión monolítica para ISUP de 64 Kbit/s ISDN.

Los protocolos de aplicación de la señalización para la NNI se denominan ISUP de banda ancha (B-ISUP). Para permitir la independencia de protocolos existentes, se acordó que el nuevo protocolo sea un nuevo ISUP. El B-ISUP utiliza un nuevo punto de código para la información de servicio, esto lo hace diferente al ISUP.

El "itinerario" para el B-ISUP es el mismo que se usó para el protocolo Q.2931. Las modificaciones para el B-ISDN se pueden clasificar en dos partes:

- Modificaciones requeridas para proporcionar señalización.
- Reparaciones para permitir una transición uniforme hacia versiones futuras.

2.4.5.2.1 Modificaciones al B-ISDN.

Las modificaciones más importantes con respecto al ISUP para 64 Kbit/s es la sustitución del código de identificación de circuito (CIC) y sus funciones. Esto también influyó en los procedimientos relacionados con el CIC. En ISUP el CIC identifica:

- El canal de transmisión (elemento de conexión)
- La asociación del control del portador
- La asociación del control de llamada

Canal de transmisión: El valor de 12 bit del CIC está estrechamente asociado a un circuito, el cual es un canal de 64 Kbit/s. En ATM, el canal transmisor está identificado por un nuevo identificador asociado al VP y al VC. El VC está identificado por el VCI, mientras que el VPCI identifica al VP. La razón del porqué el VPI no es útil como identificador único para la UNI también es válido para la NNI. El VPCI es semi-permanente y consiste de 16 bits. Ambos, el VPCI y el VCI están codificados en el parámetro del identificador del elemento de conexión (CEI). El CEI será asignado y usado bidireccionalmente, esto es, que el mismo valor será usado por ambas direcciones.

Asociación del control portador: El comportamiento dinámico del CEI, el cual consiste de 32 bits, es desventajoso para la identificación de la asociación del control del portador lógico. Por consiguiente, la asociación del plan de control está denominada por un identificador de control separado (BCI). Un mecanismo de transacción, es decir, usando origen y destino BCI, será usado, similar a la parte de aplicación de capacidades de transacción (TCAP).

Asociación de control de llamada: En el release 1 no hay distinción entre llamada y conexión. Por consiguiente, la identificación de la asociación de control de llamada está implícitamente proporcionada por el BCI.

Transporte de banda ancha: En contraste con el ISDN de 64 Kbit/s, la banda ancha de una conexión está indicada en forma explícita. La nueva información transfiere el parámetro de tasa que será usado para este propósito. Este parámetro consiste de la tasa de celda máximo trasera y delantera.

Procedimientos OAM: En ISUP, los procedimientos OAM como **reset** y **blocking** y **testing** están estrechamente asociados al CIC. Debido a que CIC fue trasladado, estos procedimientos no pueden usarse para B-ISDN. Es muy probable que estos procedimientos sean separados de los procedimientos del control portador.

Operación de ambas formas: La operación de ambas formas de canales se aplica a Vps y Vcs. En B-ISDN se pueden identificar dos tipos de captura dual:

1. Captura dual del CEI.
2. Captura dual de tasa celda, esto es, requerimiento simultáneo para la última tasa celda disponible en un VPC.

Como los procedimientos de prevención y resolución de captura dual en ISUP no son aplicables, se definen unos nuevos.

Ruteo B-ISDN: El ruteo en ISUP se basa en la indicación de la capacidad de transferencia de información requerida y capacidad de señalización, ambos son valores únicos. El ruteo en B-ISDN vendrá más complejo porque más información (tasa celda, servicio de calidad, subcategoría de servicio de conexión-orientada de banda ancha, simetría, etc.) se toman dentro de una lista.

Formato del parámetro: Todos los parámetros del B-ISUP tendrán un formato común: Nombre del parámetro seguido por un indicador de longitud y el contenido del parámetro. Este formato es idéntico al utilizado para la UNI.

Formato del mensaje: Simplificación del formato del parámetro (solamente uno para todos los parámetros), significa que el formato del mensaje será simplificado para incluir la etiqueta de ruteo seguida del tipo de mensaje, un indicador de longitud y los parámetros B-ISUP. La parte mandatario fija y la parte mandatario variable son longitudes necesarias. El orden de los parámetros puede elegirse arbitrariamente. Este formato es también muy similar al usado para la UNI.

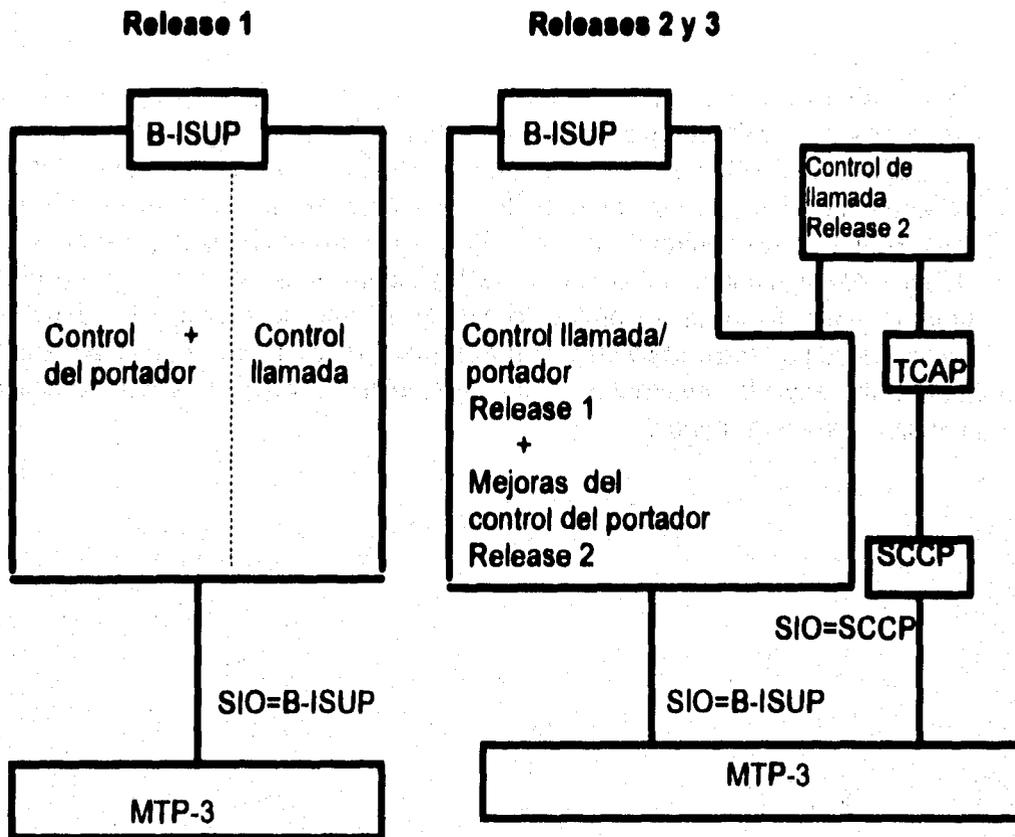
Mecanismos de compatibilidad: Al permitir la compatibilidad hacia adelante, el mecanismo ISUP también será aplicado al B-ISUP. Todos los mensajes y parámetros contendrán instrucciones de compatibilidad para desconocimiento de transporte (nuevo) de información de señalización.

2.4.5.2.2 Evolución del protocolo.

En los releases 2 y 3, el control de llamada y control portador/conexión serán separados. La estructura de niveles de aplicación para OSI serán aplicados a protocolos. El B-ISUP será usado principalmente como control portador. Por consiguiente, el reuso de del B-ISUP -con algunas modificaciones y mejoras- como protocolo de control portador sería posible en releases 2 y 3 (figura 2.42). Algunas precauciones, tales como nivel de sintaxis, es necesario para permitir mejoras y evolución de un protocolo simple. El uso de técnicas de descripción modernas como **abstract syntax notation no. 1 (ASN.1)**, sería posible. Además, la armonía entre los elementos de los protocolos de la UNI y la NNI simplificará la interacción entre ambas.

2.4.6 Requerimientos para protocolos de señalización Release 2.

Paralelamente a la especificación de los protocolos de aplicación de la señalización para el release 1 de la UNI y la NNI, la ITU-T especificó los requerimientos para los protocolos de señalización del release 2. Estas especificaciones se enfocan en la descripción de un modelo funcional para la señalización release 2 y en la descripción del intercambio de información de señalización entre los elementos funcionales sin este modelo.



B-ISUP	Parte de usuario B-ISDN	SIO	Octeto de información del servicio
MTP-3	Parte de transferencia de mensaje	TCAP	Parte de aplicación de capacidades de transacción
SCCP	Parte de control de conexión de la señalización		

Figura 2.42 Evolución del protocolo de señalización NNI de B-ISDN

Uno de los primeros resultados fue un convenio en donde estas especificaciones se basarían en la separación del control de llamada y control de portador/conexión. Usando esta aproximación sería posible tener llamadas con conexiones diversas (llamadas de multiconexión), lo cual es uno de los requerimientos más poderosos para la provisión de servicios multimedia. En resumen la separación entre los controles de llamada y portador/conexión permitirá:

- Establecimiento y liberación de una llamada sin ninguna conexión. Así una llamada será útil para la negociación de la compatibilidad de un servicio end-to-end anterior para recursos de reservación, y algunos servicios suplementarios
- Alojamiento/Desalojamiento dinámico de conexiones para una llamada de/para.

Esta estructura básica de separación de controles de llamada y portador/conexión permite que los protocolos de señalización release 1 sean reusados como protocolos de control de portador/conexión con solamente mínimos cambios.

2.5 Protocolos de enrutamiento de ATM

Los protocolos de interface entre nodos de red (NNI) son usados dentro de las redes ATM para enrutar requerimientos de señalización entre conmutadores ATM. Debido a que ATM está orientado a conexiones, un requerimiento de conexión necesita ser enrutado desde el nodo que esté haciendo el requerimiento a la red ATM hasta el nodo destino. Los protocolos NNI son para las redes ATM lo que son OSPF y RIP para las redes enrutadas con IP.

El Foro de ATM ha hecho un esfuerzo por definir un protocolo denominado Private NNI (P-NNI). La meta es definir los protocolos NNI para ser usados en las redes privadas ATM o más específicamente, en las redes que usen formato NSAP para direcciones ATM.

Las redes públicas que usan números E.164 para sus direcciones serán interconectadas usando diferentes protocolos NNI basados en los protocolos de señalización ITU-T, B-ISUP y el protocolo de enrutamiento ITU-T MTP Nivel 3. Este trabajo, ha sido desarrollado por Broadband Inter-Carrier (B-ICI), el Foro de ATM, y otros cuerpos de estándares internacionales.

El protocolo P-NNI consiste de dos componentes: El primero es un protocolo de señalización P-NNI usado para soportar los requerimientos de conexión dentro de las redes ATM, entre origen y destino UNI. El requerimiento de señalización UNI es mapeado dentro de la señalización NNI en el conmutador origen (ingreso). La señalización NNI es remapeada nuevamente dentro de la señalización UNI en el conmutador destino (salida).

Los protocolos P-NNI operan entre los sistemas de conmutación ATM (los cuales pueden representar conmutadores físicos o redes enteras operando como una sola entidad P-NNI), las cuales están conectadas por ligas P-NNI. Las ligas P-NNI pueden ser ligas físicas o virtuales (ligas "multi-hop"). Un ejemplo típico de una liga virtual es una dirección virtual que conecta dos nodos juntos. Todos los canales virtuales, incluyendo la conexión de envío de señales P-NNI, deben ser transportadas transparentemente a través de cualquier conmutador intermedio entre estos dos nodos de una ruta virtual, los dos nodos son lógicamente adyacentes en relación a los protocolos P-NNI.

El protocolo ILMI, está definido principalmente para usarse a través de ligas UNI, aunque puede ser usado a través de ligas físicas y virtuales NNI; mejoras a los MIBs ILMI permiten un reconocimiento automático de ligas NNI contra ligas UNI, y de UNI privadas contra UNI públicas.

El actual protocolo de señalización P-NNI empezó a desarrollarse en el Foro de ATM como una extensión de la señalización UNI al incorporar Elementos de Información (IE) adicionales como parámetros relacionados con NNI por ejemplo Listas de Tránsito Designadas (DTL). La señalización P-NNI es enviada a través de ligas NNI sobre el mismo canal virtual, VCI=5, el cual es usado para la señalización a través de la UNI. El valor VPI depende de si las ligas NNI son físicas o virtuales.

El segundo componente del protocolo P-NNI es un protocolo de enrutamiento de circuitos virtuales. Este es usado para enrutar los requerimientos de señalización a través de las redes ATM. Esta ruta es sobre la cual las conexiones ATM son levantadas, y eventualmente a través de donde viajarán los datos. La operación de un requerimiento de enrutamiento para señalización a través de una red ATM, paradójicamente, dada la naturaleza de orientación a conexión, es similar al enrutamiento de paquetes en una red no orientada a conexión como (IP).

El protocolo P-NNI es mucho más complejo que cualquier protocolo de enrutamiento existente. Esta complejidad surge debido a dos metas del protocolo: permitir que la escalabilidad sea mucho mayor de lo que es en cualquiera de los protocolos existentes, y para soportar el ruteo verdaderamente basado en QoS.

El estado actual de los protocolos P-NNI debe ser examinado de la misma forma como cualquier protocolo que tomó estas tendencias. Cabe resaltar, sin embargo, que el Foro de ATM no tiene fecha para completar el "P-NNI Fase 1", mientras tanto, el Foro de ATM ha definido el protocolo "P-NNI Fase 0".

El protocolo de señalización intermedio entre conmutadores (IISP) será analizado después del protocolo fase 1.

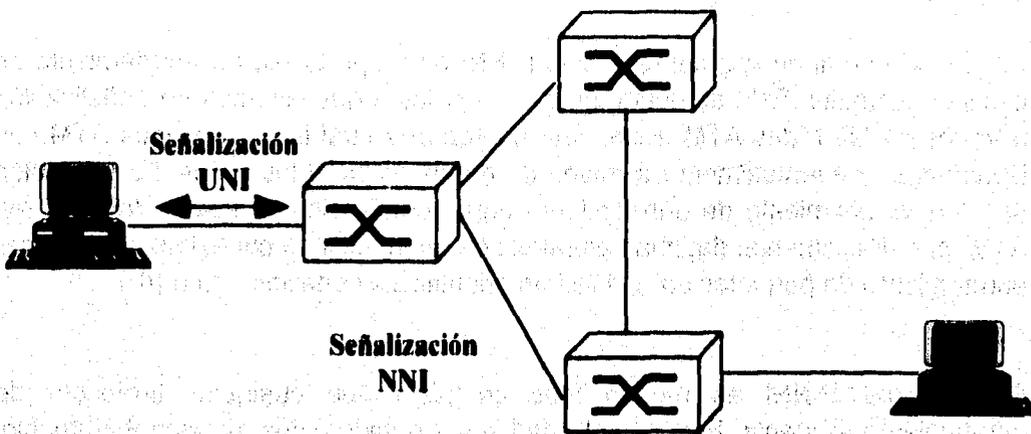


Figura 2.43

2.5.1 P-NNI Fase 1: QoS Support

Una de las ventajas más grandes de ATM es su soporte en la calidad de servicio (QoS). Para garantizarla, los conmutadores ATM implementaron una función conocida como Connection Admission Control (CAC). Un requerimiento de conexión es recibido por el conmutador, el conmutador realiza la función CAC. Esto es basado en los parámetros de tráfico y requerimientos de QoS de la conexión, el conmutador determina si la nueva conexión no afecta la calidad de servicio de las conexiones establecidas. El conmutador acepta la conexión sólo si no son reportadas violaciones. El CAC es una función de conmutador local y depende de la arquitectura del conmutador y de las decisiones locales que garanticen la QoS.

El protocolo de ruteo de las VC debe asegurar que un requerimiento de conexión sea enrutado hacia una ruta que permita su destino y que tenga una alta probabilidad de cumplir los requerimientos de la QoS en la conexión.

Para hacer esto, se usa un protocolo de enrutamiento de estado de la topología en el cual los nodos alimentan la información de la QoS y de las disponibilidades, así todos los nodos obtienen el conocimiento acerca de la disponibilidad dentro de la red y los recursos de tráfico existentes dentro de la red.

Control de admisión de conexiones

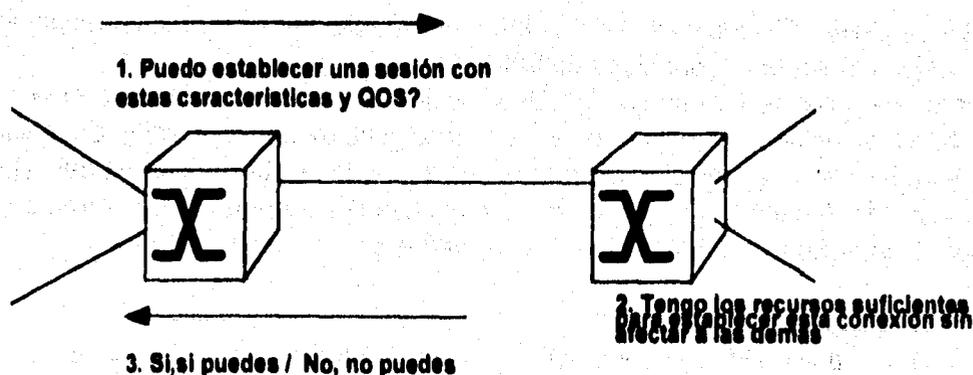


Figura 2.44

Esta información es difundida dentro de los paquetes de estado de la topología (PTSP).

Hay dos tipos de parámetros de liga: los atributos de las ligas no-aditivas son usados para determinar si una red o nodo puede cumplir un requerimiento de QoS; y una liga aditiva mide qué se está usando, para determinar si una ruta dada, que puede consistir de un conjunto de ligas y nodos concatenados, pueden cumplir los requerimientos de la QoS.

El conjunto actual de las métricas de enlace son:

- **Máximo retardo de transferencia de celdas (MCTD)** por clase de tráfico.
- **Máxima variación de retardo (MCDV)** por clase de tráfico.
- **Máxima razón de pérdida de celdas (MCLR)** para celdas CLP=0, para las clases de tráfico CBR y VBR.
- **Peso administrativo:** Esto es un conjunto de valores definidos por el administrador de la red y son usados para indicar la preferencia de una u otra forma de liga de red.

El conjunto actual de los atributos de liga son:

Valor de Celdas Disponibles (ACR): Una medición del ancho de banda disponible en celdas por segundo, por clase de tráfico.

Margen de valor de Celdas (CRM): Una medición de la diferencia entre el ancho de banda efectivo por clase de tráfico, y la localización del valor de celdas sustentable, es una medición del margen de seguridad localizado arriba del valor.

- **Factor de Variación (VF):** Una medición relativa del margen (CRM) normalizado por la variación de la suma del valor de celdas de las ligas.

Todos los nodos de la red pueden obtener un estimado del estado actual de la red entera a través de PSTP que contiene la información de la lista de arriba. Típicamente, el PTSP incluye información bidireccional acerca del tránsito de los nodos particulares basados en las entradas y salidas del puerto y el estado interno actual.

La necesidad de agregar elementos a la red y su información de métricas también tiene importantes consecuencias en la exactitud de la información. Hay dos características posibles para enrutar una conexión a través de la red: ruteo hop-by-hop y ruteo de origen.

El ruteo hop-by-hop es usado por muchos de los protocolos actuales de red como IP o IPX, donde un paquete es enrutado hacia un nodo dando un solo salto para otro nodo, el más cercano a un destino final. La fuente del ruteo, el nodo inicial y la ruta determinan el ruteo entero hacia el destino final.

El ruteo hop-by-hop es bueno para la conexión actual de protocolos porque ellos procesan pequeños paquetes por cada nodo intermedio. El protocolo P-NNI, sin embargo usa un ruteo de origen por varias razones. En primera instancia, es muy difícil que el ruteo basado en QoS se implemente con un protocolo hop-by-hop ya que cuando se realiza un CAC local se necesita evaluar la QoS a través de la red entera para determinar el siguiente brinco. El ruteo hop-by-hop también requiere una ruta estándar para la determinación de algoritmos de cada brinco para tratar de evitar el peligro de un loop.

Sin embargo, en un protocolo basado en ruteo de origen, sólo el primer nodo debe necesitar determinar una ruta a través de la red, basado en el requerimiento de QoS y en el conocimiento del estado de la red, el cual es dado desde el PTSP. Esto puede entonces insertar un enrutamiento de origen completo dentro de un requerimiento de señalización que debe enrutarse hasta un destino final. Idealmente, un nodo intermedio sólo necesita un CAC local antes del requerimiento. También, de esta forma es fácil predecir loops cuando calculamos una ruta de origen, una ruta particular determinada no necesita ser estandarizada, dejando esto en otra area para hacer la diferenciación.

Esta descripción es sólo ideal, sin embargo en la práctica, el ruteo de origen es determinado por un nodo, esto es porque en una red práctica, un solo nodo puede tener sólo una aproximación imperfecta para el estado real de la red.

El protocolo P-NNI toma estos problemas para definir un algoritmo CAC genérico (GCAC). Esta es una función estándar donde cualquier nodo puede ser usado para realizar el CAC esperado por otro nodo. El GCAC es un algoritmo que fue realizado para proveer una buena predicción de un nodo CAC, mientras requerimos un número mínimo de ligas de medición de estado. Los nodos individuales pueden controlar el grado de GCAC involucrado en un nodo particular para conservarse dentro de las métricas advertidas por el nodo.

El GCAC actualmente usa una métrica de adición descrita. Los nodos individuales (físico o lógico) deben ser determinados y avisados de los valores de estos parámetros, los cuales están basados en la estructura y carga interna. Sin embargo, en la fase 1 de P-NNI el algoritmo GCAC está principalmente diseñado para conexiones CBR y VBR; variantes del GCAC son usadas dependiendo del tipo de requerimiento de garantía de la QoS y del tipo de ligas métricas disponibles.

La única forma de hacer GCAC para conexiones UBR es para determinar si un nodo puede soportar estas conexiones. Para conexiones ABR, una validación es realizada para determinar si la liga o nodo está autorizada para conducir y adicionar conexiones ABR y asegurarse de que para el tráfico el nodo tenga un número mayor que el Valor de Celdas Mínimas especificadas por la conexión.

Usando el GCAC, un nodo presentado con un requerimiento de conexión procesa los requerimientos como se muestra a continuación:

1. Todas las ligas no pueden proveer el requerimiento de ACR, y si éstos exceden los CLR de los requerimientos de conexión, son eliminadas a un conjunto de posibles rutas usando el GCAC.
2. Desde este conjunto reducido, sólo con la información para determinar un conjunto de una o más rutas posibles para el destino.
3. Estas posibles rutas son disminuidas usando la adición de líneas métricas, como retraso, y las posibles restricciones. Una de las rutas aceptables deben ser seleccionadas. Si una ruta múltiple es seleccionada, el nodo puede opcionalmente realizar una tarea de carga balanceada.
4. Cuando una ruta es encontrada (nota que esto significa sólo una ruta "aceptable" para el destino, pero no la "mejor" ruta, el protocolo puede ser que no trabaje de la manera óptima), el nodo construye una lista de tránsito designada (DTL) que describe la ruta completa para el destino e inserta este dentro de un requerimiento de señales. El requerimiento es entonces enviado a esa ruta.

Cada nodo dentro de la ruta debe realizar su propio CAC en un requerimiento de enrutamiento porque éste puede cambiar el estado dentro del PTSP. El algoritmo CAC es también usado para asegurar el GCAC.

El protocolo P-NNI también soporta el concepto de "Crankback". "Crankback" es cuando una conexión es bloqueada sólo para una ruta seleccionada y el requerimiento es regresado a un nodo intermedio, anterior en la ruta. Este nodo intermedio se utiliza para descubrir otra ruta para el destino final, usando el mismo procedimiento como un nodo original, pero usa uno más nuevo. Este es otro mecanismo que puede ser fácilmente soportado en un protocolo de origen más que en un protocolo hop-by-hop.

Operaciones del Crankback

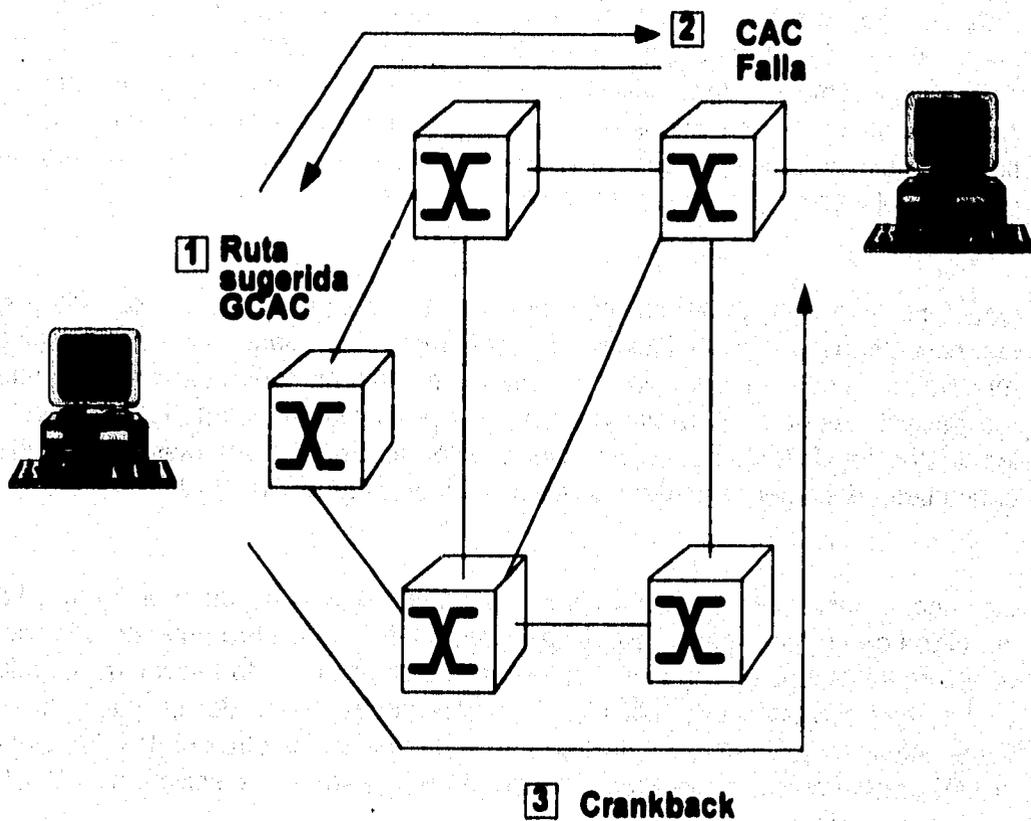


Figura 2.45

2.5.2 P-NNI Fase 1: Escalabilidad y alcance

El protocolo P-NNI Fase 1 se diseñó para ser capaz de aplicarse en redes pequeñas con pocos conmutadores y para un posible futuro global de millones de conmutadores. La llave para hacer el protocolo escalable es la organización jerárquica de la red, con información sumariada al alcance entre los niveles de jerarquía. El protocolo P-NNI, sin embargo, usa el direccionamiento NSAP de 20 Bytes para indentificar niveles dentro de la red jerárquica y soportar un número limitado de niveles: un máximo de 105.

Para soportar esta jerarquía, el modelo P-NNI define un modelo de red uniforme para cada nivel de la jerarquía. El modelo jerárquico P-NNI explica como opera cada nivel, como múltiples dispositivos o nodos de un nivel que pueden ser sumariados dentro de un alto nivel, ya que la información se cambia entre niveles. Este modelo es recursivo y es el mismo mecanismo es usado para un primer nivel y para los niveles siguientes.

Cada nivel en la jerarquía consiste de un conjunto de nodos lógicos, interconectados por ligas lógicas. El nivel más bajo, para cada nodo lógico representa un conmutador físico consistiendo de sólo un conmutador físico o una red de switches para operar internamente un protocolo propietario NNI y soporta los protocolos P-NNI para conectividad externa. En el nivel más bajo, cada conmutador debe ser asignado a una dirección única del ATM NSAP.

Los nodos dados dentro de un nivel son grupos dentro de un "peer grup". La definición de un "peer group" es: Una colección de nodos para obtener todas las bases de datos topológicamente idénticas e intercambiar la información del estado de las ligas con otro nodo. Mientras todos los nodos dentro de un "peer group" tienen información completa del estado en cada uno de los otros nodos, los "peer group" no pueden ser extendidos por todo el ancho para un excesivo tráfico PTSP y procesamiento.

Normalmente, los "peer group" son identificados por prefijos de direccionamientos ATM privados. El nivel más bajo, donde los sistemas de conmutadores consisten de conmutadores actuales, y donde por default, todos los sistemas conectados para conmutador obtienen su prefijo de direccionamiento de red.

Los nodos dentro de un "peer group" son identificados por un nodo de 22-byte. El nivel más bajo es esencialmente el mismo direccionamiento de conmutadores ATM. El nivel más alto del nodo incluye dos niveles indicadores para los niveles jerárquico de ambos "peer group" asociados.

Cada "peer group" selecciona un solo nodo dentro del grupo para realizar las funciones de un nodo de grupo lógico. Este nodo, conocido como un "peer group leader (PGL)", es seleccionado a través de un mecanismo de elección y está basado en la prioridad del líder en nodo de conmutadores. Cada PGL es identificado por una direccionamiento único de ATM, si un nodo actúa como un PGL dentro de múltiples niveles de "peer groups", entonces éste puede tener un direccionamiento único ATM para cada uno de estos niveles.

Los PGL dentro de cada "peer group" tiene la responsabilidad de formular y cambiar PTSP con sus nodos dentro del grupo para informar estos nodos. Así como sucede con la información recursiva obtenida por el PGL acerca del grupo.

Un crankback trabaja dentro del mismo mecanismo, para hacer una descripción previa más precisa, las conexiones pueden ser sólo regresadas para nodos que actualmente han creado e insertado DTLs dentro del requerimiento, el nodo fuente original, mantiene el estado de información acerca de todos los requerimientos que ellos tengan hasta que la conexión sea confirmada o una conexión sea recibida en el destino final.

El protocolo P-NNI permite un "peer group" para ser modelado a un alto nivel, para propósitos de advertencia, no es sólo un nodo pero es un "nodo complejo", dentro de una estructura interna. El protocolo P-NNI en su Fase 1 permite nodos complejos para ser modelados como una estrella de nodos que consiste de un "pseudonodo" conectado a un grupo de nodos de bordes a través de una "pseudoliga", cada una con radios idénticos por cada parámetro de liga. Estos nodos no necesariamente corresponden a nodos físicos actuales.

El modelo jerárquico de PNNI

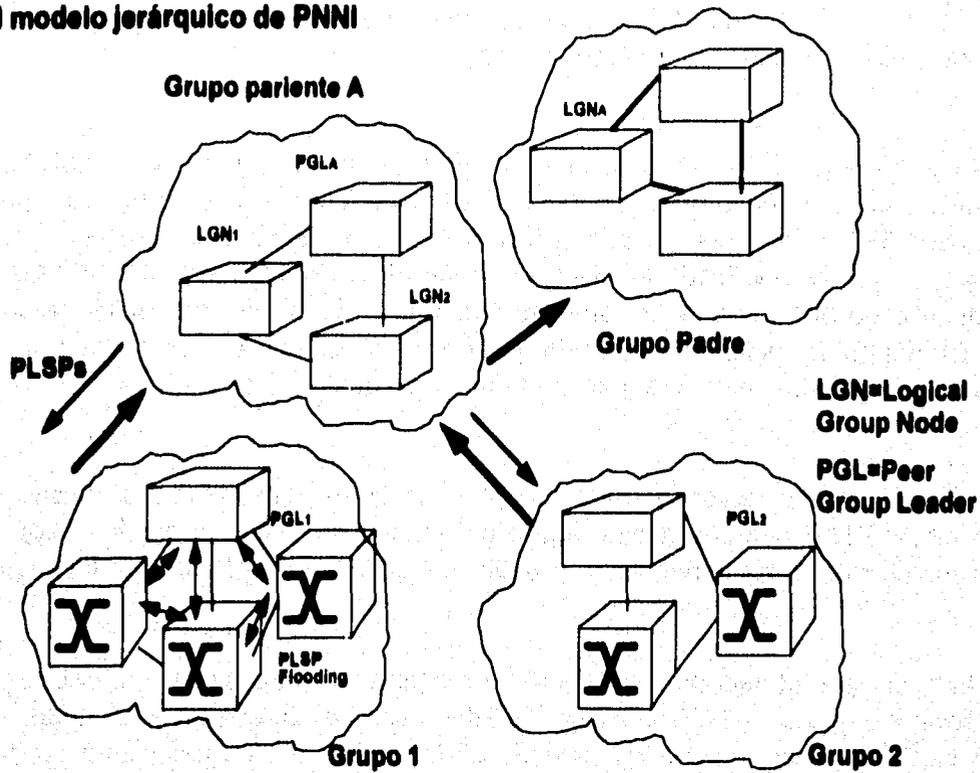


Figura 2.46

2.6 Emulación LAN

Dada la vasta base instalada de LANs y WANs hoy en día, es fundamental permitir la interoperabilidad entre estas tecnologías y ATM. Pocos usuarios aceptarán la presencia de ATM sin conectividad a las redes actuales. La llave para esta conectividad radica en usar las mismas capas de protocolos de red, como IP o IPX, tanto en redes ya existentes como en ATM, para proveer una vista de red uniforme en los niveles altos de los protocolos y las aplicaciones.

Hay dos métodos fundamentales para que una red funcione a través de ATM. En uno de los métodos, conocido como modo nativo, los mecanismos de resolución de direcciones son usados para mapear las direcciones de las capas de red y las direcciones ATM. Un método alternativo de envío de paquetes a través de una red ATM es conocido como emulación de LAN.

Como su nombre sugiere, la función del protocolo LANE (Emulación de LAN) es la de emular una red de área local sobre una red ATM. Específicamente, el protocolo LANE define el mecanismo para emular una red IEEE 802.3/Ethernet o una red 802.5/Token Ring.

La emulación de LAN significa que el protocolo LANE define un servicio de interface en las capas altas (red, transporte, etc), la cual es idéntica a una LAN ya existente y los datos son enviados a través de la red ATM encapsulados en un paquete de formato LAN MAC. Esto no significa que cualquier cosa va a ser realizada para emular el acceso actual de un protocolo concerniente a LAN.

En otras palabras, el protocolo LANE hace que una red ATM se vea como una red Ethernet o Token Ring, pero con una operación mucho más rápida que una red real. La justificación para esto se basa en que no se requieren demasiadas modificaciones en las capas más altas de los protocolos para permitir su operación sobre una red ATM. El servicio LANE presenta el mismo servicio de interface que un protocolo MAC existente para los manejadores de las capas de la red, debido a esto no se requieren hacer cambios en los manejadores. La intención es acelerar el desarrollo de ATM.

El protocolo LANE está situado dentro de dos tipos de equipo:

a) **ATM Network Interface Cards (NIC):** Las NICs ATM deberán implementar el protocolo LANE y además ser la interface de conexión a la red ATM, pero presentarán los servicios de interface LAN para los manejadores de protocolos de alto nivel dentro de los sistemas finales. Los protocolos de red en los sistemas finales deben continuar comunicándose como si estuvieran en una LAN, usando los mismos procedimientos conocidos. Sin embargo, son capaces de usar un ancho de banda mayor.

b) **Internetworking and LAN Switching Equipment:** La segunda clase de redes que se implementan en LANE serán los conmutadores de LAN con conexión ATM. Estos dispositivos, junto con los equipos conectados directamente a ATM, deben ser usados para proveer el servicio de LAN virtual, donde los puertos de los conmutadores LAN pueden ser asignados a diferentes LANes virtuales, independientemente de la localización física. La emulación LAN se adapta bien particularmente a la primera generación de conmutadores LAN que actúan efectivamente como puentes multipuertos rápidos, LANE es esencialmente un protocolo para hacer puenteo a través de ATM. Los equipos de redes, como los enrutadores deberán implementar LANE para permitir su interconexión a LAN virtual.

Debe notarse que el protocolo LANE no impacta directamente a los conmutadores ATM. LANE, como muchos otros de los protocolos ATM, construye un modelo de capas superiores y opera transparentemente a través de los conmutadores ATM, usando sólo los procedimientos de señalización estándares de ATM. Los conmutadores ATM deberán ser usados en plataformas que tengan implementados algunos de los componentes de LANE server.

La función básica del protocolo LANE es para resolver direccionamientos MAC dentro de direccionamientos ATM, por lo que se implementa un protocolo para puentear MAC sobre ATM. La meta de LANE es realizar direccionamiento de mapeo para sistemas finales que puedan establecer conexiones directas entre ellos mismos y los datos.

2.6.1 Tipos de conexión y componentes LANE

El protocolo LANE define la operación de una LAN emulada. Múltiples ELANs pueden coexistir simultáneamente en una red ATM. Una emulación de ELA ya sea Ethernet o Token Ring, consiste de las siguientes entidades:

- **LAN Emulation Client (LEC):** Un LEC es una entidad en un sistema final que realiza envíos de datos, resolución de direcciones y otras funciones de control para sólo un sistema final dentro una ELAN. Un LEC también provee un servicio de interface estándar para cualquier entidad en una capa de nivel superior que interactúe con los LEC.
- **LAN Emulation Server (LES):** El LES implementa las funciones de control para una ELAN en particular. Hay una sola LES lógica por ELAN, y el pertenecer a una ELAN particular significa tener un control de las relaciones con las ELAs particulares. Cada LES es identificado por una dirección única ATM.
- **Broadcast and Unknown Server (BUS):** El BUS es un servidor de multicast que es usado para alimentar el tráfico de direcciones destino desconocidas y difundir el tráfico Broadcast y Multicast. Cada LEC está asociado con un solo BUS por ELAN, pero pueden existir múltiples BUS dentro de una ELAN particular.
- **LAN Emulation Configuration Server (LECS):** Los LECS son una entidad que asigna clientes LAN individuales a ELANs particulares direccionando cada LES que corresponda a una ELAN. Hay lógicamente un LECs por cada dominio administrativo, y éste sirve a todas la ELANs dentro de este dominio.

El protocolo LANE especifica la operación de la emulación de LAN de la Interface de usuario a la red (LUNI) entre un LEC y la red que provee los servicios LANE. Esto puede contrastar con el "LAN Emulation NNI" (LNNI), el cual opera entre los componentes del server dentro de un sistema ELAN. La Fase 1 LANE especifica sólo la operación LUNI, sin embargo, la fase 1 LANE no permite el soporte estándar de múltiples LESs o BUSs dentro de una ELAN. Estos componentes representan los potenciales puntos de falla. La interacción entre cada uno de los componentes del server dentro de la Fase 1 LANE actualmente no están especificados, y deben ser implementados dentro de una manera propietaria para cada elemento.

Las entidades de la Fase 1 LANE se comunican entre ellas usando una serie de conexiones ATM, donde LECS mantiene separadas las conexiones para la transmisión de datos y el control del tráfico.

El control de las conexiones se realiza de la siguiente forma:

- Configuración Directa VCC: Esta es un VCC bidireccional punto a punto que se establece por el LEC con otro LEC.
- Control Directo VCC: Este es un VCC bidireccional que se establece de LEC hacia los LES.
- Control de Distribución VCC: Este es un VCC unidireccional establecido desde el LES anterior hacia el LEC, éste es típicamente una conexión punto a multipunto.

La conexión de datos es de la siguiente forma:

Data Direct VCC: Este es VCC bidireccional punto a punto establecido entre dos LECs que quieren intercambiar datos. Dos LECs típicamente usan el mismo VCC de datos directos para transportar todos los paquetes entre ellos, en lugar de abrir un nuevo VCC para cada par de direccionamiento MAC.

Multicast Send VCC: Este es un VCC bidireccional punto a punto establecido por el LEC hacia el BUS.

Multicast Forward VCC: Este es un VCC unidireccional establecido hacia el LEC desde el BUS, éste es típicamente una conexión punto a multipunto.

2.6.2 LANE Operación

Las operaciones de LANE comprenden diferentes etapas que se describen a continuación:

Inicialización y Configuración

Para realizar la inicialización, el LEC debe primero obtener su propia dirección ATM, el LEC levanta una conexión directa hacia el LECs, para hacerlo, el LEC debe encontrar primero la localización de los LECs para ya sea que use el procedimiento ILMI para determinar la dirección LECs, utilice una dirección de LECs bien conocida, o que use una conexión permanente bien conocida hacia los LECs.

Después de encontrar la localidad de los LECs, el LEC debe establecer un VCC de configuración directa a los LECs. Una vez conectados, un protocolo de configuración es usado por los LECs para informar al LEC de los parámetros que son requeridos para conectarse a la ELAN. Esto incluye la dirección ATM de los LES, el tipo de LAN que se emulará, el tamaño del paquete máximo de la ELAN y el nombre ELAN. El LECs está generalmente configurado por el administrador de red con esta información, la que indica efectivamente a cual LAN virtual pertenece el LEC.

2.6.3 Unión y Registro

Una vez que el LEC obtiene la dirección LES, puede opcionalmente limpiar el VCC de configuración directa con los LECs, entonces establece un VCC de control directo al LES. Una vez hecho esto, el LES asigna al LEC un identificador de LEC único (LECID). El LEC entonces registra sus direcciones ATM y MAC con el LES. Este opcionalmente también pudiera registrar cualquier otra dirección MAC.

Una razón típica por la que el LES no conoce un mapeo es porque la dirección está atrás de un puente MAC, y el puente puede no tener registrada la dirección. Un ATM NIC, debe presumiblemente no sólo soportar una sino un pequeño número de direcciones MAC las cuales pueden fácilmente ser registradas. Típicamente, una dirección MAC no conocida por el LES puede ser encontrada sólo en un LEC dentro de un puente, y no dentro de un NIC, y sólo el LECs para estos dispositivos necesita necesariamente recibir un LE-ARPs redireccionado.

Para completar la inicialización, un LEC usa el mecanismo de LE_ARP para determinar las direcciones ATM del BUS. Esto lo hace enviar un LE_ARP a la dirección MAC broadcast para el LES, el cual responde con la dirección del BUSs ATM. El LEC entonces levanta un VCC multicast de envío para el BUS. El BUS en turno, establece un VCC de regreso al LEC, típicamente agregando el LEC en una conexión punto a multipunto. El LEC está ahora listo para la transferencia de datos.

2.6.4 Transferencia de Datos

Durante la transferencia de datos, un LEC recibe un paquete de la capa superior del protocolo para ser transmitido o recibe un paquete MAC para difundirlo a través de los puertos LAN. En esta primera instancia, el LEC fuente no tiene la dirección ATM para el LEC destino a través del cual el destino particular puede ser alcanzado. En este caso, el LEC primero formula y envía hacia el LES una respuesta LE_ARP.

Mientras espera una respuesta del LE_ARP, el LEC también envía el paquete hacia el BUS, usando una encapsulación definida. El BUS, envía el paquete hacia los LECs. Esto se hace porque, en el caso de un dispositivo pasivo que esté atrás del conmutador LAN, el LEC quizá no conoce donde se encuentra la dirección MAC. De este modo, el BUS provee un procedimiento análogo de inundación usado por los puentes "spanning tree" para paquetes con destino desconocido.

Si una respuesta del LE_ARP es recibida, el LEC entonces establece un VCC directo de datos al nodo destino, y lo usa para la transferencia de datos en lugar de la ruta de BUS. Este mecanismo, es la forma garantizada de cumplir con los estándares de LAN actuales que requieren de puentes de LAN para reservar un orden estricto de frames, las celdas de control son enviadas hacia la primera ruta de transmisión, siguiendo el último paquete.

Si no es recibida una respuesta del LE_ARP, el LEC debe continuar enviando paquetes hacia el BUS, pero regularmente debe re-enviar LE_ARPs hasta que una respuesta sea recibida. Típicamente un solo paquete es enviado a través del BUS, y la respuesta destino hacia la fuente, algunos LEC deben conocer la localización del destino, y entonces enviar la respuesta hacia el subsecuente LE_ARP.

2.6.5 BUS Inteligente

Un BUS es aquél que obtiene conocimiento de las localizaciones de las direcciones de MAC a través de algún medio, para este caso, el BUS quizá no inunde con paquetes de destino desconocido, pero puede direccionarlos directamente al LEC a través del VCC de multicast de envío.

De este modo, un BUS inteligente efectivamente opera como un servidor de conexión, desde un punto de vista extremo, éste necesita un VCC de datos directos para cada uno, y si un LEC mínimo puede enviar todos los paquetes hacia el BUS y evitar la necesidad de soportar uno o más de los complejos elementos del protocolo LANE. Este no sería un modo deseable de operar, sin embargo, como el BUS, pueden ser rápidamente saturados. Un LEC mínimo usado dentro de un BUS normal puede también inundar rápidamente la red con paquetes, para evitar estos problemas, el protocolo LANE, permite que el BUS inteligente establezca los VCC de datos directos que pueda y restringe de esta forma el número de paquetes que van a ser enviados al BUS en un período dado.

2.6.6 LANE y Redes Virtuales

LANE es usado para proveer un servicio de LAN virtual sobre "backbones" ATM. Las LANES virtuales son implementadas sobre redes conmutadas que consisten de una combinación de conmutadores LAN. Los sistemas finales ATM y los enrutadores con interfaces ATM todos conectados hacia un ELAN. Las ELAN miran igual a una LAN normal con excepción del ancho de banda que es más rápido.

En particular, a través de la administración de red y el uso de mecanismos como el de los LECS, el administrador de la red puede configurar múltiples ELANs a través de un solo "backbone" ATM y asignar puerto al conmutador LAN o al host ATM para diferentes ELANs, independientemente de la localización física de los dispositivos.

Esto implica inmediatamente la necesidad de dar un significado de interconexión de todos hacia los ELANs, y las redes LAN y WAN existentes. La forma más fácil y común en la cual se hace esto es a través de enrutadores ATM. Muchos de los enrutadores convencionales conectan LANES y los enrutadores ATM interconectan LANs virtuales, ellos soportan el alto performance nativo de las interfaces ATM implementados en LANE para soportar múltiples enrutadores LEC en una sola interface ATM nativa, cada uno con una conexión ELAN.

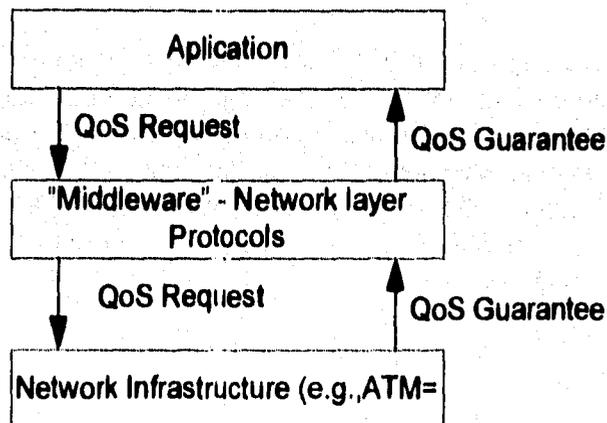
2.7 Protocolos de modo nativo

Esta sección discute la manera alterna de llevar protocolos de red a través de un backbone ATM, pero no a través de LANE, con protocolos en modo nativo. Mientras todos los protocolos actuales de red pueden ser mejorados para correr directamente a través de una red ATM, actualmente, los únicos protocolos que se han hecho son IP e IPX. Novell ha publicado un protocolo conocido como Connection Oriented IPX (CO-IPX), el cual tiene un adaptador IPX específicamente para redes ATM, y agrega el soporte de QoS, pero el desarrollo total de este protocolo no se espera en corto plazo.

2.7.1 Servicios Integrados

La principal razón de utilizar protocolos de modo nativo, es opuesta a utilizar LANE ya que en este momento no se contempla en los protocolos de red el uso que puede garantizar la QoS. Consecuentemente, no existen protocolos de red que puedan requerir una QoS específica en la red.

Por otra parte, la proliferación de redes ATM, se basará en el uso de los beneficios de la QoS, un trabajo considerable se ha hecho para construir una infraestructura de red capaz de soportar nuevas clases de aplicaciones multimedia que combinen voz, video, imágenes y tráfico de datos. Para soportar estas aplicaciones, la garantía de la QoS es requisito de la red.



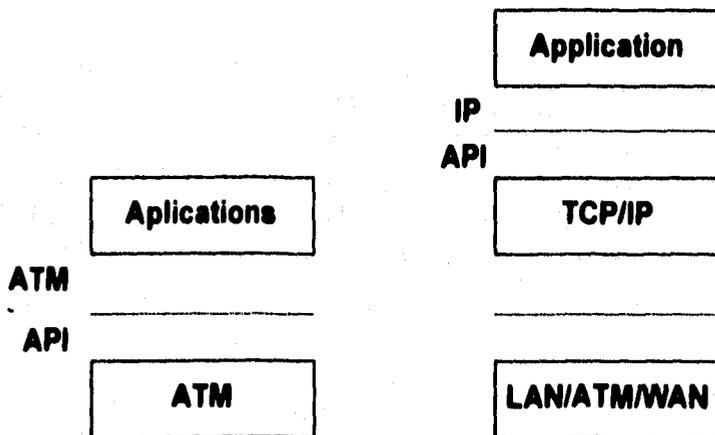
Aplicación QoS Support through the Network Layer

Figura 2.47

Una forma en la cual estas aplicaciones pueden ser construidas es ejecutando las aplicaciones o los protocolos directamente a través de ATM, o sobre una capa mínima de red. Esta es la aproximación propuesta con un protocolo como TCP y UDP, Lightweight TCP (TULIP) o UDP sobre IP no existente (TUNIP). El Foro ATM está trabajando también en el desarrollo de modelos para un API de acceso directo a ATM dentro de sistemas operativos.

Análisis e implementaciones recientes muestran que los diseños corregidos y optimizados de estos protocolos pueden operar redes de altas velocidades, pero algunas veces se olvida que una de las principales funciones de un protocolo de red es ofrecer conectividad universal, y una interface de servicios uniforme, para los niveles superiores, en particular para la capa de transporte, independiente de la naturaleza de una red física. Correspondientemente, la función de la capa de transporte es proveer el servicio de control de sesión para aplicaciones, esto se constituye sin considerar un tipo de red en particular. A menos que las aplicaciones corran sobre una red común y un protocolo de transporte, la interoperabilidad entre dos aplicaciones corriendo de dos diferentes tipos de red puede ser difícil si no es que imposible (como ejemplo una red ATM y una red convencional).

En el caso específico de un IP, el IETF ha desarrollado la noción de un Integrated Services Internet. Este conjunto de condiciones para IP permite soportar servicios integrados o multimedia. Estas mejoras incluyen mecanismos de manejo de tráfico que son parecidos a los mecanismos de manejo de tráfico ATM. Por ejemplo, los protocolos como el Resource Reservation Protocol (RSVP) están empezando a definirse para permitir la reservación de recursos a través de una red IP, parecida al concepto de señalización ATM.



Native and Conventional Applications

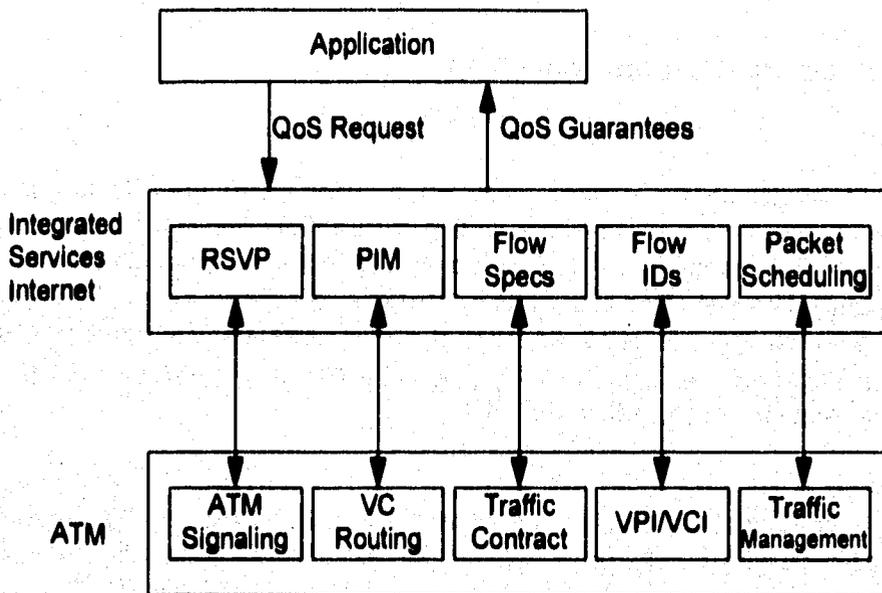
Figura 2.48

RSVP es un protocolo de control, parecido a ICMP, que será usado para aplicaciones dentro de IP en sistemas finales para indicar los nodos que están transmitiendo hacia ellos (la naturaleza de las cadenas de paquetes que les gustaría recibir). Los sistemas intermedios, sólo con la ruta de origen al destino deberán interpretar los paquetes de control RSVP para realizar controles de admisión (análogos con el CAC de ATM) y reservar los recursos requeridos para el soporte de requerimiento de flujo de tráfico.

RSVP está fundamentado sobre un paradigma multicast, y sólo con los flujos de las rutas de tráfico las fuentes pueden determinar las rutas point-to-multipoint. Los nuevos protocolos multicast como Protocol Independent Multicast (PIM) y sus paquetes unicast asociados, estarán acoplados con RSVP tanto como los protocolos de ruteo VC y adaptados a la señalización UNI y NNI.

La versión 6 del protocolo IP, la cual la IETF está ahora desarrollando el reemplazo de la versión actual Ipv4, incorpora soporte para un flujo ID dentro del encabezado del paquete, el cual puede ser usado para identificar el flujo, como los VPI/VCI son usados para identificar los flujos de celdas ATM. Así como Ipv6 debe ser incorporado con un soporte total para servicios integrados a través del uso de mecanismos y de la definición de protocolos como RSVP. El soporte quizá deba ser extendido hacia el actual protocolo Ipv4 y otros componentes de protocolo de los Integrated Service Internet, deben ser totalmente estandarizados para finales de 1995 y sus componentes pueden ser liberados antes.

IETF está también en proceso de desarrollo de un nuevo protocolo de transporte, el Real-Time Transport Protocol (RTP). RTP está diseñado para proveer funciones de transporte para transmisión de aplicaciones en tiempo real, como son audio, video o simulación de datos, sobre multicast o servicios de red unicast, y construir sobre protocolos como RSVP para reservación de recursos y sobre tecnologías de transporte como ATM para garantizar QoS. Estos servicios proveer un RTP para aplicaciones tiempo real incluyendo pagos, tipos de identificación, número de secuencia y monitoreo.



Mapping of the Integrated Services Internet into ATM

Figura 2.49

2.7.2 IP sobre ATM

Para prepararse en esta necesidad, el grupo de trabajo de IP-sobre-ATM del IETF ha desarrollado un protocolo para el transporte de IP sobre ATM. El transporte de cualquier protocolo de red sobre una red ATM, involucra dos aspectos: encapsulamiento de paquetes y resolución de direcciones. Ambos han sido considerados por IETF.

2.7.2.1 Encapsulamiento de Paquetes

El IETF trabaja primero en la definición de métodos de transporte de múltiples tipos para redes o liga de paquetes a través de una conexión ATM y también para múltiples tipos de paquetes en la misma conexión. Como en una LANE, hay valores para el reuso de una misma conexión para la transferencia de datos entre dos nodos, esto conserva el espacio de recursos de conexión, y salva una conexión después de levantada la primera conexión. Esto es sólo posible si es utilizada una conexión UBR o ABR.

2.7.2.2 Resolución de Direcciones

La tabla de resolución de direcciones puede ser construida manualmente pero ésta no es una solución muy escalable. El grupo de trabajo de IP-sobre-ATM ha definido un protocolo para soportar una resolución automática de direcciones en el estándar 1577. Este protocolo se conoce como "IP clásico sobre ATM".

2.8 Control del congestionamiento

2.8.1 Definición

El congestionamiento se define como la condición que se presenta cuando la demanda de recursos, excede a los recursos disponibles durante un cierto intervalo de tiempo. Se puede tomar como ejemplo un embotellamiento de tráfico. El congestionamiento ocurre, porque el número de vehículos que desean usar la carretera (demanda) es mayor que el número de vehículos que pueden usarla (recursos disponibles) durante una hora pico (intervalo de tiempo).

Se define el congestionamiento específicamente para ATM, como la condición que se da cuando la carga ofrecida (demanda) del usuario a la red se aproxima o excede los límites de diseño de la red, que garantizan la Calidad de Servicio (QoS) especificado en el contrato de tráfico. Esta demanda puede exceder los recursos límites de diseño, porque éstos exceden las especificaciones o por fallas en la red.

En redes de ATM, los recursos pueden llegar a congestionarse incluyendo; conmutadores, puertos, buffers, cadenas de transmisión, adaptación de los procesos de las capas de ATM (AAL), procesos de control y admisión de conexiones (CAC). Cuando la demanda excede la capacidad, se conoce como cuello de botella o punto de congestionamiento.

2.8.2 Determinación del impacto del congestionamiento.

Un número de características de aplicación, determinan el impacto de congestionamiento, como son: Formas de conexión, políticas de retransmisión, políticas de asesorías y flujo de control, junto con las características de aplicación de la red, son también responsables del congestionamiento; estrategias de espera, políticas de programas de servicio, estrategias de eliminación, rutas de selección, retraso en la propagación, retraso en el proceso y formas de conexión.

El congestionamiento puede también ocurrir en diferentes niveles, puede ocurrir a tiempo en el nivel de la celda, el nivel de explosión o el nivel de llamada. El congestionamiento puede ocurrir en el espacio entre un recurso sencillo o múltiples recursos. La detección de congestionamiento se conoce como una instrucción, retroalimentación o notificación.

La reacción al congestionamiento puede ocurrir en el mismo tiempo y espacio. La reacción en tiempo, puede ser básicamente celda por celda, irrumpir bruscamente o al nivel de llamada. En espacio la reacción puede ser en un nodo simple en la fuente, en el receptor o en múltiples nodos.

La definición de un problema de control de congestiónamiento, se dificulta por un gran número de combinaciones de características de aplicación, características de la red, detección de niveles de congestiónamiento y reacción. Un esquema de control de congestiónamiento que trabaja bien para ciertas aplicaciones y características de una red en un cierto nivel, puede tener un desempeño pobre para diferentes características y/o a diferente nivel. El control del congestiónamiento en redes de bandas anchas ha sido tema de investigación intensa y muchas publicaciones.

2.8.2 Control del comportamiento del congestiónamiento

Hay dos medidas básicas que deben ser consideradas en el estudio del congestiónamiento *throughput util* y *retraso efectivo*. Se define como *throughput útil* el *throughput* que se realiza al final de la aplicación. Por ejemplo en la transferencia de un archivo si un paquete se pierde, ese paquete y los paquetes enviados posteriormente deben ser retransmitidos. Aunque la red ATM transfirió al principio algunas de las celdas correspondientes al paquete perdido (y posiblemente algunos posteriores), éstas no son de utilidad hasta que todas las células sean retransmitidas. De igual manera el *retraso efectivo* no es el retraso requerido para enviar por primera vez sin éxito el archivo, pero sí el intervalo desde la primera transmisión hasta la recepción final exitosa en el lugar de destino. El *throughput util* y el *retraso efectivo* pueden ser idénticos para algunas aplicaciones fundamentales de la red ATM. Por ejemplo, voz o vídeo codificados para operar satisfactoriamente en niveles de pérdida no son transmitidos por lo tanto el *throughput disponible* y el *retraso efectivo* son los mismos como en las capas de ATM. Prácticamente sólo pérdidas o retrasos arriba de un valor crítico son aceptables; entonces el comportamiento de la aplicación, la percepción subjetiva de la imagen o reproducción de audio llegan a ser inaceptables.

Estos dos ejemplos de aplicaciones susceptibles de perderse, serán usados durante el resto de este capítulo para ilustrar lo relativo al comportamiento de varios esquemas de control del congestiónamiento. Cuando se da el congestiónamiento puede también ocurrir un fenómeno crítico llamado *congestiónamiento colapsado*, como se ilustra en la figura 2.50. La oferta de carga se incrementa dentro de los límites de la región de congestiónamiento, la carga actual limitada por el ancho de banda y recursos del buffer se van arriba de los valores máximos. Como la oferta de carga se incrementa incluso dentro de la zona de congestión severa, la carga transmitida puede reducirse debido a la aplicación de retransmisión ordenada por el usuario, originada por pérdidas o retraso efectivo. El grado en que la carga transmitida disminuye en la zona de congestiónamiento severo se conoce como *fenómeno de congestiónamiento*

colapsado. El colapso está determinado por la aplicación y las características de la red.

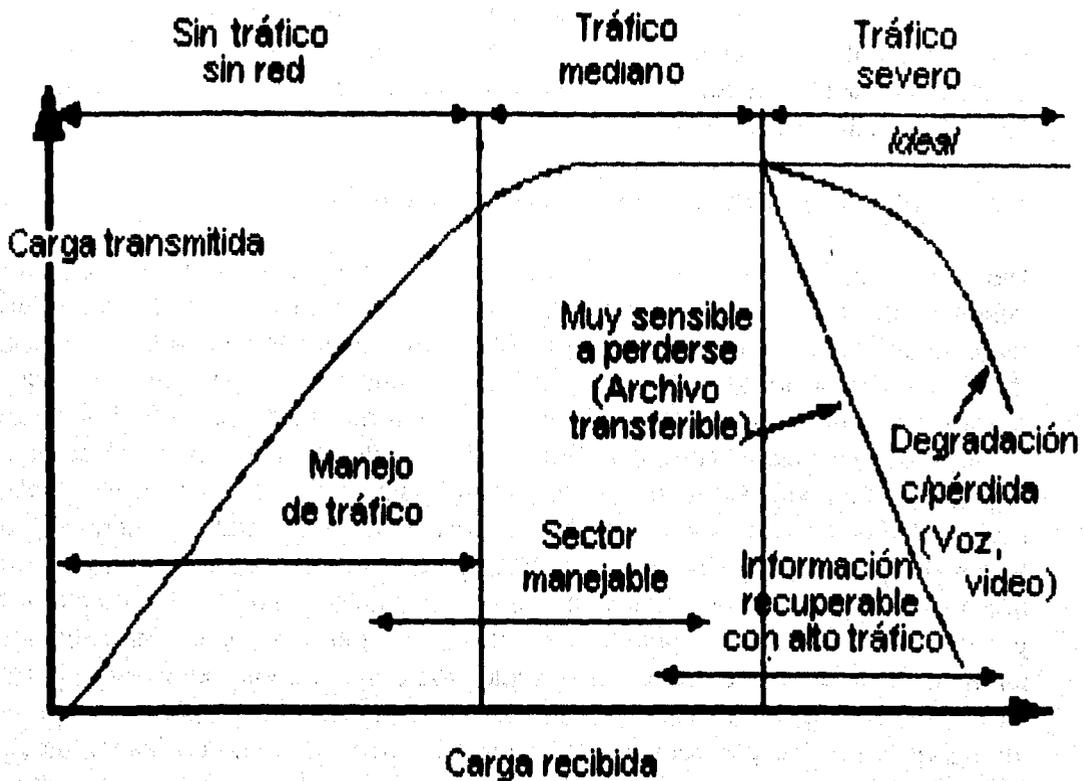


Figura 2.50 Ilustración de las zonas de Congestionamiento y Colapso.

La simple transferencia de un archivo es susceptible de sufrir un *congestionamiento colapsado* de esta manera vemos que el *throughput* disponible se precipita bruscamente en una pendiente al alcanzar un congestionamiento severo, porque la retransmisión improductiva en turno, incrementa la oferta de carga en proceso de realización empeorando el congestionamiento. El otro ejemplo (de codificación de voz o video) es fuerte para perderse y extiende su caída hasta la oferta de carga es algunas fracciones más grande que el recurso cuello de botella; en otras palabras es una pérdida limitada. Un esquema ideal de control del congestionamiento, es el que no tiene congestionamiento colapsado y los incrementos de carga manejada incrementan la disponibilidad de capacidad de recursos del cuello de botella, y permanecen constantes.

En el área de congestiónamiento severo, la degradación principal del QoS puede también ocurrir si se incrementa el retraso o la pérdida. La efectividad particular de un esquema de control del congestiónamiento puede también ser medida considerando qué tantos retrasos o pérdidas ocurren bajo la situación de una oferta de carga que exceda los límites de diseño, como se ilustra en la figura 2.51. Una aplicación de carga muy susceptible tiene retrasos y pérdidas que incrementan la ocurrencia de congestiónamientos severos. Una aplicación de pérdida limitada puede lograr que se mantenga un comportamiento aceptable hasta el threshold entre el congestiónamiento medio y severo se alcancen. La aplicación ideal de congestiónamiento controlada ha pasado de retrasos y pérdidas a valores de oferta de carga. Otras aplicaciones pueden tener pérdidas y retrasos que son menos sensibles a cargarse. La figura 2.51 ilustra la relación de retrasos y pérdidas contra carga. En general las curvas pueden verse marcadamente diferentes cuando graficamos retrasos contra carga recibida. Normalmente retraso se indica sobre una línea escalar mientras la pérdida se indica sobre una escala logarítmica.

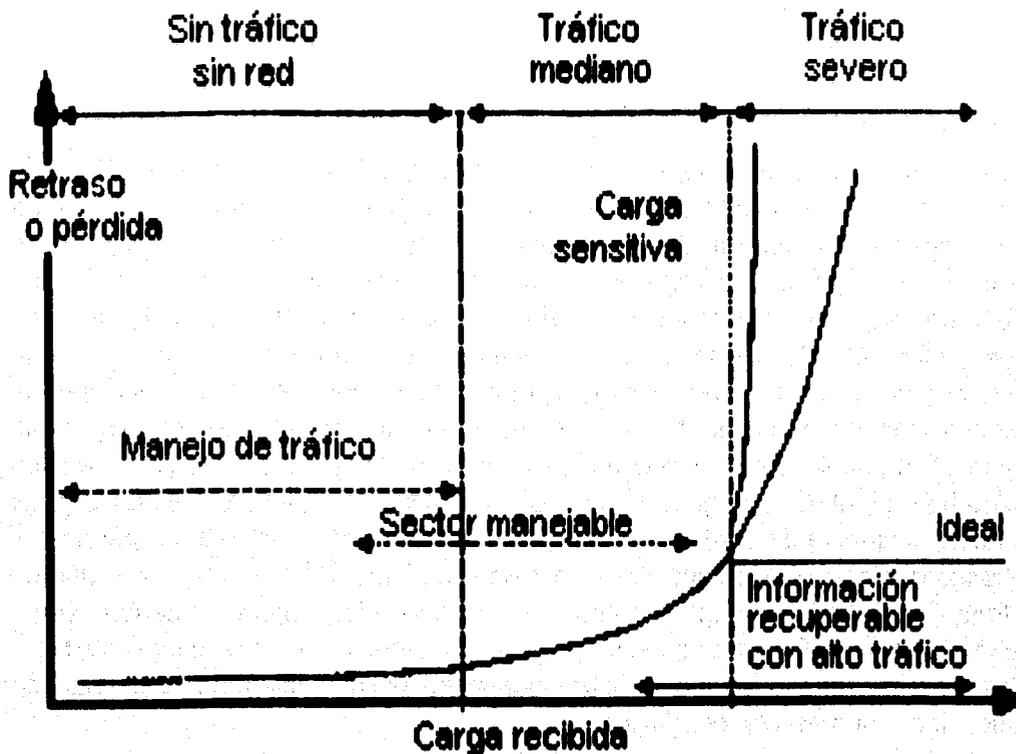


Figura 2.51 Efectos del congestionamiento en retrasos

2.8.4 Categorías de control de congestionamiento

La terminología de categorización de control del congestionamiento varía. Se han escogido las siguientes categorías que estructuran la presentación de técnicas de control del congestionamiento. Las categorías de respuesta al congestionamiento son: Manejarlo, evitarlo y recobrarlo. Cada una de éstas pueden operar a nivel de celdas como se ilustra en la tabla 2.5.

Categoría	Nivel de celda	Nivel de Explosión	Nivel de llamadas
Manejo Evitarlo	UPC Desecho EFCI	Destino de recursos Ventana, rango o crédito	Red de Ingeniería Sobreespecificaciones CAC
Recuperación	UPC Seguimiento Descuento Dinámico UPC	Retroalimentación pérdidas	Bloqueo de llamadas Procedimientos de Operación

Tabla 2.5 Categorías y Niveles del Control de Congestionamiento

El manejo del congestionamiento opera en la zona de no congestionamiento con el objetivo de vigilar que las zonas de congestionamiento como se ilustra en las figuras 2.50 y 2.51 nunca se dé. Esto incluye relocalización de recursos, descartar el uso de parámetros de control (UCP), ancho de banda absolutamente garantizado, y terminado, Control de Admisión de Conexiones (CAC) y red de Ingeniería.

Evitar el congestionamiento es un juego de mecanismos tiempo-real para prevenir y recobrar durante los periodos en que coinciden el tráfico intenso (picos) y la demanda de carga excesiva de la red. Un ejemplo de este uso se da cuando los nodos y/o las cadenas han fallado. El procedimiento para evitar el congestionamiento generalmente opera alrededor del punto entre el no congestionamiento y la media, y throughput de la zona media como se ilustra en en las figuras 2.50 y 2.51. El evitar el congestionamiento incluye Indicación Adelantada Explícita del Congestionamiento (EFCI). El Uso de Parámetros de Control (UPC) uso etiquetado de Perdida de Celdas Prioritarias (CLP) Control de Admisión de Conexiones Excesivas (CAC), Bloqueo CAC y también flujo básico de ventana-rango.

Los procedimientos de recuperación se inician para evitar el congestionamiento que degrada severamente la Calidad de Servicio que el usuario final detecta. Estos procedimientos son típicos y se inician cuando se tienen pérdidas en la red o se incrementan marcadamente los retrasos provocados por el congestionamiento. La recuperación del congestionamiento incluye el descarte selectivo de la celda, Juegos Dinámicos de Parámetros UPC, manejo de la retroalimentación por pérdidas o desconexión y procedimientos de operaciones.

2.8.5 Manejo del congestionamiento

El manejo del congestionamiento pretende asegurar que éste nunca se experimente. Por ejemplo, la forma de manejar el congestionamiento es un viaje anormal rápido en horas de tráfico, esperar hasta conocer que habrá rutas cortas en espera de un servicio particular. Esta sección cubre los siguientes métodos de manejo de congestionamiento:

- Asignación de recursos
- Uso de Descarte de Parámetros de Control (**UPC**).
- Control Completo de Admisión de Conexiones (**CAC**).
- Ingeniería de Redes

2.8.6 Asignación de recursos

Dese luego una forma de controlar el congestionamiento es evitarlo totalmente. Esto puede hacerse efectuando una asignación propia de recursos. El tema de asignación de recursos incluye:

- Capacidad de Contenido
- Espacio en Buffer
- Parámetros **UPC/NPC**
- Parámetros (**VPC**) de Conexión vía Virtual

Si la acción **UPC** (norma) es puesta para descargar celdas que exceden del rango pico y todo el contenido y recursos del buffer son asignados para éste, entonces el congestionamiento simplemente no ocurre. Este diseño puede utilizarse para manejar el peor caso de falla que se presente, bajo condiciones normales, la red responderá bien a carga completa hasta que alguna capacidad de reserva se asigne para restauración. De esta manera esta aproximación a la supresión completa del congestionamiento, el resultado de la utilización de la red puede ser muy baja, haciendo esta propuesta potencialmente cara. Esta puede ser una aproximación viable en una área local donde la transmisión y los puertos relativamente no son caros. Esta aproximación se refiere como una "sobreingeniería" de la red.

La manera en la cual los recursos son asignados para encontrar una garantía **QoS** es desde luego una decisión de red. Si son opcionales, de cualquier modo debe asignarse a los flujos **CLP=1**. Debe haber suficientes recursos asignados para encontrar los requerimientos del comportamiento para la mezcla esperada de tráfico clase **QoS**. La función del Control de Admisión de Conexiones (**CAC**) decide llamada por llamada si una conexión solicitada puede ser admitida con recursos disponibles. Los recursos para todas las clases **QoS** pueden ser una

acción sola del banco o localizada en bancos separados con objeto de lograr el aislamiento entre las clases.

2.8.7 Uso de parámetros de control de Descarte

El uso de Parámetros de Control UPC actúa como un policía de tránsito en el punto de ingreso de la red. UPC con un manejo de capacidad de descarga para asegurar que el congestionamiento no pueda ocurrir si los recursos están completamente asignados como se describe en el párrafo anterior. Al primer nodo implementado en la red UPC, por lo tanto el tráfico que podía congestionar la red no es admitido, posiblemente congestione otros nodos que reducirán su flujo. El UPC descartado puede ser utilizado en exceso, en tal caso el congestionamiento de la red puede ocurrir.

2.8.8 Control de admisión de conexiones especificadas

El rango pico de la celda, rango que sostiene a ésta, y el máximo tamaño de burst para el flujo Prioridad de Pérdida de Celdas (CLP) pueden ser usados para llenar el buffer, el almacenamiento y recursos del conmutador tal como se definió en el contrato de tráfico. Esto asegura que si todos los recursos son enviados, en el peor caso, el comportamiento del flujo de celdas se mantendría dentro de la Calidad de Servicio (QoS) especificada. Esto se conoce como Control de Admisión de Conexiones Especificadas (CAC) porque admite sólo llamadas que tengan parámetros que no puedan afectar el QoS de otras conexiones que puedan ser violadas. Estos parámetros de tráfico deben ser reforzados utilizando Parámetros de Control (UCP).

2.8.9 Ingeniería de redes

Un método para asignaciones eficientes de recursos se basa en considerar en cada decisión (incluso las de largo plazo), tendencias históricas y proyecciones. Este es el método utilizado actualmente en la mayoría de redes públicas y privadas. Este tipo de decisiones incluye la determinación de cuándo y cómo actualizar la capacidad de conmutadores o de almacenamiento. Pueden obtenerse varias mediciones estáticas del tráfico y del comportamiento para asegurar las fuentes que se utilizaron en el algoritmo de planeación de la red. Esencialmente esta área es de no estandarización por lo tanto ésta es una decisión que proporciona la red.

2.9 Ingeniería de tráfico

Esta sección contempla los modelos de las fuentes de tráfico y su tiempo de respuesta. Se cubren algunas aproximaciones para la estimación del tiempo de respuesta. Se describen los modelos de tráfico, y una introducción de sus aplicaciones, se presentan varios modelos divididos por las diferentes fuentes de tráfico, cada una se ha seleccionado para ilustrar de manera simple los conceptos clave, así como el tiempo de respuesta para la mayoría de los esquemas analizados previamente. También se analiza el tiempo respuesta para fuentes de tráfico variable (VBR). Se describe también la definición de la ganancia múltiple estática y las características de tráfico mas notorias. Finalmente se presenta un análisis de las curvas de comportamiento en el tiempo de control del tráfico. Todas las fórmulas utilizadas en estos ejemplos son muy simples y pueden aplicarse en hojas de cálculo para evaluar el comportamiento de una máquina en particular o en una configuración de red.

2.9.1 Filosofía

Esta sección contempla diferentes parámetros de la Ingeniería de tráfico :

- Características de los parámetros
- Fuentes de tráfico
- Especificaciones de respuesta y su medición
- Exactitud de los modelos

2.9.1.1 Características de los parámetros de las fuentes de tráfico

Existen dos filosofías básicas que caracterizan los parámetros de las fuentes de tráfico: Determinística y Aleatoria. Debe haber un equilibrio entre obtener exactitud y simplicidad, y entre claridad y ambigüedad.

Los parámetros determinísticos se basan en los contratos de tráfico explicados en secciones anteriores. La fracción de celdas consideradas en el contrato de tráfico pueden ser claramente medibles en diferentes puntos para verificar, conforme al contrato, que sea la adecuada para el usuario y la red. Cualquier cambio puede ser claramente negociado entre el usuario y la red. En resumen se establece el acuerdo de tráfico transmisión-recepción para obtener un tiempo de respuesta .

La otra filosofía de parámetros para modelos de fuente de tráfico utiliza modelos de probabilidad. Generalmente son confiables después de un largo plazo. Ya que el método y el intervalo para calcular el tiempo pueden diferir en las pruebas de confrontación, deben definirse los detalles del método de medición. Además de especificar los parámetros se requiere también la especificación del modelo estadístico. Con esta información el usuario y la red pueden acordar un tiempo de respuesta para un cierto nivel de tráfico transmisión-recepción. Mientras estos métodos estadísticos no sean estandarizados, su uso nos aproximará al establecimiento del contrato determinístico de tráfico. Estos métodos son muy aplicables a los análisis si se selecciona un modelo estadístico simple como se mostrará más adelante en esta sección.

2.9.1.2 Especificaciones y mediciones del desempeño

La calidad de Servicio es especificada y medida para cualquiera de los métodos siguientes:

- Conexión Virtual Individual (VPC)
- Conexión de Circuito Virtual (VCC)
- Conjunto de Conexiones (VCC o VPC).

Esta selección tiene algunas implicaciones para el tiempo de respuesta y la medición de una o varias conexiones. La QoS se especifica y se mide para cada conexión. La QoS es medida insertando en cada conexión celdas de Operación Administración y Mantenimiento (OAM), esto incrementa el tráfico de celdas e introduce más complejidad por el proceso de éstas.

Con especificaciones y mediciones individuales, existe una situación análoga a las clásicas líneas digitales privadas, donde se mide el tiempo de respuesta sobre todas y cada unas de las líneas. Por ejemplo, las estadísticas de error sobre una línea DS1 son estimadas con el Chequeo con Ciclo de Redundancia (CRC) del Frame Super Extendido (ESF) para cada DS1.

En el caso de los agregados (o conjuntos de conexiones), la QoS es promediada sobre un gran número de conexiones, lo que es el símil más natural de los circuitos virtuales. La medición en los agregados asume que el desempeño de todos los VCCs, dentro de un mismo VPC, es idéntico, lo que reduce significativamente el número de celdas de medición que deben ser transmitidas y procesadas. Típicamente el costo y complejidad de las mediciones individuales se justifica cuando el desempeño de una conexión virtual individual es crítica. Normalmente las mediciones sobre los agregados es adecuada para asegurar que la QoS de un grupo de conexiones virtuales sean conocidas y por lo tanto la QoS de una conexión virtual individual sea soportada por bases estadísticas.

2.9.1.3 Adecuación del modelado

Existe también un aspecto de la filosofía relacionado a cómo debe ser la exactitud del modelado de la Ingeniería de tráfico. Como es de esperarse, entre más complicado sea el modelo, los resultados serán más difíciles de calcular y entender. La adecuación del modelo matemático del conmutador y de la red es comparable a la adaptación del modelo de la fuente de tráfico. Si sólo se conocen aproximaciones, información no precisa acerca de la fuente, entonces es apropiada una aproximación con un modelo simple del conmutador y de la red. Si se conoce una gran cantidad de información exacta acerca de la fuente tráfico, entonces se justifica una inversión en un modelo más exacto del conmutador y de la red, así como una simulación detallada.

Mientras que el modelado detallado de la fuente teóricamente es óptimo, puede ser muy complejo y generalmente requiere simulaciones basadas en computadora. Como normalmente este nivel de detalle no está disponible al usar detalles de las fuentes y un modelo adecuado del conmutador y de la red los resultados serán suficientemente reales. Ahora cuando el tráfico o el intercambio o los detalles de red no están disponibles los modelos aproximados son la única alternativa disponible.

El modelado aproximado es más simple, puede casi siempre ser hecho usando sólo métodos analíticos, una ventaja de usar del método analítico es que proporciona una vista del comportamiento y de los intercambios muy clara. El método analítico es el utilizado en este trabajo. Sin embargo cabe advertir que estos modelos, pueden producir resultados muy optimistas o muy pesimistas dependiendo de la relación entre lo asumido con respecto a la realidad. El modelo debe ser un proceso continuo. Entre más información se tenga acerca de las características de la fuente, el tiempo de respuesta del dispositivo y las expectativas de calidad, se tendrá una mejor retroalimentación en el modelo.

2.9.1.4 Modelos de la fuente

El uso de modelos particulares, y la exactitud en la representación del tráfico es un tema de mucha discusión y es objeto de intensa y continua investigación y difusión. Este capítulo utiliza probabilidad básica y teoría de colas, con parámetros seleccionados de algunos modelos de tráfico típicos, para comentar y explicar su aplicación en situaciones extrañas.

2.9.2 Parámetros generales de modelado de las fuentes

Esta sección define algunos parámetros generales del modelado de fuentes usados a través del capítulo.

Burstiness (o *explosividad*) es un término comúnmente utilizado para medir qué tan frecuentemente una fuente envía tráfico. Una fuente que envía tráfico sin frecuencia homogénea o en picos, es conocida como explosiva, mientras que una fuente que casi siempre está enviando la misma cantidad, es conocida como no explosiva.

La fórmula que define la explosividad en términos de la cuota promedio de celdas se define como:

$$\text{Explosividad} = \text{Velocidad pico} / \text{Velocidad promedio}$$

La probabilidad de actividad de la fuente es la medida de qué tan frecuentemente la fuente transmite, definida por la probabilidad de explosividad de la fuente:

$$\text{Probabilidad Actividad Fuente} = 1 / \text{Explosividad}$$

Utilización es una medida comúnmente usada para medir la cantidad de la capacidad de enlace de transmisión que está usando la fuente, teóricamente medida sobre un período de tiempo infinito, sin embargo en la práctica la medición se hace sobre un amplio intervalo de tiempo. La definición de la utilización está dada en términos de la tasa pico de celdas y la tasa del enlace de transmisión como se indica:

$$\text{Utilización} = \text{Tasa pico} / \text{Tasa de enlace}$$

2.9.3 Procesos de arribo de Poisson y de Markov

Los procesos donde se tiene un arribo aleatorio son descritos como generales mientras que los procesos de Poisson (o de Markov) como particulares.

Con referencia en la figura 2.52 la recepción Poisson ocurre cuando para cada incremento de tiempo (T), no importando qué tan grande o pequeño sea, la probabilidad de recepción es independiente de cualquier hecho anterior. Estos eventos pueden ser celdas individuales, celdas explosivas, una celda o un paquete completo de servicio, u otros eventos arbitrarios en el modelo.

Ilustración de un Proceso de Llegada

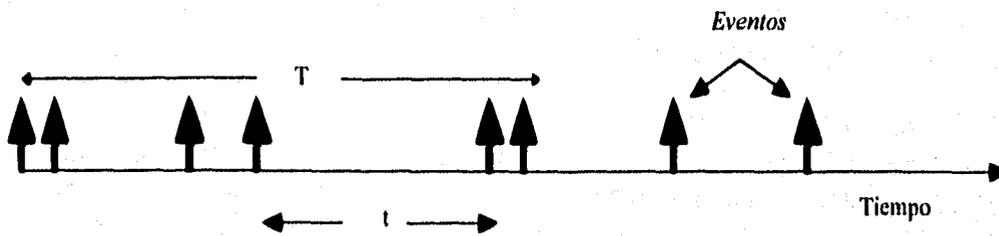


Figura 2.52

La probabilidad del tiempo entre arribo de eventos t , como se muestra en la figura 2.52, tiene un cierto valor conocido como la *densidad de probabilidad de tiempo entre arribos*. La siguiente ecuación da el resultado probabilístico donde el tiempo entre las recepciones t es igual a un valor x cuando la velocidad promedio de arribo es λ eventos por segundo.

$$\text{Probabilidad } (t=x) = \lambda e^{-\lambda x}$$

Este se conoce como proceso de pérdida de memoria, porque la probabilidad de que el tiempo entre arribos sea x segundos es independiente de la memoria o de cuanto tiempo haya transcurrido. Este hecho simplifica enormemente el proceso de análisis aleatorio ya que no se tiene historia pasada o ninguna memoria que deba ser conservada. Este tipo de procesos es normalmente conocido como procesos de Markov, en honor del matemático ruso de siglo XIX.

La probabilidad de que ocurran "n" recepciones independientes en T segundos esta dada por la famosa distribución de Poisson:

$$\text{Prob. } (n,T) = \frac{(\lambda T)^n e^{-\lambda T}}{n!}$$

Combinando estos dos conceptos en un modelo común denominado Proceso de Poisson modulado por Markov (MMPP). Existen dos tipos básicos de este proceso: El *discreto* que corresponde a celdas ATM y el *continuo* que corresponde mejor a las Unidades de Datos de Protocolo (PDUs) que generan

explosiones de celdas. Las figuras siguientes dan un ejemplo de los modelos discretos y continuos.

Las etiquetas sobre las flechas de la figura 2.53 muestran la probabilidad de transición de las fuentes entre los estados de explosión activo, inactivo o permanecer en el mismo estado. En otras palabras durante cada unidad de tiempo, las fuentes tienen una transición de estado, ya sea cambiando a otro estado o volviendo a su mismo estado. La probabilidad para cada acción se indica por las flechas en el diagrama.

Modelo del proceso de Markov para Tiempo Discreto

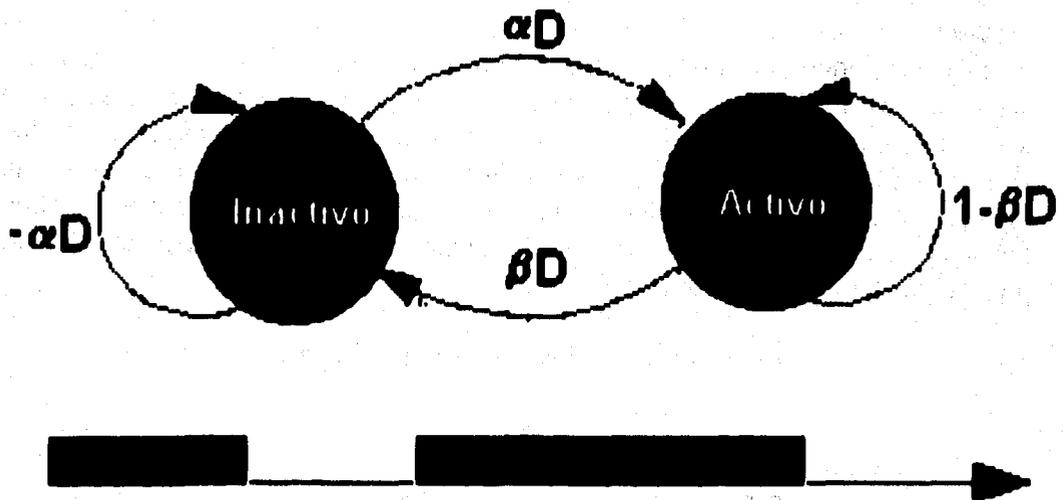


Figura 2.53

La explosividad o tasa pico-a-promedio del modelo de fuente discreta está dado por la siguiente ecuación:

$$b = \frac{\alpha + \beta}{\beta}$$

Donde α = número promedio de recepciones explosivas por segundo
 β = tasa promedio de los picos completos.

Pensando en términos de β^{-1} , que tiene unidades de números de segundo promedio por explosión. D se define como el tiempo de cuantificación de celda en unidades de segundo por celda. De otra manera αD define la probabilidad de que inicie una explosión de celdas en un tiempo particular y βD define la probabilidad de que termine esta explosión en un tiempo particular. La duración promedio de la explosión d (en celdas) se calcula con una serie geométrica estándar como se muestra:

$$\delta = \frac{1}{\beta D}$$

El caso de tiempo continuo se muestra en la figura 2.54. El tiempo empleado desde que inicia una explosión hasta que termina, es modelado en lugar de modelar las celdas individualmente. Se pierde alguna exactitud en la cuantificación inherente en la segmentación y reensamble que no se considera, sin embargo en este trabajo se utiliza este modelo por su simplicidad. El diagrama se conoce como diagrama de estados de transición de velocidades ya que las variables asociadas con las flechas refieren a una tasa exponencial en la distribución exponencial negativa, presentada al principio de esta sección. Ambos modelos discreto y continuo de Markov preeven resultados equivalentes excepto para las celdas que cuantifican el factor D .

Proceso de Markov de Tiempo Continuo

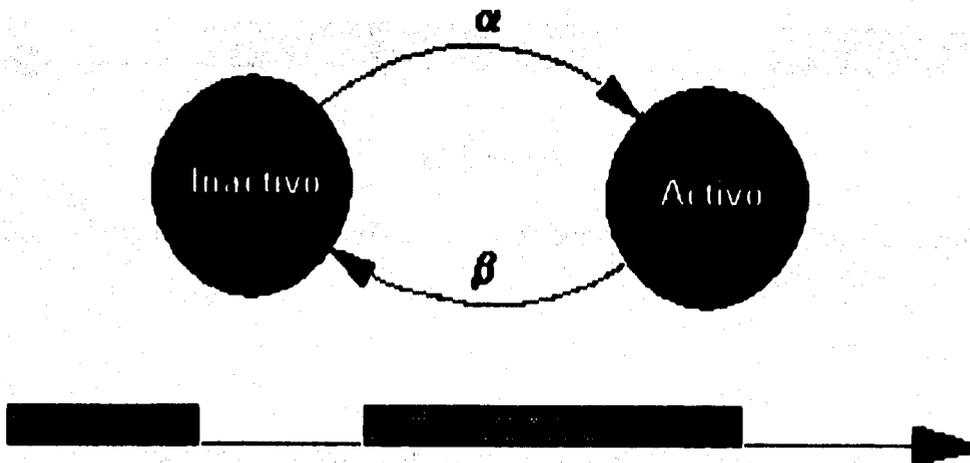


Figura 2.54

La correspondiente explosividad b para el proceso continuo es:

$$b = \frac{\alpha + \beta}{\beta}$$

La duración promedio de las explosiones (en seg.) está dada por:

$$d = \frac{1}{\beta}$$

Note como estas fórmulas son idénticas para los casos discretos excepto para la ausencia del tiempo de celda discreta D en el denominador de la ecuación de la duración para el promedio de explosión del modelo continuo. Otra distribución que se utiliza algunas veces para modelar tráfico explosivo extremo es la hiperexponencial, la cual es la suma efectiva de un amplio número de recepciones exponenciales negativas. Esto lo convierte en un modelo más pesimista que el modelo de tráfico de Poisson, porque la explosividad y las recepciones pico son más densas.

Un trabajo efectuado recientemente basado en la medición de tráfico en redes LAN indica que los modelos tradicionales de tráfico pueden ser demasiado optimistas. Los resultados mostrados en las LAN en Bellcore son muy similares, lo que significa que el tráfico tiene propiedades similares sin importar la escala de tiempo en la que se observa. Este es un contraste entre los modelos de Poisson y Markov, donde el tráfico tiende a ser más suave y más predecible entre más muestreos se consideren.

2.9.4 Modelos de sistemas de colas

La categorización de los Sistemas de Colas se muestra en la figura 2.55. Usaremos esta terminología en este capítulo ya que se utiliza ampliamente en la literatura técnica.

Analizaremos dos ejemplos particulares en los sistemas de cola: El M/D/1 y el M/M/1, de la notación podemos observar que ambos tienen recepciones Markovianas (arribos de explosiones en forma exponencial negativa con pérdida de memoria) a una cuota de λ explosiones por segundo. El sistema M/M/1 tiene longitudes de explosiones aleatorias con una distribución exponencial negativa (Markov), mientras que el sistema M/D/1 tiene explosiones de longitud constante. El parámetro μ^{-1} define cuántos segundos (en promedio) pueden ser requeridos para que un enlace de transmisión envíe cada explosión. Para el sistema M/M/1 éste es un número aleatorio de duración promedio calculado con distribución exponencial, mientras que para el sistema M/D/1 cada explosión es de

longitud constante. Ambos sistemas tienen también un solo servidor (por ejemplo un enlace físico de transmisión), una población infinita (número de posibles explosiones) y un número infinito de buffers (Espacio de almacenamiento temporal). Las unidades de los buffers en el modelo M/D/1 son celdas mientras que en el caso de M/M/1 son explosiones. La figura 2.56 muestra estos Sistemas de Cola física y sus relaciones específicas con ATM.

A / B / s (/ W) (/ p)

A Procesos de arribo :

M = Markoviano

G = General

D = Determinístico

B Proceso de salida :

M = Markoviano

G = General

D = Determinístico

s Número de servidores de colas

w Espacio de espera (posiciones de buffer)

p Población fuente

Figura 2.55

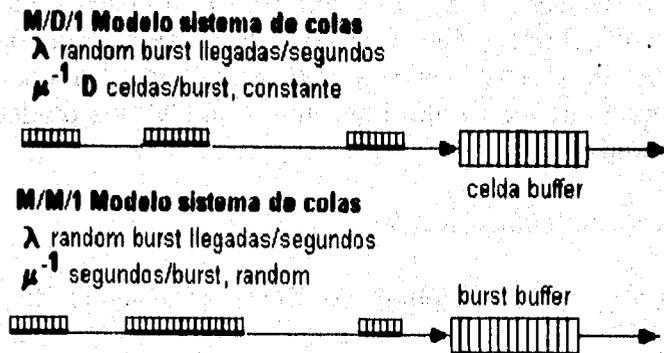


Figura 2.56

Este es un buen ejemplo de los intercambios encontrados en el modelado. El sistema M/D/1 representa exactamente el hecho de que los buffers en el conmutador son unidades de celdas; sin embargo, el modelado de las explosiones las contempla todas de longitud constante. El sistema M/M/1 no modela exactamente los buffers del conmutador ya que éste utiliza unidades de explosión y no celdas, sin embargo, el modelado de longitudes aleatorias de explosión es más apropiada para muchas fuentes de tráfico. El modelo M/M/1 es también muy simple de analizar, por lo que será usado extensivamente para ilustrar tendencias específicas en sistemas ATM. En general, si el tráfico es más determinístico que en el modelo M/M/1 (por ejemplo como el modelo M/D/1), entonces el modelo M/M/1 será pesimista (habrá menos colas de espera y más retardos en la red modelada). Si el tráfico es más explosivo que en el modelo M/M/1 entonces los resultados del M/M/1 serán optimistas (habrá más colas y menos retardos en la red modelada). En muchos de los resultados siguientes los retardos del sistema y las bajas en el desempeño se presentarán en términos de la carga ofrecida ρ , dada por la siguiente fórmula:

$$\rho = \lambda / \mu$$

Remarcando que λ es el número promedio de llegadas de explosiones por segundo y que μ^{-1} es el promedio de segundos por explosión, esto refleja que la carga ofrecida ρ es adimensional y se interpreta como la parte, en promedio, de la capacidad de los recursos que están usando.

La relación de servicio μ es calculada como sigue para una explosión de B bytes en una velocidad de línea de R byts por segundo:

$$\mu = \frac{B \text{ (explosión)}}{R \text{ (segundos)}}$$

La probabilidad que haya "n" explosiones esperando en la cola M/M/1 está dada por la siguiente fórmula:

$$\text{Prob (n explosión en la cola M/M/1)} = \rho^n (1-\rho)$$

El promedio de retardo del encolamiento (tiempo de espera) se da por la siguiente fórmula:

$$\text{Avg(retraso de encolamiento M/M/1)} = \frac{\rho / \mu}{1-\rho}$$

El encolamiento M/D/1 predice un mejor desempeño que el M/M/1. El retardo promedio de un encolamiento M/D/1 es exactamente una y media veces el retardo de M/M/1. La probabilidad para el número de celdas en la cola del M/D/1 es mucho más complicada, por lo cual el modelo M/M/1 será utilizado en la mayoría de los ejemplos siguientes.

2.9.5 Proceso de Bernoulli y aproximación Gaussiana

Un proceso Bernoulli es esencialmente el resultado de N lanzamientos de moneda independientes (o intentos de Bernoulli) de una "moneda injusta". Una moneda injusta es aquella donde las probabilidades de cara y cruz no son iguales, con p siendo la probabilidad de que una cara ocurra como resultado del lanzamiento de la moneda y $(1 - p)$ es la probabilidad de que una cruz ocurra. La probabilidad de que K caras ocurran como el resultado de N intentos de Bernoulli es llamada *distribución binomial* y está dada por:

$$\Pr (k \text{ "caras" en } N \text{ "intentos"}) = \binom{N}{k} p^k (1 - p)^{N-k}$$

donde:

$$\binom{N}{K} = \frac{N!}{(N-k)! k!}$$

La distribución gaussiana o normal es una aproximación continua a la distribución binomial donde Np es un número muy grande. En la figura 2.57 se compara la distribución gaussiana y binomial para un ejemplo donde $N= 100$ y $p= 0.1$. Las distribuciones tienen básicamente la misma forma, y para valores grandes de Np , en la región $Np(1-p)$, la distribución gaussiana es todavía una aproximación razonable a la distribución binomial.

Esto es útil en el análisis relativo al desempeño ya que el área de probabilidad bajo la campana de Gauss o normal, está ampliamente tabulada e implementada en varias hojas de cálculo y sistemas o programación matemática. Aproximamos la curva de la distribución binomial a través de las distribuciones acumulativas de densidad normal, $Q(x)$. Usaremos la siguiente aproximación varias veces para estimar probabilidad de pérdida o ganancia de multiplexaje estático:

$$\text{Prob}[k > x] = Q \left[\frac{x - \mu}{\sigma} \right] = Q(\alpha) \approx \frac{1}{\alpha} e^{-\alpha^2/2}$$

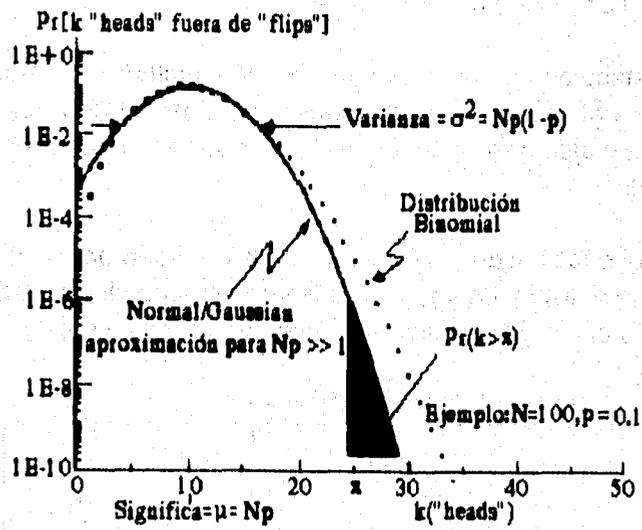


Figura 2.57

2.9.6 Desempeño de métodos de buffer

Esta sección analiza varios modelos simples de retardo del conmutador y pérdida de desempeño y cómo son impactados por varios aspectos de la arquitectura del buffer del conmutador. Por simplicidad, entradas de Poisson y tiempos de servicio exponenciales negativos son asumidos. El desempeño del retardo en la cola de salida se comporta como un sistema M/M/1 clásico. En el encolamiento de entrada incurre en un problema conocido como Bloqueo de la cabeza de línea (Head Of Line HOL). Este Bloqueo ocurre cuando la celda en la cabeza de la cola de entrada no puede entrar a la matriz del conmutador porque la celda a la cabeza de otra cola está cruzando la matriz.

Para tráfico distribuido no uniformemente y con longitudes de mensajes aleatorios la carga máxima ofrecida soportable para la cola de entrada está limitada al 50% mientras los mensajes de longitudes fijas incrementan la carga ofrecida soportable a sólo aprox. 58%.

Por otro lado, el encolamiento de salida no está limitado por la utilización como el encolamiento de entrada. La figura 2.58 ilustra este resultado graficando el retardo promedio contra el throughput para las colas de entrada y salida.

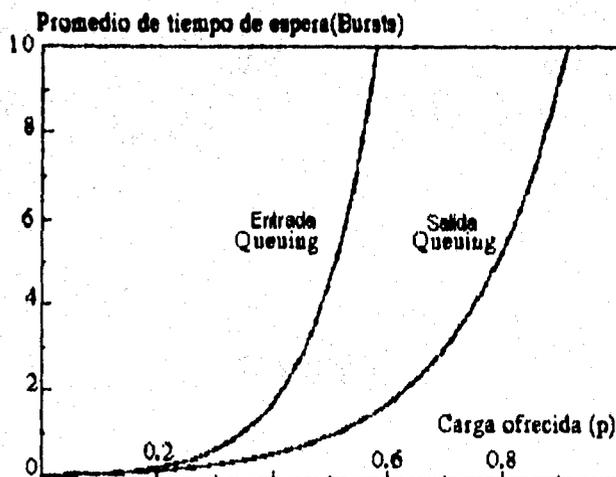


Figura 2.58

La consecuencia de estos resultados es que la mayoría de los conmutadores ATM tienen alguna forma de encolamiento de salida.

Si el buffer de entrada es utilizado en un conmutador que es considerado, verifique que algún mecanismo de control del HOL esté implementado. Ejemplos de los métodos para manejar el bloqueo HOL son: un conmutador con electrónica que opere más rápido que las velocidades acumuladas de los puertos de entrada, o utilizar prioridad de encolamiento a la entrada.

El siguiente ejemplo proporciona una simple y muy útil aproximación para la probabilidad de desbordamiento del buffer de salida. Por simplicidad un sistema de encolamiento $M/M/1$ que tiene un buffer infinito es utilizado en lugar de un sistema $M/M/1/B$ que tiene un buffer finito. La probabilidad de desbordamiento para un buffer de tamaño de B (celdas) es aproximadamente la probabilidad que hay de B/P explosiones en el sistema de cola infinita. La comparación del resultado de la simulación y del análisis exacto muestran que hay una aproximación razonable. Cuando el promedio de la explosión de celdas, originadas por PDUs, es de tamaño P celdas, la aproximación a la probabilidad del desbordamiento del buffer está dada por la siguiente fórmula:

$$\text{Prob(Overflow)} \approx \rho^{B/P+1}$$

La Figura 2.59 grafica aproximadamente la probabilidad del desbordamiento del buffer contra el tamaño de buffer (en B celdas) para varios niveles de throughput ρ asumiendo un tamaño de PDU de una celda $P=1$. El desempeño para otros tamaños de explosión pueden ser leídos a partir de esta gráfica multiplicando el eje de las X por el tamaño de la explosión de PDUs de tamaño de P celdas.

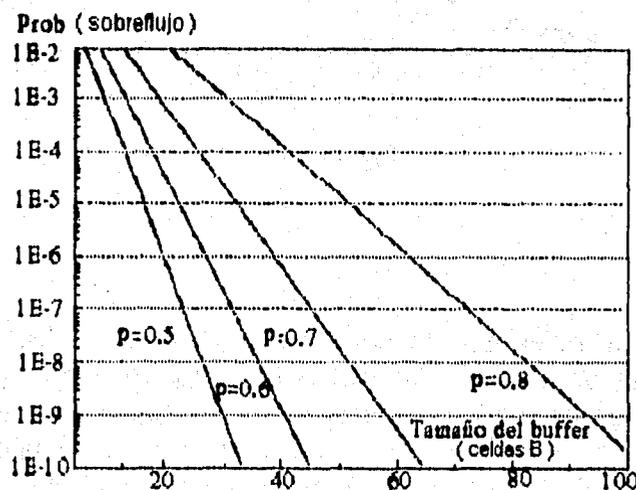


Figura 2.59

Note que para una probabilidad específica de desbordamiento objetiva y el tamaño fijo del buffer deben ser limitados a un valor máximo. Ilustramos este concepto resolviendo la ecuación anterior para la probabilidad de desbordamiento en términos del tamaño del buffer requerido B para lograr un objetivo de porcentaje de pérdida de celdas (CLR). El resultado es el siguiente:

$$B \approx \frac{P \log(\text{CLR})}{\log(\rho)}$$

La figura 2.60 muestra la gráfica del número de celdas requeridas en el buffer para lograr un objetivo de promedio de pérdida de celdas (CLR) para un tamaño de PDU de $P=1$ (celdas) para esta ecuación. Note como los incrementos de la carga ofrecida requieren incremento en el número de buffers en forma no lineal.

Buffers requeridos para alcanzar objetivo de perdidas

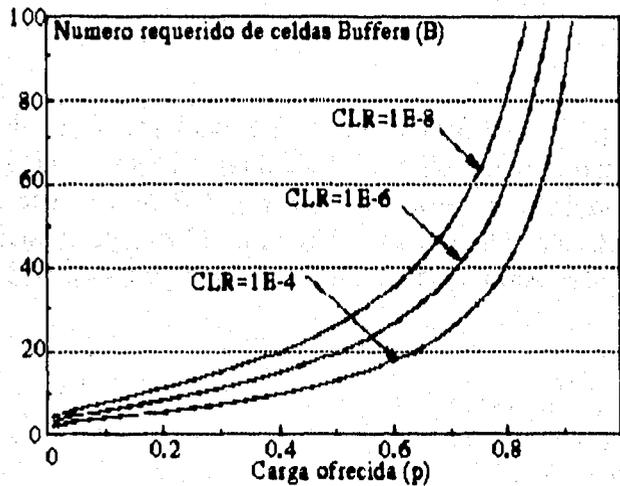


Figura 2.60

La figura 2.61 ilustra el impacto del tamaño (P) de las PDUs de las capas superiores en el desempeño del desbordamiento del buffer para diferentes tamaños de buffers de salida (B celdas). Como es esperado la probabilidad del desbordamiento del buffer crece con los incrementos del tamaño de las PDUs. Cuando el tamaño de la PDU se aproxima al tamaño del buffer el promedio de pérdida es casi del 100%.

El esquema de un buffer de salida compartido tiene una marcada mejora en el desempeño del desbordamiento del buffer porque se comparte un solo buffer que es más grande que los buffers de muchos puertos. Y ya que es muy inusual que todos los puertos estén congestionados al mismo tiempo, las pérdidas serán mucho menores que un número equivalente de buffers dedicados a cada puerto.

Probabilidad de desbordamiento vs el tamaño de la explosión de PDU

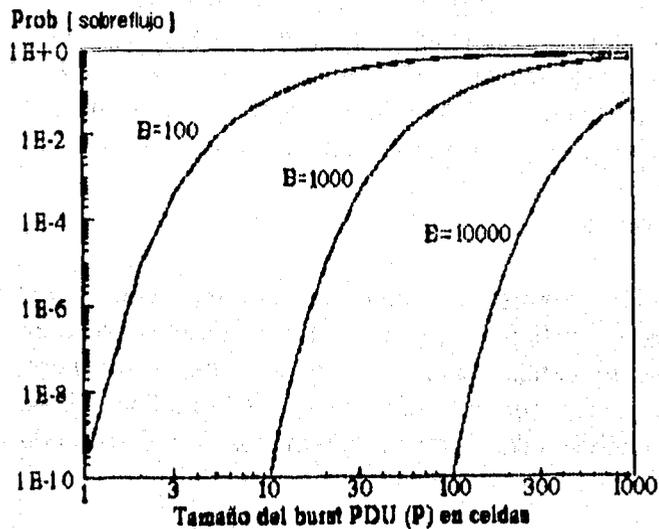


Figura 2.61

Como el análisis exacto del desempeño del buffer compartido es algo complicado presentamos una simple aproximación basada en una distribución normal. En la arquitectura del buffer compartido, N puertos del conmutador comparten un buffer común, cada uno con aproximadamente los requerimientos de probabilidad de distribución $M/M/1$ en el espacio del buffer. La suma de la demanda de cada puerto individual determina la distribución de probabilidad de un buffer compartido. La distribución normal se aproxima a la suma de cada variable aleatoria para valores altos de N .

La eficiencia y la varianza de la aproximación normal son entonces dadas como sigue:

$$\text{Eficiencia} = \frac{N_0}{1 - \rho} \quad \text{Varianza} = \frac{2 N_0^2}{(1 - \rho)^2}$$

La figura 2.62 muestra una gráfica de la probabilidad de saturación contra el tamaño del buffer equivalente por puerto para buffers compartidos en conmutadores con incremento del tamaño del puerto (N) y la gráfica del desempeño de un buffer de salida dedicado para valores altos de N (de la figura 2.59) para propósitos de comparación. La carga ofrecida es:

$\rho = 0.8$ o 80% de carga

La capacidad total del buffer en el de un buffer compartido de un conmutador es N veces la capacidad del buffer en el eje de las x. Nótese que cuando se incrementa N, la capacidad requerida por puerto se aproxima a un valor constante. Esto ilustra la eficiencia teórica del buffer compartido. Desde luego, una implementación práctica tiene límites en términos de velocidad de acceso al buffer compartido.

Desempeño de Buffers Compartidos vs Dedicados

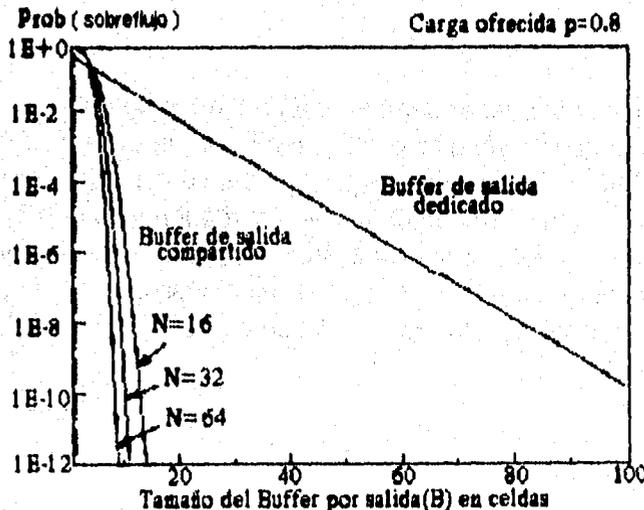


Figura 2.62

2.9.7 Desempeño CBR determinístico

La medida adecuada de la pérdida de desempeño de otro importante tipo de tráfico, Velocidad continua de bits (CBR), se calcula fácilmente. La figura 2.63 ilustra el modelo de la fuente básica de tráfico con N fuentes idénticas emitiendo una celda cada T segundos, cada inicio de transmisión en una fase aleatoria en el intervalo $(0, T)$, define el modelo de tráfico fuente.

La velocidad de pérdida de celdas como entrada de tráfico CBR se aproxima con la siguiente fórmula:

$$P_L = \text{Prob (pérdida de celda)} \approx \exp [-2B^2 / n - 2B (1-\rho)]$$

Donde

- n es el número de conexiones CBR
- B Es la capacidad del buffer (en celdas)
- $\rho = nT$ es la carga ofrecida

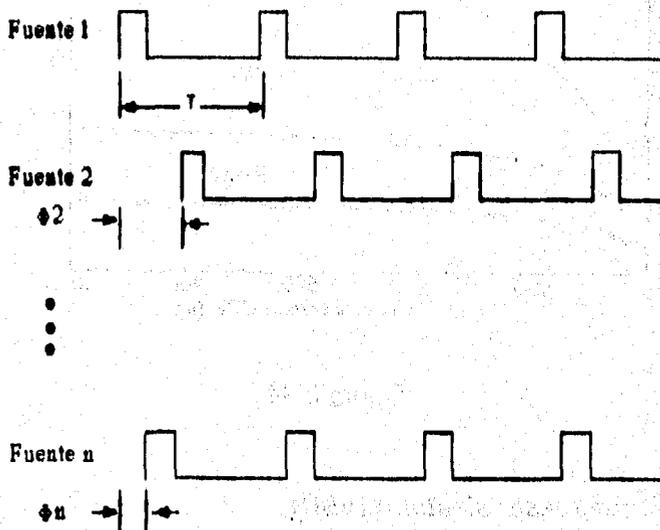


Figura 2.63

Una forma aproximada de solución puede ser fácilmente derivada del número de buffers requeridos para lograr una cierta probabilidad de pérdida de la fórmula anterior con el siguiente resultado:

$$B \approx \frac{\sqrt{[n(1-p)]^2 - 2n \ln(P_L)} - n(1-p)}{2}$$

La figura 2.64 muestra el resultado de este cálculo graficando los Buffers requeridos B contra el número de conexiones CBR (n) para diferentes niveles de throughput. Cuando el conmutador implementa prioridades de encolamiento, las mediciones de desempeño efectuadas pueden ser aplicadas independientemente unas de otras.

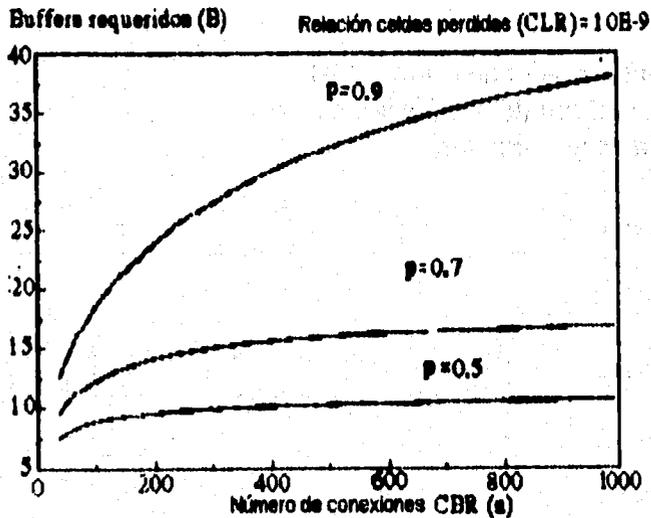


Figura 2.64

2.9.8 Tiempo de respuesta aleatorio (VBR)

La distribución de tráfico para velocidades de bit variables (VBR) puede ser modelada usando una aproximación normal a la distribución binomial para fuentes V VBR con una actividad promedio por fuente de p, usando los siguientes parámetros:

$$\text{Eficiencia} = Vp \quad \text{Varianza} = Vp(1-p)$$

De estos parámetros la pérdida esperada puede ser estimada y utilizada para saber el número requerido de buffers como se muestra:

$$B \approx Vp + \alpha \sqrt{Vp(1-p)}$$

Donde el parámetro α está determinado por la ecuación de la razón de pérdida de celdas (CLR) al final de la distribución normal llamada $Q(\alpha) = CLR$. La figura 2.65 ilustra el número requerido de buffers para lograr un objetivo de pérdida de celdas específica para diferentes valores de la actividad de la fuente p .

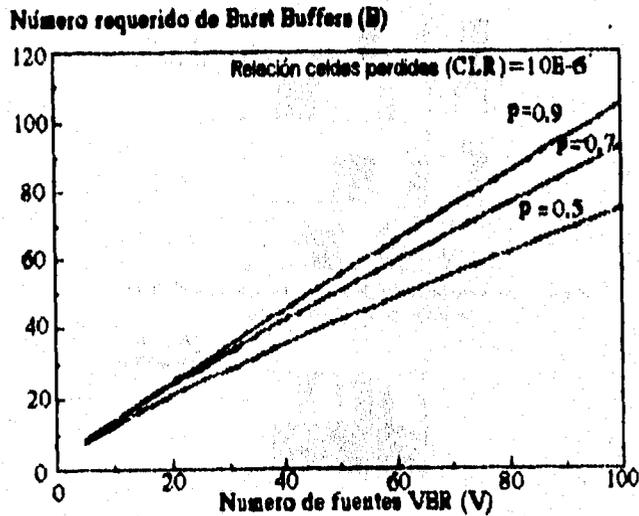


Figura 2.65

2.9.9 Ganancia de multiplexaje estadístico

Una capacidad clave que ATM permite es el multiplexaje estadístico, el cual intenta explorar la activación/desactivación, de la naturaleza explosiva de muchos tipos de fuente mostrados en la figura 2.66. En el lado izquierdo existen algunas fuentes de explosiones de celdas ATM: una pantalla de video, un servidor, una cámara y un monitor. El trazo inferior en la figura muestra una gráfica de la suma de estas celdas pico en este particular ejemplo, sólo dos canales son requeridos en cualquier punto de tiempo. Entre más y más fuentes sean multiplexadas juntas, las estadísticas de la suma compuesta permitirán mayor predictibilidad.

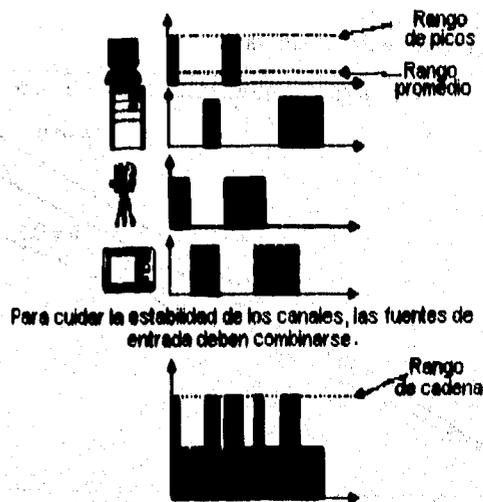


Figura 2.66

La ganancia del multiplexaje estadístico G es definida por el siguiente porcentaje:

$$G = \frac{\text{Número de fuentes soportadas}}{\text{Número de canales requeridos}}$$

La ganancia del multiplexaje estadístico G puede ser calculada con la distribución binomial o estimada de la distribución normal con los siguientes parámetros:

$$\text{Ganancia} = \frac{N}{b}$$

Donde N es el número de fuentes
 b es la explosividad (rango pico / rango promedio)

El número requerido de canales, C (en unidades de número de fuentes de rangos pico), para obtener una objetiva razón de pérdida de celdas (CLR) de $Q(\alpha)$ está dado por :

$$C \approx \frac{N}{b} + \alpha \sqrt{\frac{N(b-1)}{b}}$$

El parámetro η define la razón pico de la velocidad-fuente-a-la-velocidad-de-enlace, que significa que la capacidad de enlace es:

$$\text{Capacidad de enlace} = 1/\eta$$

De esta manera la ganancia del multiplexaje estadístico se reduce a :

$$G = N/C = N\eta$$

Substituyendo C en la ecuación anterior, igualando a la capacidad de enlace $1/\eta$ y resolviendo para N usando la fórmula cuadrática el resultado es :

$$G \approx \frac{\eta(\sqrt{\alpha^2(b-1) + 4b/\eta} - \alpha\sqrt{b-1})^2}{4}$$

La figura 2.67 muestra la ganancia del multiplexaje estadístico G lograda contra el promedio de velocidad pico-a-enlace η con la explosividad b como un parámetro para el promedio de pérdida de celdas de 10^{-6} esta figura muestra el comportamiento del multiplexaje estadístico: La velocidad de cualquier fuente individual debe ser menor con respecto a la del enlace η , y la explosividad de las fuentes b debe ser mayor para lograr una alta ganancia del multiplexaje estadístico G .

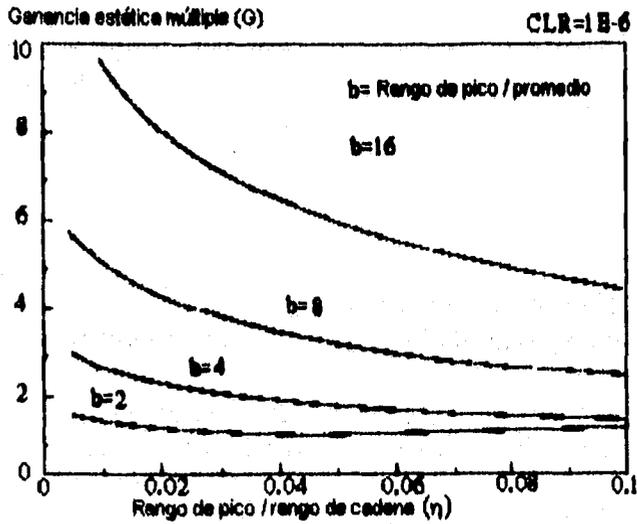


Figura 2.67

La figura 2.68 muestra como muchas fuentes deben ser multiplexadas juntas para obtener la ganancia de multiplexaje estadístico prevista en el ejemplo anterior. Esto confirma la aplicabilidad de la ganancia del multiplexaje estadístico en un amplio número N de fuentes, de baja velocidad promedio $1/b$ y una velocidad pico modesta, con respecto a la velocidad de enlace η , deben ser multiplexadas juntas para lograr una mayor ganancia del multiplexaje estadístico G.

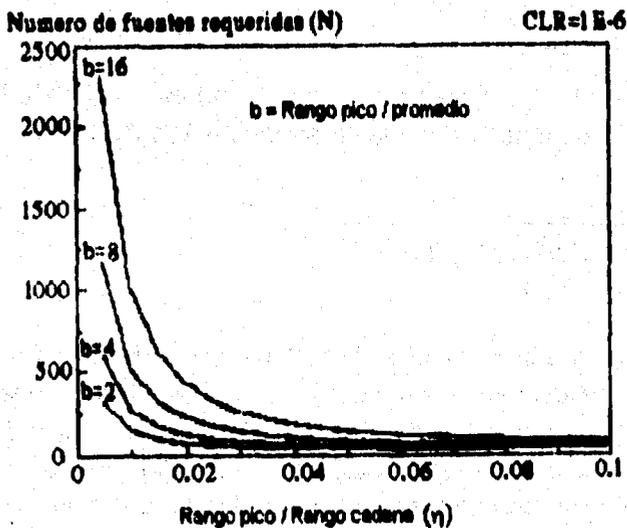


Figura 2.68

CAPITULO 3

PLANTEAMIENTO DEL PROBLEMA

En este capítulo se aborda el análisis de una empresa con requerimientos de red, donde el esquema con ATM puede funcionar. Se analizan diversos aspectos que definirán las bases sobre las cuales se diseñará esta solución de red y proporcionará los lineamientos generales que determinarán el desarrollo de los capítulos subsecuentes.

3.1 Antecedentes

El grupo empresarial que sirvió de base para este estudio es un corporativo constituido por diversas empresas de un giro afin. La estructura organizacional define diversas entidades independientes entre sí, que incluso por la naturaleza del negocio pueden competir por proyectos, aunque por definición existen puntos específicos de interdependencia entre las diferentes entidades como son los servicios de telecomunicaciones; sin embargo cada empresa organizó departamentos internos independientes unos de otros que atendieran sus necesidades específicas. Este hecho generó que las diversas empresas eligieran equipos de cómputo, aplicaciones, protocolos de comunicación, topologías o herramientas de monitoreo que mejor satisficieran las necesidades particulares, desarrollando centros de cómputo diferentes, con manejo de recursos propios.

De aquí se derivan situaciones especiales como son:

- Duplicación de funciones
- Aislamiento tecnológico y de información
- Alto costo en inversiones particulares de equipo
- Falta de estándares
- Difícil consolidación de información financiera

Por la naturaleza del negocio se tienen localidades remotas con posición geográfica variable que dependen administrativamente de diferentes empresas. La comunicación entre estas entidades y las oficinas centrales se realiza por medio de una red satelital que cuenta con una antena central y 35 antenas receptoras. Esta red proporciona servicios de voz principalmente al utilizar conmutadores telefónicos (PBX) conectados a las estaciones receptoras. Esta red ha funcionado por casi dos años satisfaciendo los requerimientos de voz de la compañía.

La red es administrada por un departamento de telecomunicaciones que se encarga de supervisar la operación de la red satelital que proporciona los servicios de voz y video a las localidades remotas. La red corporativa presta servicios a todas las empresas del grupo.

El departamento corporativo de informática se encargó de diseñar la red local de datos corporativa, y determinó los estándares y normas de conectividad que seguiría el grupo.

Aunque no existe un centro de cómputo centralizado el grupo utiliza equipos de cómputo estándares, entre los de capacidad media podemos mencionar máquinas UNIX HP9000 de diferentes modelos y capacidades.

Una de las empresas pioneras en la instalación de redes es la Empresa A, localizada en la Torre Y. En base al esquema presentado por esta empresa el resto implementó su solución de red. Esta consistió en un cableado estructurado nivel 3 con comunicación remota basada en enrutadores multiprotocolo y servidores de archivo e impresión Novell.

3.2 Organización y estructura

El grupo corporativo denominado "La empresa" comprende once unidades en total (seis empresas y cinco departamentos). Cuatro empresas y cuatro departamentos tienen implementadas redes locales. Las seis empresas tienen localidades foráneas (se tiene comunicación de voz en 31 de ellas), independientes y cada una ataca nichos específicos de mercado, aunque éstos en ocasiones pueden coincidir de una empresa con otra. Todas cuentan con departamento de sistemas.

De estas compañías, la Empresa A está asociada con una empresa americana que le ha impuesto estándares de conectividad, lo que se ha convertido en una de las más avanzadas, en tecnología de cómputo y comunicaciones del grupo.

Existe también la Empresa B que aunque es la más grande del grupo en recursos materiales y humanos, carece de una sólida infraestructura de cómputo, por este motivo se contempla un desarrollo sostenido en los próximos años y es fundamental definir una estrategia que permita soportar los altos requerimientos del crecimiento de esta empresa.

También está la Empresa C que se puede considerar de tamaño medio dentro del grupo y que cuenta con una avanzada red inalámbrica que presenta problemas de crecimiento por costo.

Existen otras tres compañías que desarrollan su actividad independiente del resto de las empresas del grupo. Dentro de éstas sólo una es foránea y cuenta con equipo de cómputo y una red local.

Las cinco entidades restantes son departamentos que prestan servicio a todas las demás estructuras del grupo y aunque algunas cuentan con servicios propios como finanzas y recursos humanos; todas concentran información para reportes ejecutivos y reportes a la Bolsa Mexicana de Valores. Estas empresas también cuentan con subdivisiones de servicio que establecen e integran soluciones de cómputo y comunicaciones.

Dentro de estas empresas se encuentra una área de telecomunicaciones que opera la red satelital, además de proveer servicios de portadora a las otras empresas, también ofrece y mantiene los servicios de telefonía. Esta área cuenta con la única red Token Ring del grupo, y además brinda, a algunas áreas y empresas, servicios de asesoría en instalación de servidores de Red y PC's clientes.

3.3 Distribución física

Las diversas empresas y departamentos del grupo se encuentran distribuidos en dos esquemas principales:

- Central
- Remoto

El Esquema Central se divide en tres estructuras principales :

a) Conjunto Corporativo

Está formado por seis edificios independientes, localizados alrededor de un edificio principal donde se encuentran las oficinas ejecutivas del grupo y unidos por una área común de estacionamiento. Cada uno de los edificios que conforman este complejo consta de tres niveles y cada uno tiene una letra de identificación, las letras asignadas a estos edificios son D,R,S,T,U,V,W.

b) Edificio Y

Este consta de 9 niveles, físicamente es independiente del conjunto Corporativo y se encuentra a una distancia de 600 mts. de éste.

c) Edificio Z

Es un edificio de tres niveles; es el más grande del grupo y se encuentra localizado a 900 mts. del conjunto corporativo.

El esquema remoto se divide en dos:

- Planta y Abastecimientos.

Nave industrial donde se tiene sólo una pequeña parte de oficinas.

- Localidad remota

Unidades móviles que son transportadas según las necesidades de las empresas y que constan de oficinas con capacidad para seis personas.

El esquema central está representado en la figura 3.1:

Esquema de edificios de la empresa

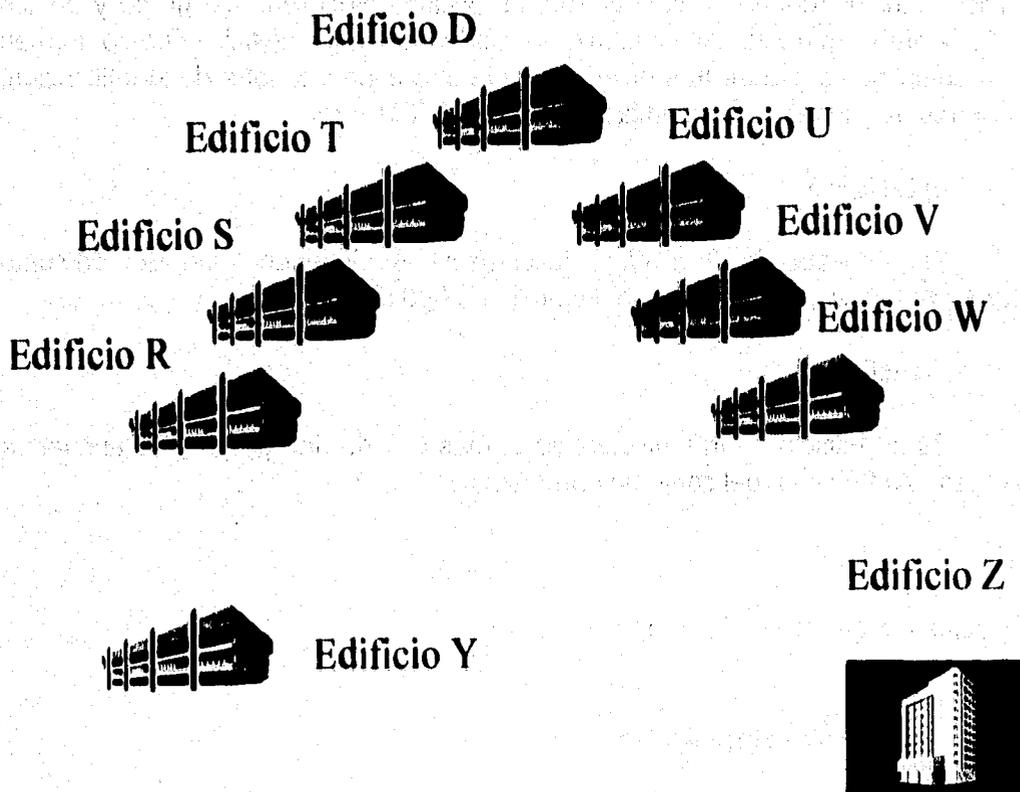


Figura 3.1

Distribución de empresas en edificios

Empresa	Núm PC's	Núm. Usuarios	Edificio	Localidades Remotas
Empresa A	200	300	Y	5
Empresa B	480	800	R,S,U,Z	20
Empresa C	150	300	T,D	5
Empresa D	080	080	V,Z	2
Empresa E	120	150	Z	1
Empresa F	030	040	Z	2
Administración	080	160	U,V,Z	-
Finanzas	050	090	W,Z	-
Telecomunicaciones	020	030	D,U	-
Rec. Humanos	060	080	W,T	-
Total	1250	2030		35

Tabla 3.1

3.4 Análisis y evaluación de las redes actuales

3.4.1 Generalidades

En el grupo se tienen redes locales para resolver tres necesidades específicas:

- 1.- Servidor de archivos
- 2.- Servidor de impresión
- 3.- Acceso a microcomputadoras (HP9000 UNIX-TCP/IP)

Cada empresa ha resuelto estas necesidades de diferente forma, pero en general podemos detectar que la mayoría ha implementado Servidores Novell como servidores de archivos e impresión; así como Servidores de comunicación para conexión Ethernet/Asíncrona de terminales tontas para acceso a las minicomputadoras. Estas redes se tienen implementadas con UTP nivel 3 utilizando cableado estructurado y concentradores HP o Synoptics y coaxial delgado.

Para comunicación de datos con las localidades foráneas (repartidas en la República Mexicana y en EU.) se utiliza una red satelital, con una configuración punto a punto entre la localidad foránea y el Corporativo, o con las obras. Estos enlaces tienen un ancho de banda en general de 9,600 bps, y en ocasiones se comparten estos enlaces conmutando su ancho de banda a otro enlace por horario.

En un principio la red satelital tuvo fundamentalmente propósitos de transmisión de voz, y como valor agregado la posibilidad de transmisión de datos, por esta razón la asignación de canales de datos en el grupo en estos momentos se encuentra saturada. Como se puede observar, las empresas y departamentos que requieren comunicación de datos a las localidades foráneas tienen que utilizar el conmutador, en las líneas digitales que tiene asignado para esos fines.

También se cuenta con esquemas gráficos de las telecomunicaciones que actualmente se tienen, así como esquemas típicos de las terminales VSAT utilizadas en el grupo y la comunicación del Corporativo por la fibra óptica.

Un esquema típico de conexión con el satélite se muestra en la figura 3.2.

Esquema de conexión satelital

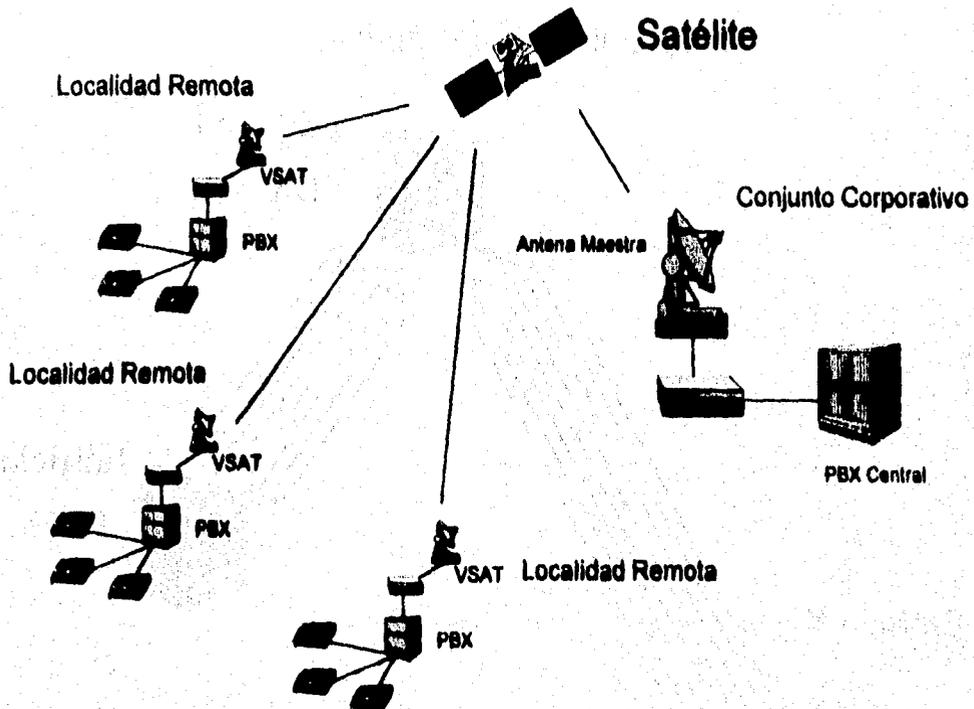


Figura 3.2

Teniendo una red satelital entre localidades foráneas y el Corporativo, se resolvió el problema de comunicación entre sus torres y el Corporativo con la utilización de conmutadores conectados entre sí, para ello se tendió una fibra óptica a cada uno de los edificios para la transmisión, tanto de voz como de datos, que llega del satélite. La distancia máxima de esta fibra entre edificios no supera los 500 mts., este tendido de fibra cuenta con 4 fibras libres para uso futuro. Ver figura 3.3.

Esquema de fibras ópticas

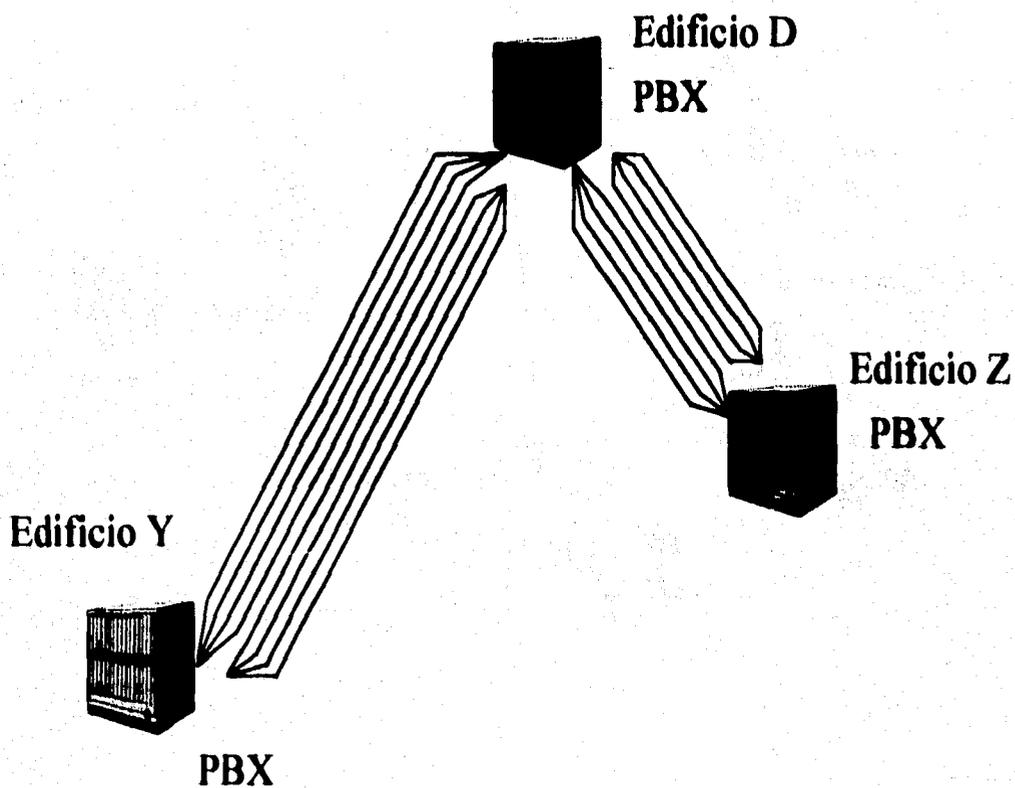


Figura 3.3

Un punto importante es el hecho de no contar con una estructura de Backbone para poder transferir información entre las empresas del grupo. Cuando se requiere este servicio se realiza con disco flexibles.

Paquetes de aplicación.

- Oracle, como base de datos de HP9000 estandarizado formalmente
- Windows, office para trabajos de oficina
- AutoCad, (windows y en estación de trabajo) esta herramienta de diseño está ampliamente difundida y utilizada en el grupo.

Hardware

- HP-9000 como minicomputadoras. En los casos donde se tiene HP3000 se piensa migrar a HP9000.
- PC's en su mayoría equipos HP.
- Tarjetas de red preferentemente de marcas Western Digital, 3com e Intel.
- DTC's de HP como servidores de terminal.

Redes

- Se utiliza generalmente Novell Netware aunque en versiones anteriores a la 4.0
- Topologías Ethernet con cableado estructurado nivel 3 y coaxial delgado, en lo general.

Equipo de comunicación

- Se utilizan concentradores Synoptics y HP.
- En cuanto a enrutadores actualmente se tienen estandarizados los Cisco en sus modelos 2500 y 4000.
- Los conmutadores que se utilizan son ROLM y Meridian de Northern Telecom

Protocolos

- Se utilizan IPX de Novell para la comunicación con estos servidores.
- Comunicación a las HP9000 con TCP/IP

A continuación se presenta una descripción detallada de cada red que integra al corporativo, así como sus necesidades y problemática.

3.4.2 Red Empresa A

El modelo que ha seguido el grupo es el tipo de red que se encuentra en la Torre Y. Esta es la más grande y cuenta con tres subredes, cada una con 2 a 4 servidores Novell. Todo su cableado es estructurado nivel 3 y cuentan con más de 200 usuarios. Esta red cuenta con analizador de protocolo y herramientas de administración como Optivity, cuentan con número de Internet y redes IPX estandarizadas por su matriz en E.U. El esquema de esta red se describe en la figura 3.4 y 3.5.

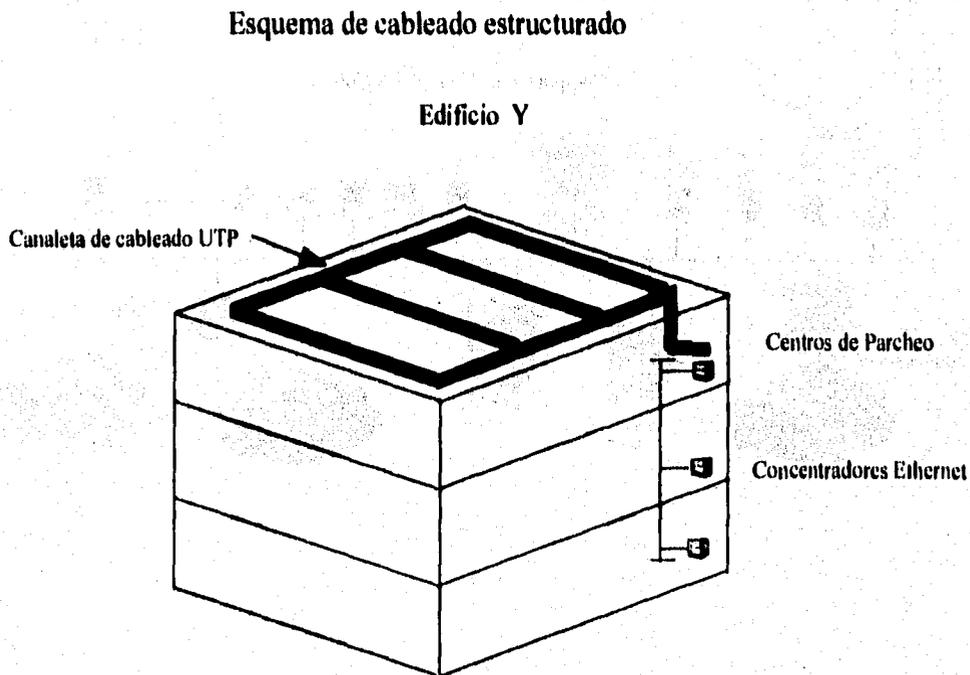


Figura 3.4

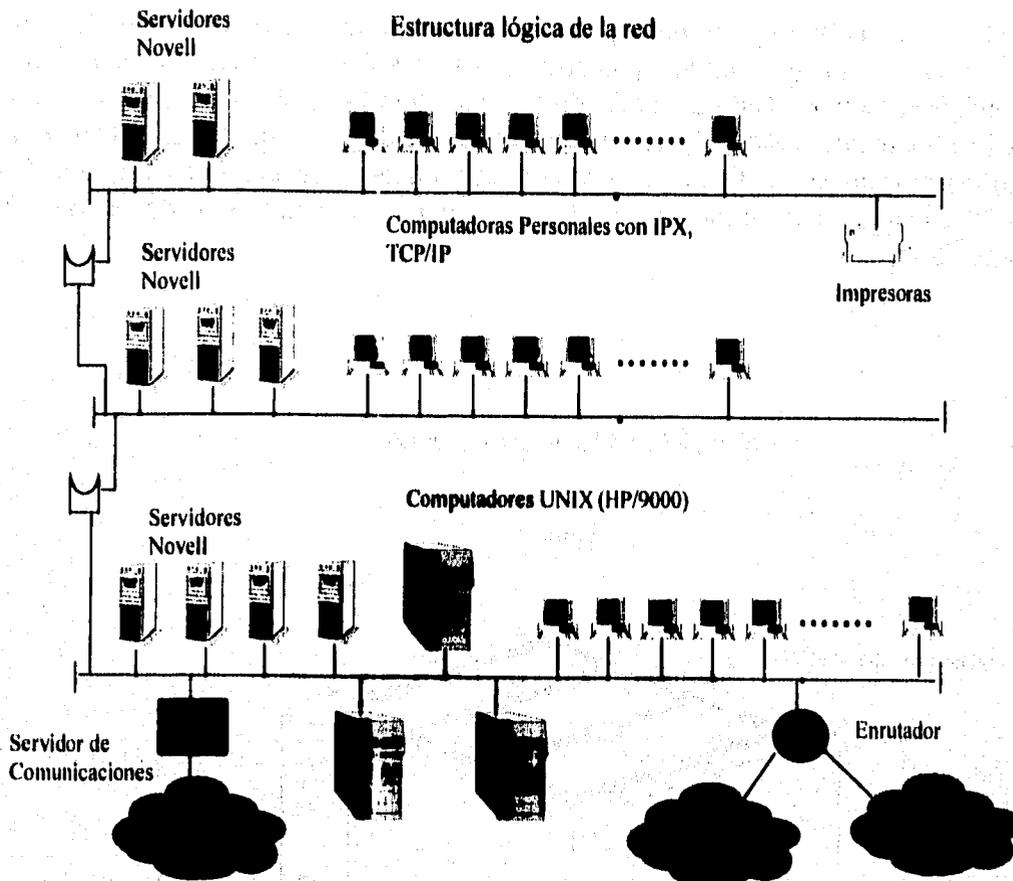


Figura 3.5

Este grupo tiene el requerimiento de videoconferencia, para ello conmutan su ancho de banda satelital cuando requieren 384 Kbps para videoconferencia con EU. Su operación normal es de 64 Kbps para datos con su oficina matriz. En esta empresa se tiene un esquema de interconexión de LANs entre sus localidades, para ello utilizan equipos enrutadores Cisco modelos 2500 y 4000. El esquema se muestra en la figura 3.6.

Esquema de conexión satelital

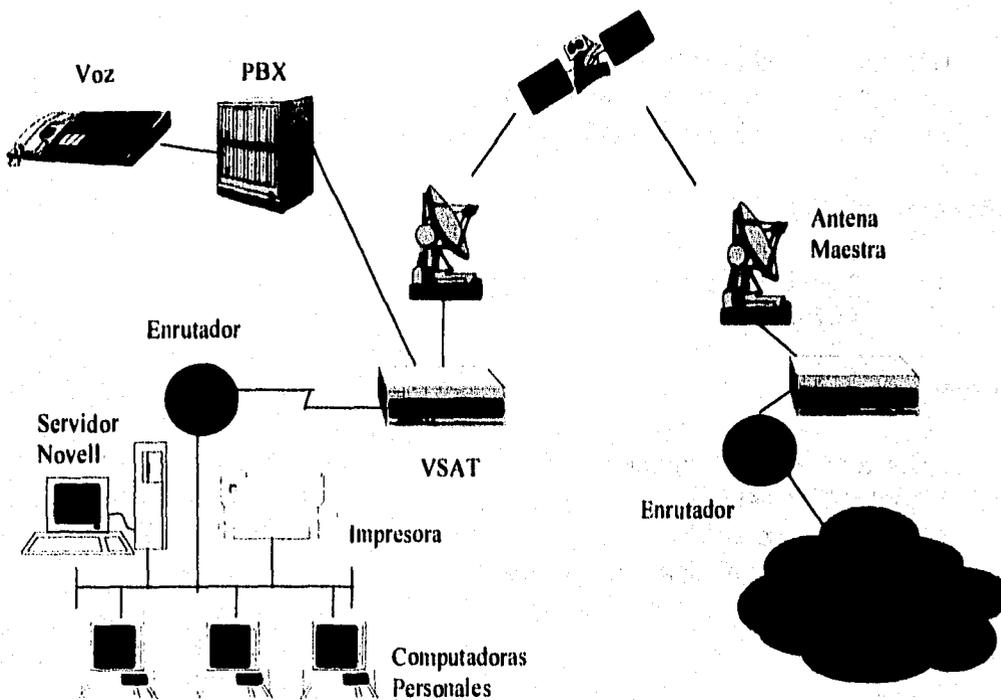


Figura 3.6

ESPECIFICACIONES

Topología Lógica(LAN)

BUS Puenteado

Topología Física

Estrella en los concentradores (LAN)

Bus entre concentradores (LAN)

Multipunto a punto (WAN)

Medio de transmisión

UTP nivel 3 entre estaciones

Coaxial delgado entre concentradores

Satelital con interface RS-449 para WAN

Protocolos de Red

IPX (Novell Netware)

IP (TCP/IP)

Hardware de red

3 Concentradores Synoptics

1 Router Cisco 4000

5 Routers Cisco 2500

1 Servidor de comunicaciones Cubix

Cobertura

Nacional

Acceso a la red

Existe un servidor de comunicaciones Cubix que permite accesos remotos vía enlaces asíncronos.

Número de estaciones

200

Aplicaciones

Servicios de impresión, servidores de archivo, aplicaciones financieras, consultas de abastecimientos, contabilidad.

Seguridad

Actualmente se cuenta con software de seguridad en los servidores Novell y se tiene implementado los servicios de TACACS para accesos de TCP/IP

Necesidades y problemática

- Conectarse con las empresas que consolidan información.
- Videoconferencia.
- Transmisión con otras empresas de imágenes y archivos de gran capacidad.
- Implementar esquemas de seguridad para evitar accesos no autorizados.
- Esquema definido de direccionamiento IP e IPX que no puede cambiarse por su asociación con una empresa americana.
- Tráfico intenso en la red, a corto plazo, previsto por la implantación de un esquema cliente/servidor con un manejador de bases de datos distribuido (Oracle).

3.4.3 Red Empresa B

Esta es la empresa de mayor tamaño dentro del grupo se encuentra localizada en los edificios corporativos. A pesar de ser la más grande del grupo, no es la más avanzada en cuanto a infraestructura computacional se refiere. En la actualidad tiene mayores requerimientos de integración de redes en sus localidades y cuenta con más ancho de banda para interconexión de éstas.

Esta empresa tiene actualmente instaladas 12 redes en sus unidades foráneas y una más en su oficina matriz, cada una de estas redes es de pocos nodos y se instalan por un tiempo límite. Las localidades remotas transfieren archivos sólo a través de paquetes de comunicación asíncrona, es decir de alguna forma sus redes están aisladas unas de otras. El esquema de la red en el grupo corporativo se muestra en la figura 3.7

Esquema de Red Empresa B

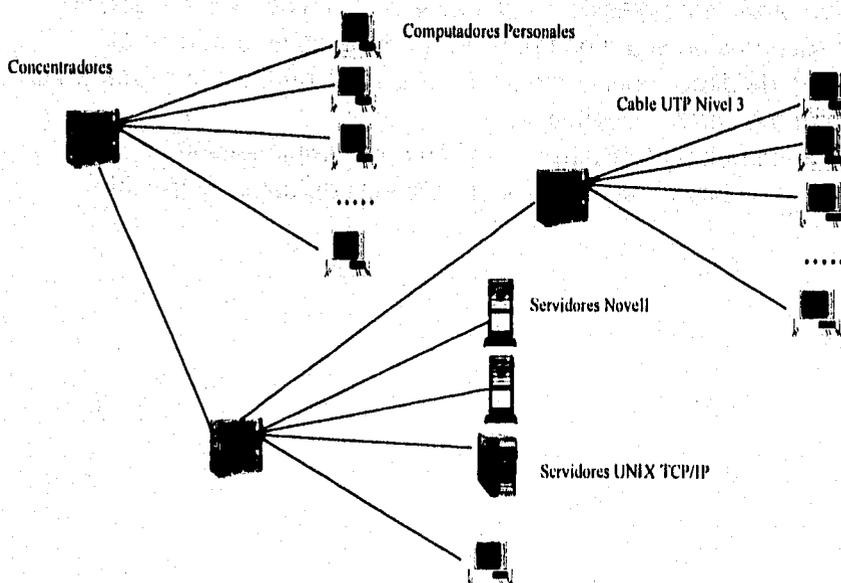


Figura 3.7

Y su diagrama de conexión actual para redes foráneas aparece en la figura 3.8

Esquema de conexión satelital

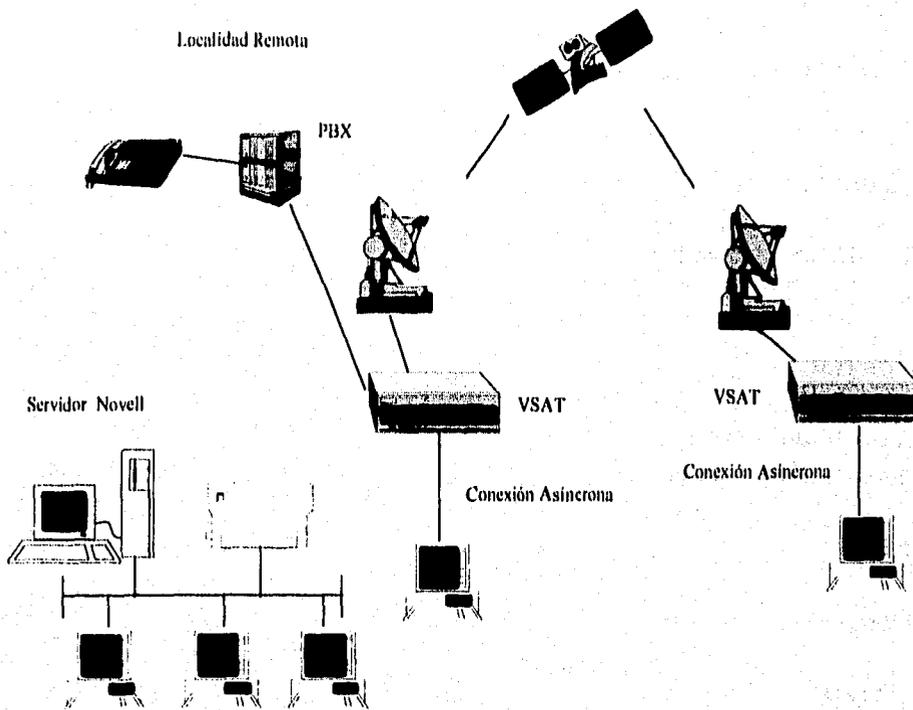


Figura 3.8

ESPECIFICACIONES

Topología Lógica(LAN)

BUS

Topología Física

Estrella en los concentradores (LAN)

Medio de transmisión

UTP nivel 3 entre estaciones

Protocolos de Red

**IPX (Novell Netware)
IP (TCP/IP)**

Hardware de red

**3 Concentradores HP
Tarjetas 3com y novell**

Cobertura

Nacional

Acceso a la red

Sólo el de las conexiones directas a la red

Número de estaciones

80

Aplicaciones

**Servidor de impresión
Correo
Servidor de archivos**

Seguridad

Sólo está implementada la seguridad que proporcionan los servidores UNIX y Novell

Necesidades y problemática

- Proporcionar accesos.
- Comunicación de datos con sus localidades remotas.
- Integración de secciones localizadas en diferentes edificios.
- Sólo doce localidades remotas cuentan con red local.

3.4.4 Red Empresa C

Es una empresa mediana dentro del grupo, sólo se comunica fuera del corporativo con dos empresas remotas. Parte de su estructura tecnológica está basada en una red inalámbrica, que presenta limitantes de distancia responsables del aislamiento de la empresa. Por el monto de la inversión se plantea integrar esta red como parte del backbone a través de un puente. La estructura de la red se muestra en la figura 3.9

Esquema de Red Empresa C

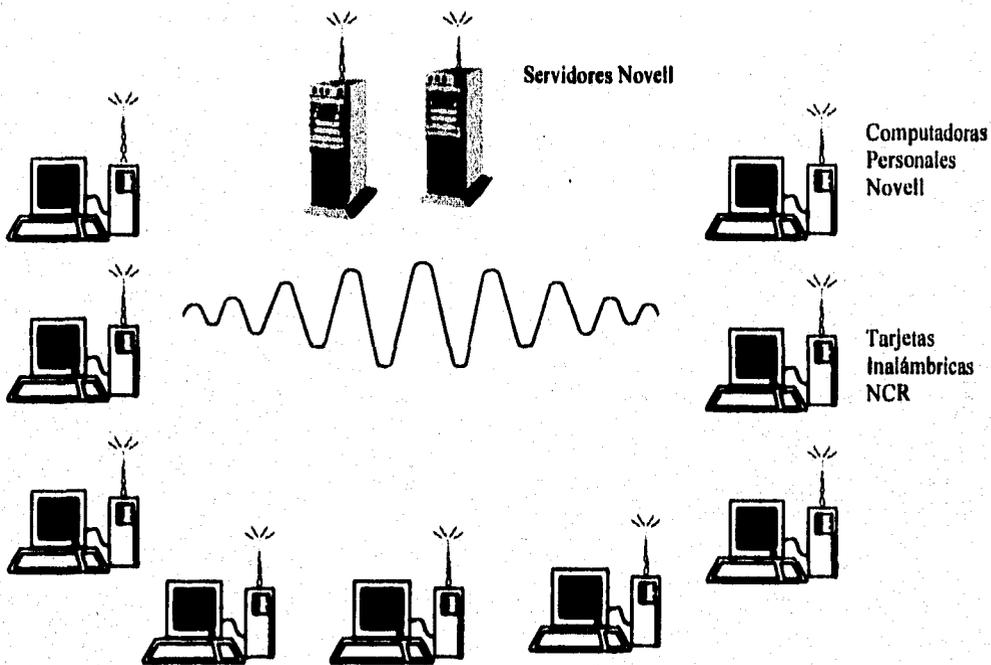


Figura 3.9

ESPECIFICACIONES

Topología Lógica(LAN)

BUS

Topología Física

BUS (LAN)

Medio de transmisión

Microondas

Protocolos de Red

IPX (Novell Netware)

Hardware de red

Tarjetas inalámbricas NCR

Cobertura

Nacional

Acceso a la red

Ninguno

Número de estaciones

20

Aplicaciones

Servidor de impresión
Correo
Servidor de archivos

Seguridad

Cuenta con la seguridad implementada en los Servidores Novell

Necesidades y problemática

Se tiene necesidad de crecimiento, pero debido a los altos costos de la tecnología de las tarjetas inalámbricas este crecimiento necesita replantearse en términos de una tecnología más barata que permita comunicación con sus localidades remotas.

Además esta empresa está valuando estaciones de diseño gráfico e imágenes con estaciones localizadas en diferentes edificios que demandarán bastante ancho de banda.

3.4.8 Red Empresa D

Dentro de las empresas que radican en localidades foráneas sólo una reside en forma fija y es la única que cuenta con servicios de cómputo además de los servidores de archivos o de impresión. La empresa D en Querétaro realiza sus aplicaciones en dos equipos HP9000 (Unix TCP/IP), pero no existe interconexión con algún otro equipo dentro del grupo. El esquema de interconexión de esta empresa se refleja en la figura 3.10.

Esquema de la Red de la Empresa D

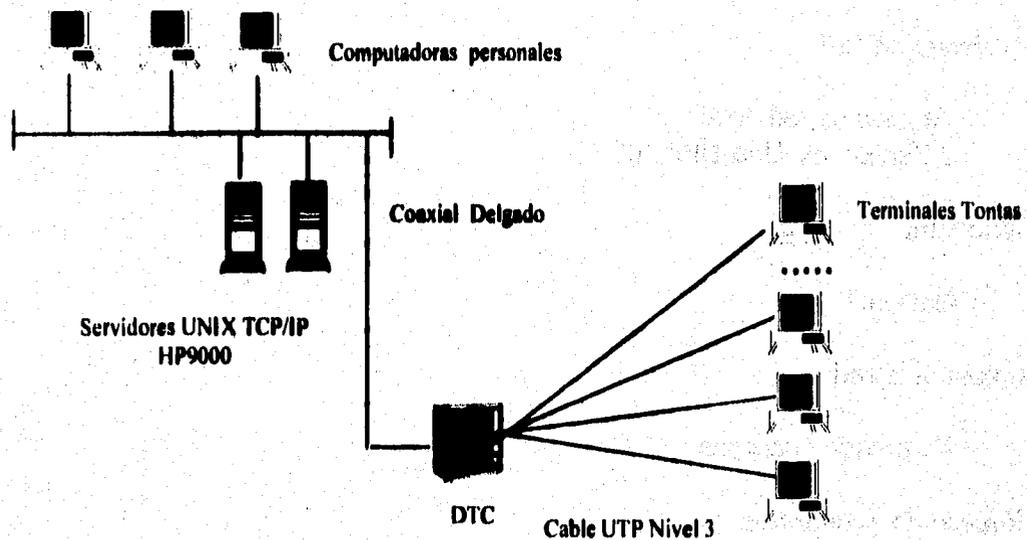


Figura 3.10

ESPECIFICACIONES

Topología Lógica(LAN)

BUS

Topología Física

Bus entre concentradores (LAN)

Medio de transmisión

Coaxial delgado entre concentradores

Protocolos de Red

IP (TCP/IP)

Hardware de red

**Tarjetas de red Intel
2 Servidores Unix HP/9000**

Cobertura

Nacional

Acceso a la red

No existen accesos

Número de estaciones

60

Seguridad

Se cuenta únicamente con la seguridad de los servidores Unix

Necesidades y problemática

Es necesario concentrar información de diferentes áreas en el Corporativo.

3.4.5 Red de Finanzas

Esta red es realmente pequeña pero de gran importancia debido a las operaciones que realiza. A pesar de no tener comunicación foránea todas las empresas consolidan aquí la información económica. La estructura de la red se muestra en la figura 3.11.

Esquema de Red de Finanzas

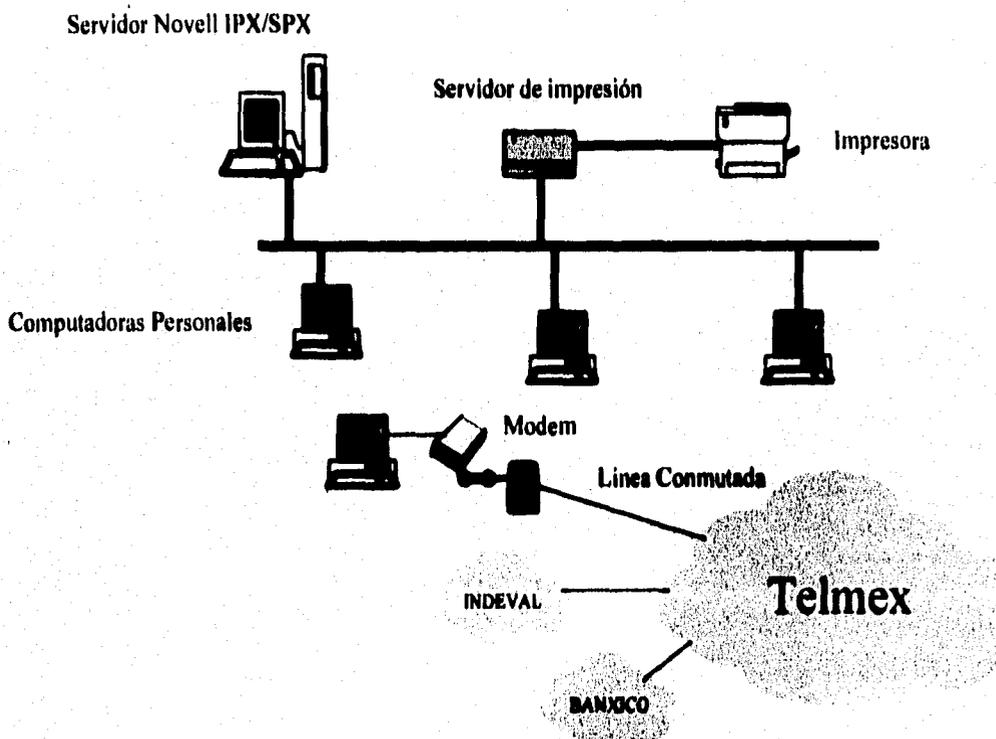


Figura 3.11

ESPECIFICACIONES**Topología Lógica(LAN)**

BUS

Topología Física

BUS (LAN)

Medio de transmisión

Coaxial delgado

Protocolos de Red

IPX (Novell Netware)

Hardware de red

Tarjetas 3com y Novell

Cobertura

Local

Accesos a la red

Por línea conmutada se tiene acceso a diferentes bancos y casas de bolsa

Número de estaciones

18

Aplicaciones

Servidor de impresión

Correo

Servidor de archivos

Seguridad

Sólo se tiene los esquemas de seguridad de los servidores Novell

Necesidades y problemática

- Interconectividad con todas las entidades de la red.
- Mejores y más confiables accesos con INDEVAL (Bolsa Mexicana de Valores) y BANXICO (Banco de México).

3.4.7 Red de Administración

En esta red se concentran los equipos de cómputo más grandes del grupo, los cuales manejan información de muchos tipos. Esta red pretendió ser el primer intento de backbone dentro del grupo y está constituido por 4 equipos HP9000 a los cuales se tiene acceso a través de terminales asincrónicas conectadas a un servidor de terminales (DTC). Ver figura 3.12.

Esquema de la Red de Administración

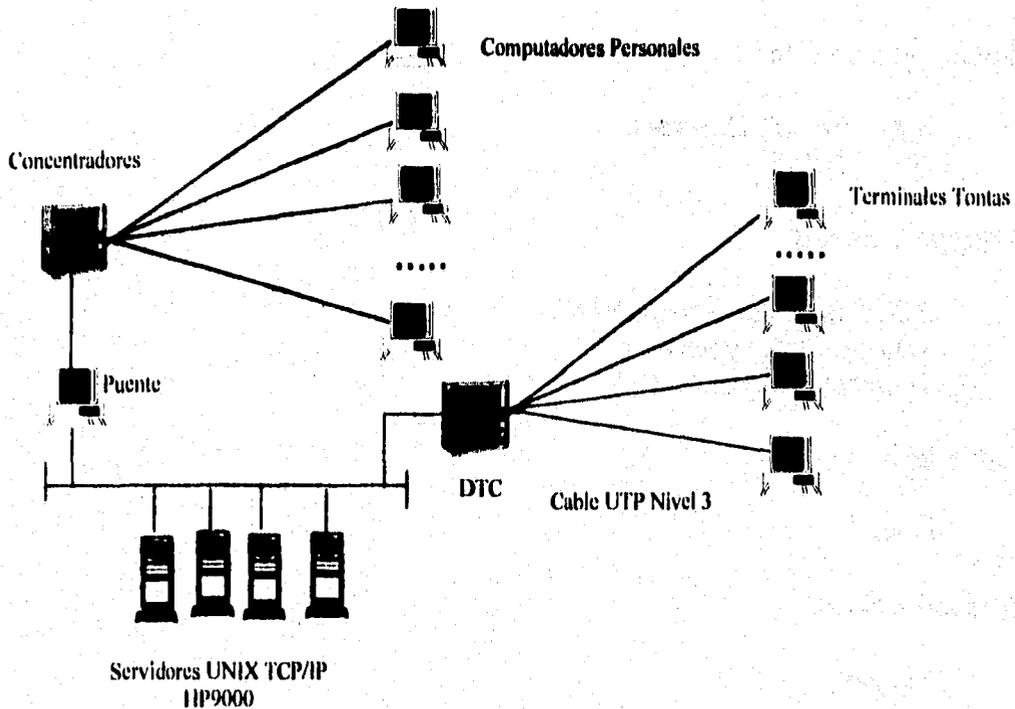


Figura 3.12

ESPECIFICACIONES

Topología Lógica(LAN)

BUS

Topología Física

BUS (LAN)

Medio de transmisión

Coaxial delgado
UTP sin certificación

Protocolos de Red

IPX (Novell Netware)
IP TCP/IP

Hardware de red

2 DTC (servidor de terminales)
Tarjetas 3com y novell
Terminales asíncronas

Cobertura

Local

Acceso a la red

Ninguno

Número de estaciones

200 terminales
23 estaciones

Aplicaciones

Servidor de impresión
Correo
Servidor de archivos

Seguridad

Sólo se cuenta con el esquema de seguridad del servidor Novell y Unix.

Necesidades y problemática

El problema de esta empresa es poder integrar servicios de emulación de terminal (VT100) para acceder sus equipos HP9000 y substituir las terminales asíncronas. Se tiene un gran número de estas terminales y se plantea substituir las por equipos PC. Además se planea implementar a mediano plazo una aplicación Cliente/Servidor que se ejecutará en la red por lo que es necesario considerar soportar este tráfico.

Este departamento también comparte información con todas las entidades de la empresa por lo que es necesario que pueda acceder las redes de toda la empresa.

3.4.8 Red de Recursos Humanos

Esta área cuenta con una pequeña red de computadoras unidas por coaxial, conectadas a la red de administración por medio de un bridge. Esta área lleva el control de la nómina global, efectúa trámites ante autoridades y pago de impuestos. Tiene mucha transferencia de información con otras áreas ya que éstas proporcionan la información de asistencia que se procesa quincenalmente. Esta información es transmitida con discos y algunas entidades que tienen conexión a través de la red de administración entregan su información por medio de Novell. La estructura de la red se muestra en la figura 3.13.

Esquema de la Red de Recursos Humanos

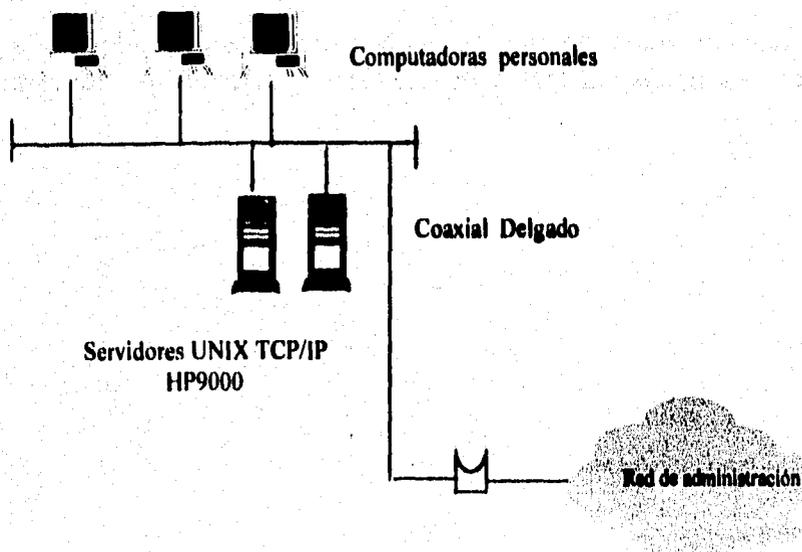


Figura 3.13

ESPECIFICACIONES**Topología Lógica(LAN)**

BUS

Topología Física

BUS (LAN)

Medio de transmisión

Coaxial delgado

Protocolos de Red

IPX /SPX (Novell Netware)

Hardware de red

Tarjetas Wenster Digital

Cobertura

Local

Acceso a la red

Ninguno

Número de estaciones

26

Aplicaciones

Servidor de impresión

Correo

Servidor de archivos

Seguridad

Cuenta con el esquema de seguridad de Novell

Necesidades y problemática

Esta es empresa comparte información con todas las entidades del grupo, sin embargo el proceso de comunicación se realiza con discos flexibles.

Se planea implementar un sistema Cliente/Servidor, con un manejador de bases de datos distribuido (Oracle), en toda la empresa para consolidar la información.

3.4.9 Red de Telecomunicaciones

Como se había mencionado antes, esta entidad presta servicios de carrier a las demás empresas a través de una red satelital, también presta servicios en la instalación de tarjetas y software de red. Es la encargada de proporcionar los estándares y es la única red que cuenta con token ring como estructura de red. Cuenta con una estructura para atención de usuarios así como diferentes plataformas de monitoreo y administración por lo que es un centro ideal para atender y administrar la red corporativa. Tienen actualmente una red basada en OS/2 pero se está migrando a Windows NT de hecho se tiene un servidor corporativo de correo basado en NT con Netbeui como estándar. El diagrama de red es como sigue:

Esquema de Red de Telecomunicaciones

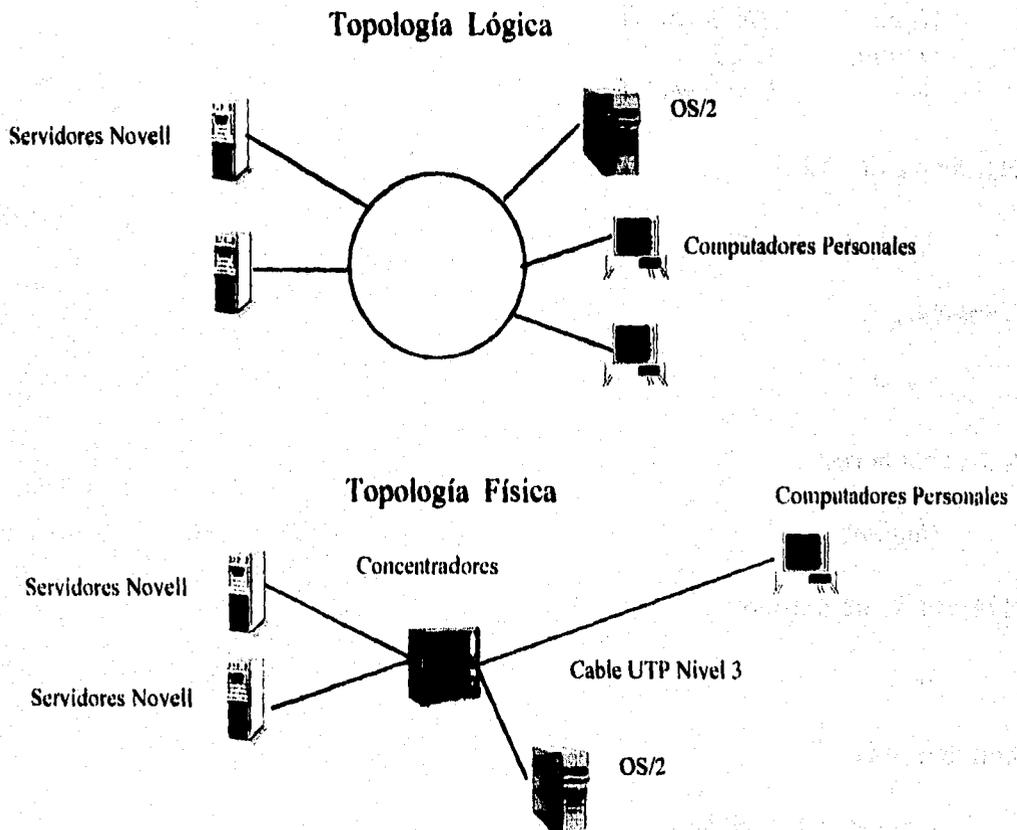


Figura 3.14

ESPECIFICACIONES**Topología Lógica(LAN)**

Ring

Topología Física

Estrella

Medio de transmisión

UTP nivel 3

Protocolos de Red

Netbeui	Windows NT
Netbios	OS/2
IP	Windows NT

Hardware de red

Tarjetas Proteon

Cobertura

Local

Acceso a la red

Ninguno

Número de estaciones

24

Aplicaciones

Servidor de impresión
Correo
Servidor de archivos

Seguridad

Esta empresa sólo cuenta con los servicios de seguridad de Windows NT

Necesidades y problemática

Se está promoviendo el uso de herramientas de diseño en plataformas Unix, que consumen una gran cantidad de ancho de banda por lo que es conveniente considerar estas cargas para el diseño de la Red.

Este departamento está promoviendo una conexión a Internet para acceder información en el extranjero que pueda apoyar los diferentes proyectos de las empresas dentro del grupo.

3.5 Necesidades y problemática.

Necesidades:

- Integrar las empresas con sus localidades remotas
- Interconectar las redes de las empresas del grupo
- Se necesita un plan de direccionamiento IP e IPX general que permita una interconexión transparente
- Incorporar, a futuro, servicios de videoconferencia en algunas empresas del grupo
- Conectar el grupo a Internet con la finalidad de aprovechar la información más reciente en cuanto a tecnología que se genere en el mundo
- Establecer estándares y lineamientos corporativos en cuanto a sistemas
- Implantar un correo electrónico para toda la corporación

Problemática:

- Existen aplicaciones de tráfico intenso como sistemas de diseño que operan bajo estaciones de trabajo UNIX
- Al usar Oracle se pretende utilizar una plataforma cliente/servidor que demandará más consumo de ancho de banda en las redes
- En este momento se utilizan líneas digitales de los conmutadores para hacer enlaces de datos, pero en general la red remota de información plantea ser una red que esté enfocada a VOZ por lo que es necesario balancear esta tendencia.

3.6 Visión a corto y mediano plazo.

Un aspecto importante es prever el crecimiento, como se muestra en la tabla 3.1 existen muchos usuarios sin PC que serán integrados a mediano plazo por lo que el diseño tiene que permitir un crecimiento escalable sin degradar el desempeño de la Red.

Es importante considerar utilerías de Multimedia y Videoconferencia ya que se piensa incorporar estas aplicaciones para desarrollar algunos proyectos dentro del grupo.

Existen planes para migrar redes Novell a esquemas con Windows NT sobre IP por su mejor comportamiento sobre la red WAN.

Debe desarrollarse una estructura de seguridad que permita que los puertos asignados a una empresa sólo accedan la información a la que deberían tener acceso.

CAPITULO 4 REQUERIMIENTOS DE LA RED

En este capítulo se exponen las diferentes soluciones que pueden satisfacer las necesidades de la empresa, además se analizan los beneficios y las desventajas de los diferentes tipos de red y como ATM , de acuerdo al estudio, resuelve mejor la problemática de la empresa.

4.1. Tipo de Red

4.1.1 Esquema LAN

En este capítulo se presentan las tres diferentes opciones de topologías de Red LAN (Red de Area Local) y los esquemas de conexión de equipos que solucionan las necesidades de la empresa.

El análisis del tipo de red está comprendido en:

- Red de conmutación Ethernet
- Red distribuida FDDI
- Red de Conmutación con ATM

4.1.1.1 Red de conmutación Ethernet.

Los productos basados en este esquema ofrecen un ancho de banda de 10 Mbps y tienen el potencial de multiplicar el ancho de banda de Ethernet en forma casi ilimitada.

Esta tecnología tiene muchas variantes, puesto que cada desarrollador adopta la suya, pero en su mayoría ofrecen interconexión con los equipos y medios de comunicación que ya se encuentran instalados, la utilidad de estos equipos es el interconectar redes locales cuya interacción no demande un medio de comunicación de mayor ancho de banda que 10 Mbps, por lo tanto para la empresa, esta tecnología no cubre sus requerimientos a futuro, por lo cual no se ahondará en su estudio, pero sí se considera en la evaluación de tecnologías que a continuación se presenta.

Se propone una conexión de 3 conmutadores Ethernet a los diferentes nodos concentradores como lo muestra la figura 4.1.

Esquema de Conmutación Ethernet

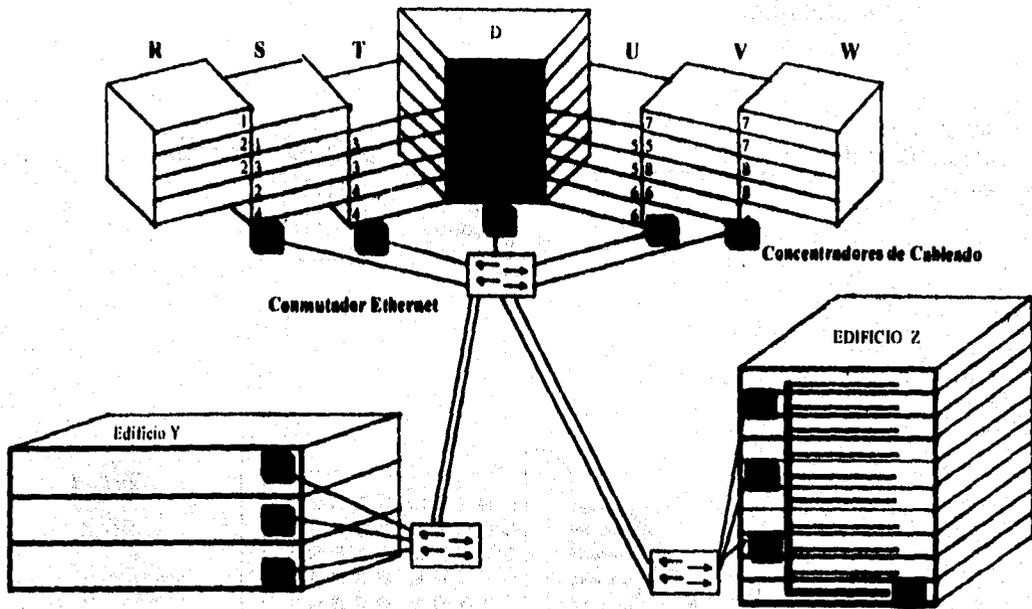
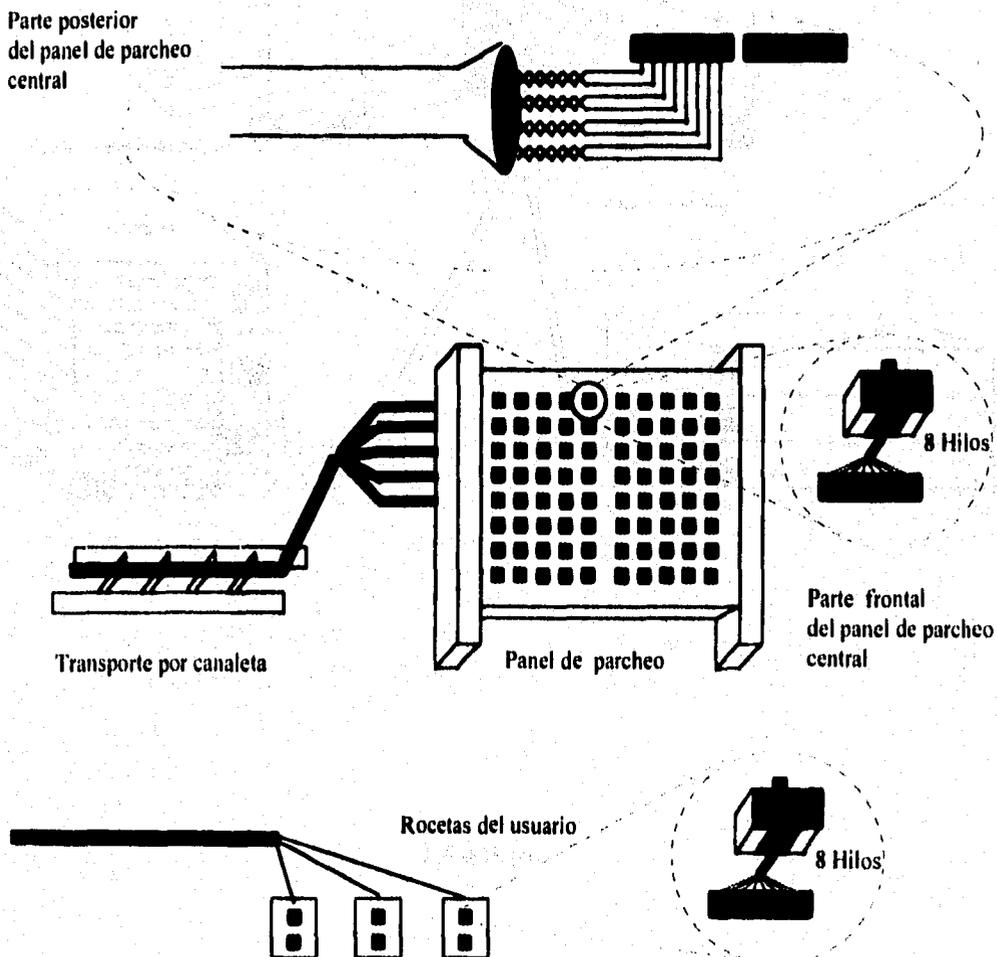


Figura 4.1

Medio de transmisión

- UTP nivel 5 para la conexión entre los Concentradores y las computadoras personales (ver figura 4.2).
- Fibra Óptica Multimodo para la conexión entre los Conmutadores Ethernet.
- UTP nivel 5 para la conexión entre los concentradores y los conmutadores.

**Figura 4.2**

Velocidad

En esta tecnología la velocidad es de 10 Mb/s., no ofrece conexión a través de Wan.

Distribución del ancho de banda

Según el esquema planteado en la figura 4.1 se asignan 10 Mb/s a cada concentrador. De allí los concentradores ofrecen puertos de 10 Mb/s que se distribuyen según la tecnología de CSMA/CD en forma aleatoria y por demanda del medio.

Elementos

Se necesitan 12 concentradores que se distribuyen de la siguiente forma:

- Cinco concentradores en el conjunto Corporativo.

Cada concentrador atenderá seis niveles de los edificios en el conjunto Corporativo.

- Cuatro concentradores en el Edificio Z.

En el edificio Z se necesitará un concentrador que se ocupe de tres niveles

- Tres concentradores en el Edificio Y

Cada concentrador se ocupará de cada nivel.

Además se necesitará :

- Tres conmutadores Ethernet (con 8 puertos de entrada)
- Cuatro Fibras Multimodo Rematadas en ST
- Cuatro convertidores de Medio ST-UTP (FOIL)
- Cinco concentradores de Fibra

Costos Promedio

Equipo	Costo / Unidad	Número	Costo / total
Conmutadores Ethernet	20,000 Dlls	3	60,000 Dlls
Concentradores Ethernet	25,000 Dlls	12	300,000 Dlls
FOIL ST/UTP-5	1,000 Dlls	4	4,000 Dlls
Concentradores Fibra (12 puertos)	2,500 Dlls	3	7,500 Dlls

Costo Total **371,500 Dlls**

Crecimiento

El crecimiento está determinado por los puertos libres de los conmutadores Ethernet (3 puertos). En los concentradores el crecimiento es por módulos de hasta 24 puertos Ethernet. Este esquema tiene la ventaja de aplicar en forma escalable, es decir, por más elementos que se incluyan a la Red el ancho de Banda sigue siendo 10 Mbps.

Limitantes

La limitante principal consiste en el bajo ancho de banda (10 Mbps), además no se tiene redundancia de equipo, es decir, si falla un Conmutador Ethernet los restantes en la Red no podrían tomar sus funciones. No se tendría la posibilidad de manejar video y voz sobre la misma Red.

4.1.1.2 Red Distribuida FDDI.

Es la tecnología existente más robusta, necesitaron ocho años para finalizar el estándar, resultando definitivamente, la tecnología de red de alta velocidad más tolerante a fallas y manejable que actualmente se encuentra disponible.

Tendencias

En la actualidad los estándares FDDI de ANSI e ISO no utilizan algoritmos para formar tablas de puentes en base a "source routing", lo que abre las puertas a esquemas incompatibles entre los diversos fabricantes.

La interoperabilidad es factor muy importante cuando se requieren implantar "backbones", especialmente si se considera que no existe un estándar para el Token Ring "source bridging" sobre FDDI.

Los puentes Ethernet no son problema porque FDDI direcciona de manera transparente los datos entre Ethernet y FDDI, agregando a esto el hecho de que todos los fabricantes lo realizan de la misma manera. Sin el estándar de source routing muchos fabricantes han implantado soluciones por sí mismos, muchos han optado por las especificaciones del 802.5, otros encapsulan los paquetes dentro de FDDI dando como resultado un bajo desempeño. Sin embargo un nuevo estándar se está definiendo para especificaciones de Token Ring Source Bridging sobre FDDI denominado FDDI MAC-2. El estándar FDDI-II contempla soportar videoconferencias y multimedia, sin embargo todavía no hay productos en el mercado. Todos los grandes proveedores de equipo de redes, ofrecen entre su línea de productos la tecnología FDDI, y es común la interconexión entre componentes FDDI de diferentes proveedores.

El nivel de soporte a la tecnología FDDI en México y otros países es de un nivel aceptable, ya que en los últimos cuatro años las organizaciones han utilizado esta tecnología para conformar sus "backbones" corporativos, por lo que en la actualidad hay una buena base instalada de este tipo de redes. Y el dominio de la tecnología en México se encuentra completamente consolidado, sin embargo no se observan esfuerzos en la implantación de FDDI-II, en contraparte con la tecnología ATM.

Para esta solución se plantea tener un esquema con FDDI para unir los nodos concentrados a través de fibra óptica. Ver figura 4.3

Esquema de Red con FDDI

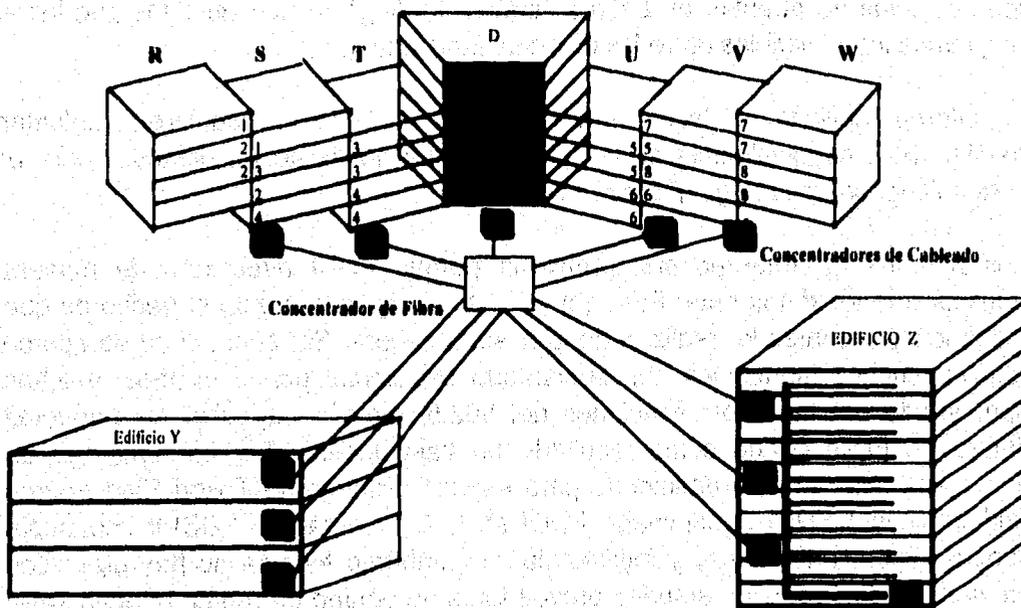


Figura 4.3

Medio de transmisión

- UTP nivel 5 para la conexión entre los concentradores y las computadoras personales (ver figura 4.2).
- Fibra Óptica Multimodo para la conexión entre los concentradores Ethernet.

Velocidad

La velocidad de FDDI es de 100 Mb/s.

Distribución del ancho de banda

El ancho de banda por principio de diseño, según la figura 4.3, se distribuye entre los 12 concentradores. Y cada servidor o elemento incorporado al "Backbone" de la Red automáticamente distribuye el ancho de banda entre más estaciones.

Elementos

12 Concentradores con interface FDDI (distribución en figura 4.3). Un tendido de fibra Multimodo de cuando menos 4 hilos entre los concentradores, y 2 hilos de respaldo. Tomando en cuenta que son 12 concentradores se necesitan 62 fibras rematadas en ST. En total se necesitan :

- 27 concentradores de fibra
- 24 cables de ST a MIC

Costos

Equipo	Costo / Unidad	Número	Costo / total
Concentradores Ethernet, con interface FDDI	37,000 Dlls	12	444,000 Dlls
Concentradores de Fibra (12 puertos)	1,000 Dlls	12	12,000 Dlls
Costo Total			456,000 Dlls

Flexibilidad

No se tiene limitante de un equipo concentrador. Tiene respaldo definido por topología al utilizar la funcionalidad de wrap, o incluso existe la posibilidad de instalar equipos de "bypass óptico" que evitarían la posibilidad de que el anillo se segmente si más de dos dispositivos fallan concurrentemente.

Crecimiento

Las opciones de crecimiento son sólo limitadas por la distribución del ancho de banda, ya que si se pretende incorporar un concentrador más, sólo hay que incorporarlo al anillo.

Limitantes

Las limitantes principales se refieren a que no es escalable en equipos, ya que por cada equipo nuevo se degrada el performance. Tampoco es escalable en distancia ya que no se permite tener una distancia total en fibra mayor a 2 Km. También tiene limitantes de interconectividad ya que algunos vendedores de equipo pueden tener diferentes implementaciones de SRB (al no implementar enrutamiento).

4.1.1.3 Red de conmutación con ATM.

Tendencias

ATM permite mezclar voz, video y transmisión de datos en la misma infraestructura de comunicación. Se espera que ATM sea el gran unificador de la mayor parte de infraestructura de comunicación (voz, video y datos) y el mayor unificador de los modos de red (WAN, LAN, remotas y móviles). Hay dos grupos de propositores de ATM: ATM WAN Y ATM LAN; este último ha tenido mayores progresos sacando mejores productos al mercado. Las tendencias son el tener Concentradores de ATM LAN, combinados con los Concentradores y Enrutadores actuales, multiplexores de E1 y T1, PBXs.

Otros aspectos a considerarse es que las primeras redes de gran escala conectan terminales a mainframes y minicomputadoras. Estas aplicaciones son todavía importantes, aun en la interred, donde la emulación de terminal de Unix continua utilizándose. Para estas aplicaciones no se requiere de conmutación de paquetes.

Actualmente la tecnología de ATM, se encuentra resolviendo problemas de enrutamiento y confiabilidad en el servicio de tráfico en tiempo real. ATM no es un estándar todavía. Muchas de las computadoras actuales no son capaces de manejar transmisiones de ATM, de igual forma existen algunas incompatibilidades para el manejo de protocolos como TCP/IP y su protocolo de administración SNMP, sobre todo en los componentes finales que tendrán que acoplarse para la conmutación de paquetes.

Son tres los principales proveedores de equipos ATM: Fore Systems, Synoptics Communications y Network Equipment Technologies; los grandes proveedores de enrutadores como son Wellfleet Communications y Cisco Systems tienen menos tiempo de haber adoptado ATM, y los productos de ATM que actualmente ofrecen están generalmente en su etapa Beta o se encuentran en sus primeras versiones.

En México por el momento no existe un número representativo de organizaciones que han utilizado la tecnología ATM, por lo que no se cuenta con un nivel de soporte aceptable, y el dominio de la tecnología no es suficiente; en los países donde ya se ha empezado a instalar equipos basados en la tecnología ATM, se recomienda utilizar equipo de un mismo proveedor, ya que en la actualidad no se ha logrado la convivencia de equipos ATM entre diversos proveedores.

Este tipo de red contempla el uso de un Conmutador ATM como nodo central y los nodos concentradores conectados con fibra óptica. Ver figura 4.5.

Medio de transmisión

- UTP nivel 5 para la conexión entre los Concentradores y las computadoras personales (ver figura 4.2).
- Fibra Óptica Multimodo para la conexión entre los Concentradores Ethernet y los Conmutadores ATM.
- Fibra Óptica Multimodo para la conexión entre los Conmutadores ATM.

Velocidad

Esta tecnología ofrece hasta 2 Gb/s, pero en términos comerciales para implementación en LAN se tienen comúnmente a 155 Mb/s.

Distribución del ancho de banda

Esta tecnología cumple con el cometido de dedicar 155 Mb/s a cada conexión con el Conmutador, teniendo sólo como limitante la velocidad del backplane. Estas propiedades permiten agregar dispositivos sin degradación de la velocidad en un enlace determinado.

Esquema de Conmutación ATM

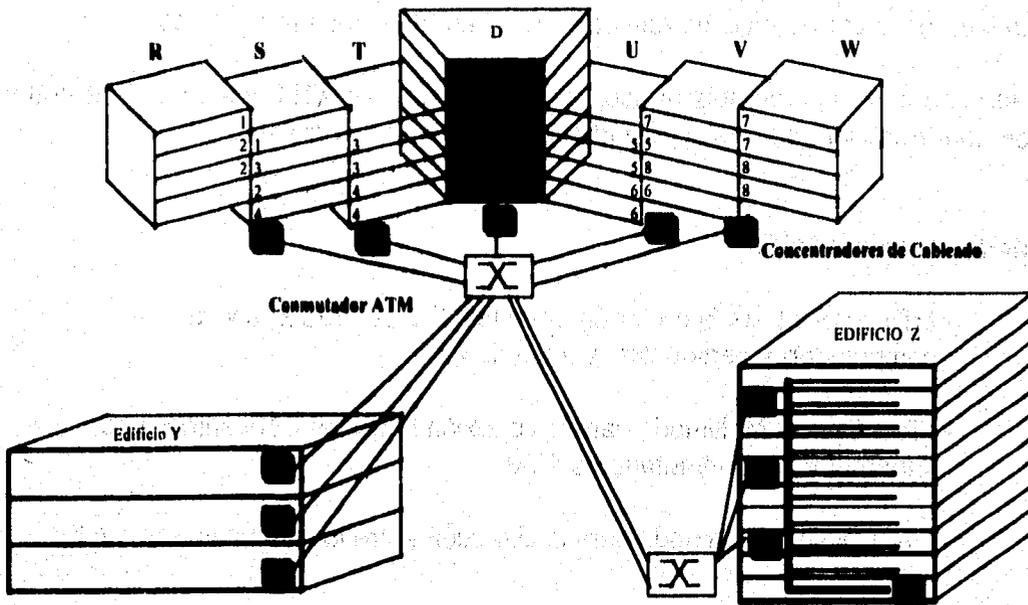


Figura 4.5

Elementos

Dos conmutadores ATM de 16 puertos cada uno, para redundancia.
 Doce concentradores con puertos de ATM.
 54 fibras Multimodo.
 9 concentradores de fibra rematados en ST.
 18 conectores ST-SC.

Flexibilidad y crecimiento

Esta tecnología es totalmente escalable en equipos y en distancia. Soporta de manera natural la conexión a WAN de tres diferentes formas: ATM, SMDS, Relay. Permite utilizar el mismo canal para voz y video. Proporciona una velocidad que supera a FDDI y Fast-Ethernet.

Costos

Equipo	Costo / Unidad	Número	Costo / total
Conmutadores ATM	30,000 Dlls	2	60,000 Dlls
Concentradores Ethernet, con interface ATM	37,000 Dlls	12	444,000 Dlls
Concentradores de Fibra	1,000 Dlls	12	12,000 Dlls

Costo Total **516,000 Dlls**

Limitantes

No tiene en forma intrínseca mecanismos de respaldo por lo que es necesario poner un equipo completo como respaldo del otro. Utiliza fibra que puede resultar un medio de transmisión caro. Existe un elemento Concentrador que impone limitantes de conexión por el número de puertos. Algunos puntos de la tecnología no están estandarizados del todo.

4.1.2 Esquema WAN

El esquema WAN de la red está basado en dos premisas fundamentales :

- La utilización de la Red Satelital existente
- La interconectividad de las Localidades Remotas al Backbone Corporativo.

Para cumplir estos requerimientos podemos considerar como base el esquema utilizado por la Empresa A. Este esquema consiste en la utilización de un Enrutador central que se interconectará por una interface al Backbone de la Red y por otra a la red satelital. En la localidad remota existirá un enrutador pequeño que en una interface se conectará a la Red Satelital y por otra interface se conectará a la red local de la localidad remota.

El router central deberá tener tantas interfaces seriales como localidades remotas que tengan capacidad de conectarse a las interfaces físicas (RS449, V.35 con interface Winchester) de la Red satelital. También debe tener conexión directa a Ethernet, FDDI o ATM.

Este esquema se muestra en la Figura 4.6

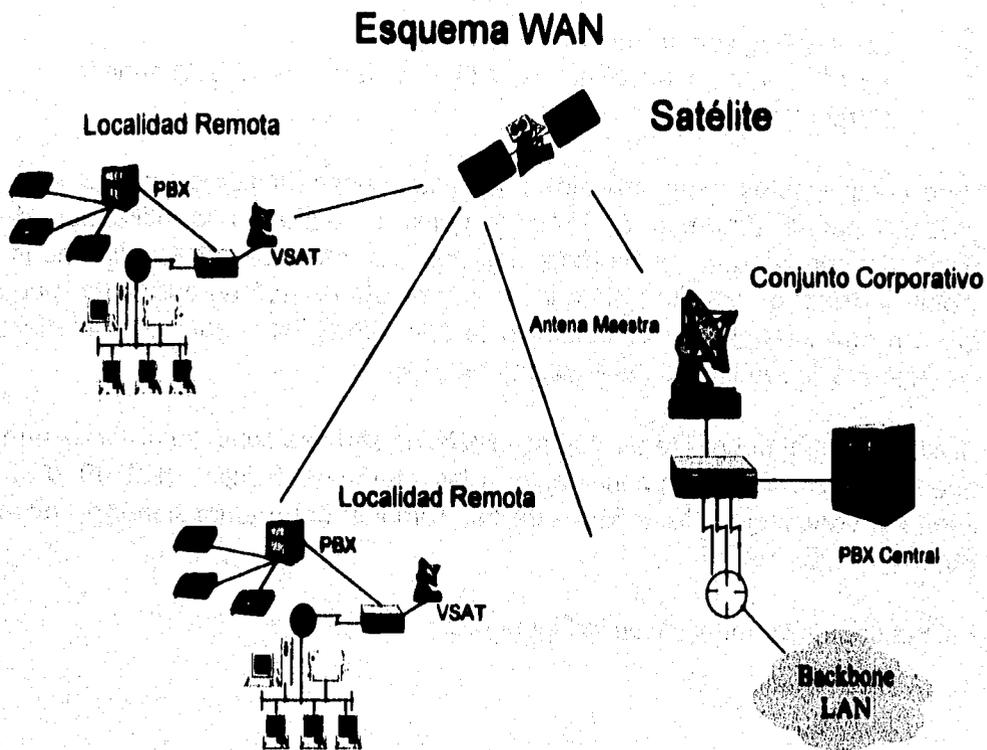


Figura 4.6

4.1.3 Otros Accesos

En este aspecto la Red debe contemplar los accesos a INDEVAL, BANXICO e Internet así como la posibilidad de acceder la Red desde una línea conmutada a través de la red de TELMEX.

INDEVAL, BANXICO e Internet tienen redes TCP/IP y conectan clientes a través de protocolos de enrutamiento EGP o BGP, por lo que el enrutador debe manejar estos protocolos de Enrutamiento.

Para el acceso por línea conmutada hay que considerar que los servidores que se accederán son:

Novell (IPX/SPX)
UNIX (TCP/IP)
Windows NT (Netbeui)
Comunicación Asíncrona

El Servidor de comunicaciones que se integre deberá manejar, a través de comunicación asíncrona, estos protocolos de red. El esquema para los accesos remotos se muestra en la Figura 4.7.

Esquema WAN

Otros Accesos

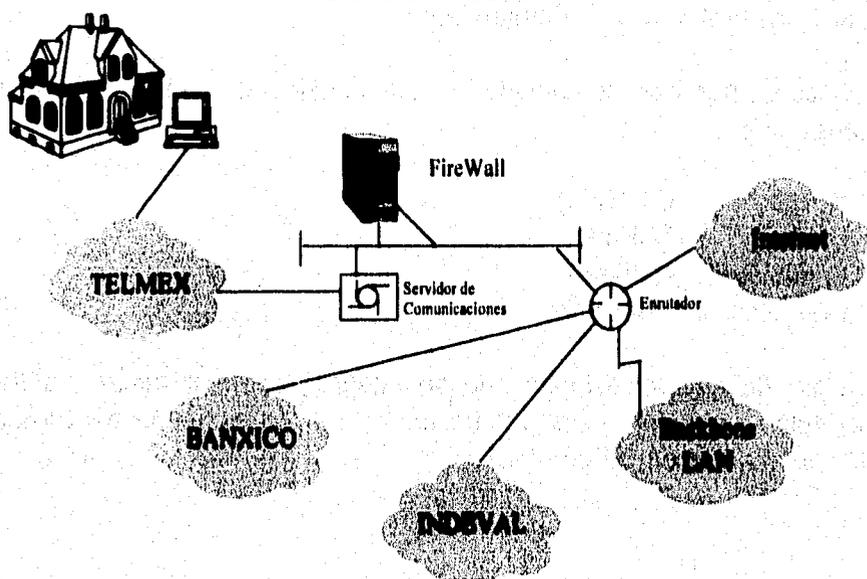


Figura 4.7

4.2 Disponibilidad en la red

El análisis de la disponibilidad de la Red está dividido en niveles para evitar que algunos promedios afecten las conclusiones.

De forma anual la compañía no trabaja los 365 días completos y además no realiza operaciones críticas todos los días. Debido a esto, tenemos que eliminar los fines de semana y los días festivos, esto es :

$$\begin{array}{r}
 - 365 \text{ días al año} \\
 - 52 \text{ semanas al año} \\
 \quad 52 \times 2 \text{ (días)} = \quad 104 \text{ días de fin de semana} \\
 \qquad \qquad \qquad \qquad \qquad \qquad 8 \text{ días festivos} \\
 \qquad \qquad \qquad \qquad \qquad \qquad \text{-----} \\
 \qquad \qquad \qquad \qquad \qquad \qquad 112 \text{ días no operables para la Red}
 \end{array}$$

$$365 - 112 = 253 \text{ días laborables}$$

Ahora de estos 253 días laborables, la empresa no trabaja las 24 horas, para efecto de estos cálculos se tomó en cuenta 18 horas de trabajo en la empresa.

$$253 \text{ días} \times 18 \text{ horas} = 4554 \text{ horas efectivas de operación de la Red}$$

$$4554 \text{ horas} \times 60 \text{ minutos} = 273240 \text{ minutos}$$

Se considera como aceptable una interrupción de 30 minutos, cada semana, dentro de la operación normal de la Red .

$$30 \text{ minutos} \times 52 \text{ semanas} = 1560 \text{ minutos de falla}$$

Esto nos dejaría :

$$\% \text{ de Disponibilidad} = 1 - \left(\frac{\text{Minutos de Falla}}{\text{Minutos de operación}} \right)$$

$$\% \text{ de Disponibilidad} = 1 - \left(\frac{1560}{273240} \right)$$

$$\% \text{ de Disponibilidad} = \underline{99.429 \%}$$

4.3 Monitoreo y control de la red

La mayoría de las arquitecturas de administración utilizan la misma estructura básica y un conjunto adicional de relaciones. Las estaciones finales (los **dispositivos administrados**), como pueden ser computadoras o dispositivos de red, ejecutan un "software" que les permite enviar alertas cuando éstos reconocen algún problema. Los problemas son identificados cuando uno o más de los límites determinados por el usuario es excedido. Dependiendo de las alertas recibidas, las **entidades administradoras** son programadas para reaccionar ejecutando una, varias o todos los grupos de acciones, que incluyen:

- Notificación al operador
- Registro de eventos
- Apagar el sistema
- Intentos automáticos para reparar el sistema

Las entidades administradoras pueden enviar también requerimientos a las estaciones para validar los valores de ciertas variables. Estos requerimientos pueden ser automáticos o controlados por el usuario. Los agentes en los dispositivos administrados responden a esos requerimientos (Polls). Los Agentes son módulos de "software" que recopilan la información de los dispositivos administrados en los cuales ellos residen, guardan esta información en una base de datos de administración, y proveen ésta (reactiva o proactivamente) a las entidades administradoras en un **Sistema de Administración de Red (NMS)** a través de un **protocolo de administración de Red**.

Los protocolos de administración más conocidos incluyen :

SNMP	(Simple Network Management Protocol)
CMIP	(Common Management Information Protocol)
RMON	(Remote Monitor)

SNMP forma parte de los protocolos TCP/IP, además tiene una gran difusión y la mayoría de los fabricantes cumplen con este estándar. Por esta causa se eligió como el protocolo de administración en la Red, pero será un requisito que los equipos cumplan también con el estándar RMON ya que está teniendo gran difusión en los ambientes conmutados.

Para la entidad administradora se necesita elegir una que tenga capacidad centralizada de administrar todos los elementos en la Red.

4.4 Tráfico de la red

4.4.1 Protocolos de RED

TCP/IP Y SPX/IPX son los protocolos bajo los cuales se establecerán la mayor parte de las comunicaciones en la red de la empresa. Por este hecho los equipos que se evalúen deben tener la capacidad de manejar eficientemente los protocolos TCP/IP Y SPX/IPX (mientras se implanta TCP/IP bajo Novell en forma estable), sin embargo también deben de operar con protocolos como XNS, Netbios, SNA, AppleTalk, etc.

4.4.2 Protocolos de Enrutamiento

Para efectos de enrutamiento existen dos filosofías para el desarrollo de algoritmos de enrutamiento, el enrutamiento en base a vectores a distancia "Distance Vector" y el enrutamiento en base al estado del enlace "Link State", RIP (Routing Information Protocol) es el protocolo basado en "Distance Vector" de mayor implantación, en el caso de "Link State" es OSPF (Open Shortest Path First).

Dada las proyecciones de la empresa, se contempla la existencia de una red compleja en cuanto a enrutamiento y especificaciones de redundancia en enlaces. Por ello se recomienda un protocolo de enrutamiento basado en "Link State" como OSPF, para el manejo más eficiente del esquema de enrutamiento en los equipos que se estén integrando.

4.4.3 Protocolos de Administración de Red

Así como en la mayor parte de las áreas computacionales, la administración de redes también se desarrolló con base en algunos estándares creados para lograr una interrelación entre la diversidad de productos en el mercado.

El protocolo dominante en estos momentos en cuanto a administración de redes es el SNMP, con su última versión SNMP V2.

4.5 Tiempos de conexión

En este punto se analizan los requerimientos que la red debe soportar en términos de número de conexiones que se realizarán. Por el tipo de conexiones (IP/IPX) debe considerarse que el tráfico originado por IPX genera una sobrecarga en los medios ya que por cada servidor la sobrecarga se incrementa en forma exponencial. Por lo que es bueno considerar, basados en el estudio de conexiones, cuáles son los períodos más críticos y de acuerdo a éstos determinar el tráfico que posiblemente se origine, dependiendo del número de conexiones y servidores.

El análisis de tiempos de conexión local para IPX/IP se muestra en la gráfica 4.8
El análisis de tiempos de conexiones entre entidades a través del backbone se muestra en la gráfica 4.9

El análisis de tiempos de conexiones hacia la WAN se muestra en la gráfica 4.10

De las gráficas se puede concluir que existirán dos períodos con un número de conexiones elevado que se presentarán de 9:00 a 12:00 hrs. En este período existirá un pico de 740 conexiones simultáneas, por lo que una de las premisas será analizar el desempeño de los equipos con carga de este tipo. Un punto que es importante es el conocer cuántas de estas conexiones necesitan interconexión que cruce el Backbone. Este dato dará pautas para analizar otro parámetro importante de los equipos, que se refiere a la capacidad de filtrar paquetes y su desempeño utilizando esta funcionalidad.

En la gráfica 2 encontramos que el período de más conexiones en el Backbone será en un período vespertino preferentemente 15:30 a las 17:40 hrs, con 340 usuarios, que es cuando se envían condensados de información. Es conveniente mencionar que en el rango de 9:30 y 13:10 hrs hay un número más o menos constante de conexiones IP, pero el tipo de conexión (Transferencia de planos de CAD) consume un ancho de banda muy alto no obstante que no hay muchas conexiones, este tipo de conexión puede requerir de mucho ancho de banda.

En la tercera podemos observar las conexiones de WAN, se localizarán en él dos periodos básicamente:

Uno matutino de 7:30 a 13:00 hrs y uno nocturno de 21:00 a 23:00 hrs y el tráfico será preferentemente IP.

Gráfica de Conexiones / Tiempo

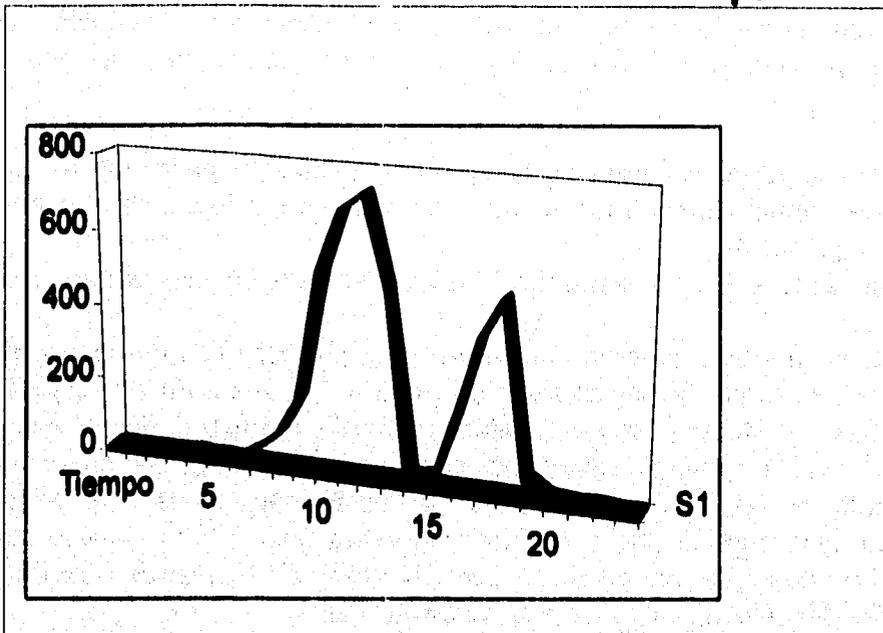


Figura 4.8

Gráfica de Conexiones en el Backbone / Tiempo

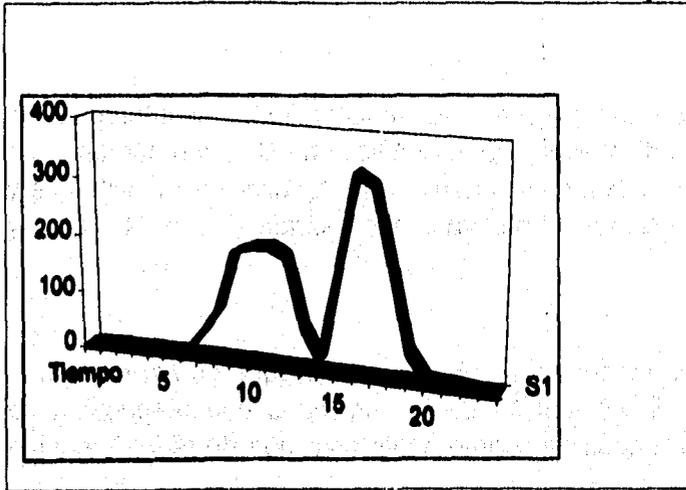


Figura 4.9

Gráfica de Conexiones en la WAN / Tiempo

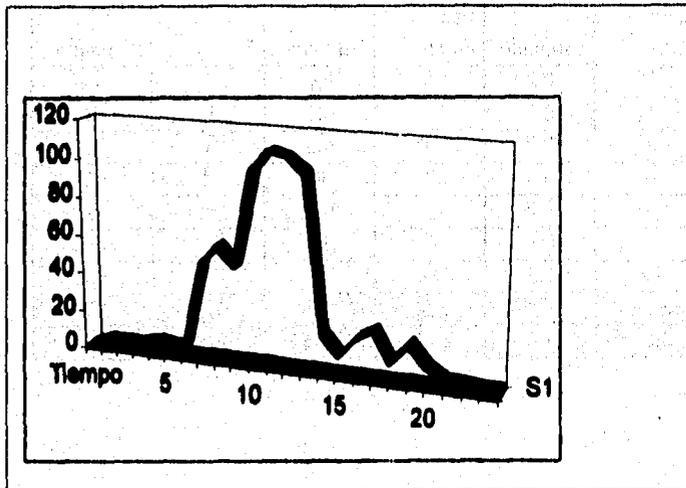


Figura 4.10

4.6 Número de conexiones

Para tener una base de estimación que refleje los requerimientos de interconexión de cada una de las unidades de la empresa, se realizó un consenso, tomando en cuenta las 6 unidades más representativas en cuanto a servicios de sistemas y telecomunicaciones, con funciones operativas, administrativas, de servicios y foráneas de la empresa.

Del análisis de la información recabada, se obtuvo la tabla (que se muestra en la tabla 4.1), la cual contiene la estimación de las unidades con respecto a su proyección de crecimiento a 5 años en cuanto a interconexión de redes y equipo de cómputo de la empresa.

Análisis y Proyección de Conexiones y Cargas						
UNIDAD DE LA EMPRESA	Núm Lan Corp	Tráfico Estimado	Núm Lan Foran.	Tráfico Estimado	Núm Loc Ext	Tráfico Estimado
	Empresa D	2	0.2	2	0.6	5
Telecomunicaciones	1	0.3	0	0.1	0	0
Empresa B	2	0.2	20	0.5	1	0.2
Administración	2	0.3	0	0	0	0
Empresa A	3	0.2	5	0.9	0	0
Empresa C	3	0.3	5	0.9	3	0.2
Total	13	1.5	32	3	9	0.6
Promedio por Unidades	2.16	0.25	5.33	0.5	1.5	0.1
Total estimado 11 unidades	30.3	7.6	61.7	40.8	21.0	2.1

Tabla 4.1

La primera columna de la tabla indica el nombre de la unidad corporativa, la columna "Núm Lan Corp" (Número de Redes Lan edificios corporativos), indica el número de redes a las que se tienen proyectado interconectarse dentro del grupo corporativo, la columna "Núm Lan Foran", indica el número de interconexiones a redes foráneas proyectadas de cada unidad, y el "Núm de Loc Ext" indica las proyecciones de requerimientos de conexión con localidades externas a la empresa.

Las columnas de "Tráfico Est", indican el porcentaje del tráfico estimado de acuerdo con el ancho de banda total que se requiere en cada red para lograr la interconexión con las demás redes, de tal forma que el 0.1 indicará que el 10% del tráfico total que fluye en la red local saldrá de ella para interconexión con otras redes.

Tomando en cuenta el número de usuarios de cada red de cada unidad, las aplicaciones y los comentarios acerca de los requerimientos de interconexión con otras unidades, se ponderaron los porcentajes del "tráfico Est" para cada unidad.

Tomando en cuenta que para el caso de interconexión entre redes locales por un "Backbone", en una buena planeación, cuando más el 20% del tráfico de la red local saldrá al "Backbone" de interconexión, no así el caso de interconexión por medio de un enlace satelital como es el caso de redes foráneas, en donde este porcentaje de tráfico se puede incrementar.

Como se puede observar los porcentajes que aparecen en la tabla superan en muchas ocasiones los estándares, queriendo con ello representar el máximo porcentaje de tráfico que se podrá dar al momento de interactuar todas las redes en forma concurrente.

Bajo estas premisas se consideró que para el caso de redes locales en la empresa, el tráfico promedio fluctuará entre el 20% y el 30%, no así el caso de interconexión de redes foráneas, en donde las diferencias de variación son muy grandes para cada caso específico de las unidades, como el caso de Telecomunicaciones e Informática, que la mayor parte del tráfico que genere será para efectos de administración y servicio de la red (que representa un 10% del ancho de banda), pero unidades con requerimientos de videoconferencia y construcción pesada que tienen prevista la transferencia de grandes volúmenes de información por la naturaleza de sus sistemas, en estos casos se prevé un 90% del tráfico estimado de su ancho de banda.

Con estas consideraciones se obtuvieron los totales de cada rubro, y con ellos se calculó el promedio por unidad, para estimar con este promedio, el total de las 11 unidades que conforman la empresa, para cada columna correspondiente.

De estos totales podemos deducir que:

Se tiene proyectado manejar 30.3 interconexiones entre redes localizadas en la empresa, que multiplicadas por su promedio de tráfico generado de cada red, (30%), requerirá un 760% del ancho de banda de las redes que se estén interconectando, de tal forma que el peor de los casos en que estas redes estén interactuando simultáneamente, (tomando en cuenta que cada red tienen un ancho de banda de 10 Mbps y que se está utilizando en su totalidad), generarán un tráfico en su conjunto de 76 Mbps.

De igual forma para el caso de interconexión entre localidades foráneas, considerando el total de ellas (81.7), multiplicadas por su promedio de tráfico 50%, se requiere de un 4,080% del ancho de banda del enlace, para ello se tomó la proyección de que cada unidad cuente con un ancho de banda de 64 Kbps, por lo que el tráfico generado en el peor de los casos será 2.6 Mbps.

Como se puede observar en el peor de los casos, el "Backbone" Corporativo tendrá un tráfico concurrente de 78.6 Mbps, esto considerando como se mencionó con anterioridad, las proyecciones a 5 años de cada una de las unidades.

Según el análisis realizado de los requerimientos de ancho de banda del "Backbone" de la empresa, el contar con una red de 155 Mbps, cubre perfectamente las necesidades de flujo de información para las proyecciones estimadas; cabe destacar que también se identificó la posibilidad de conjuntar voz, datos e imágenes dentro del mismo medio de transmisión.

4.7 Selección de la configuración de la Red

El estudio que aquí se presenta se basa en una evaluación de factibilidad y oportunidad de las diferentes tecnologías tomando en cuenta diferentes aspectos, como son:

Las capacidades de cada tecnología, su madurez, el soporte ofrecido, las tendencias del mercado, la compatibilidad con diversas topologías y equipos, costo de implantación y operación, la flexibilidad de migración y su base instalada, dando especial importancia en los requerimientos actuales de la empresa y su proyección a cinco años.

Cuadro Comparativo de Tecnologías

Cuadro de evaluación de las tecnologías FDDI, FDDI II, ATM y Conmutación Ethernet, indicando la ponderación total que se dió a cada punto de evaluación:

EVALUACIÓN DE TECNOLOGÍAS						
Descripción	FDDI	FDDI II	ATM	FAST Ethernet	Conmutación Ethernet	Pond
Tecnología	10	12	15	5	5	15
Estandarización	10	5	9	5	10	15
Costo de Implantación	8	3	5	10	10	10
Soporte Tecnológico	25	0	15	8	15	25
Flexibilidad en Conectividad	5	0	9	4	4	10
Tiempo de Vida	15	10	25	15	10	25
Evaluación	73	30	78	47	54	100

Tabla 4.2

Tecnología: Se evalúan las facilidades tecnológicas ofrecidas por cada esquema como son: velocidad de transmisión, servicios ofrecidos como transmisión de voz, datos, imágenes, etc., aprovechamiento del medio de comunicaciones, etc.

Estandarización: Madurez de la tecnología y su nivel de especificación, para fines de estandarización.

Costo de Implantación: Costo monetario de la instalación en México de equipos y componentes de cada tecnología evaluada.

Soporte Tecnológico: Nivel de soporte ofrecido en México con respecto a la base instalada y compañías que ofrezcan soporte a cada una de las tecnologías.

Flexibilidad en Conectividad: Facilidades ofrecidas por la tecnología para lograr la interconectividad con otras tecnologías, así como las capacidades de convivencia de las tecnologías entre sus diferentes proveedores.

Tiempo de Vida: Permanencia de esta tecnología en el mercado para fines de conformar un "Backbone" corporativo, tomando en cuenta la inversión actual en la tecnología evaluada.

En la empresa, se requiere de una tecnología que ofrezca medio de comunicación de alta velocidad, confiable y con facilidades de integración tecnológica con el equipo existente y proyectado; siendo la empresa una organización dedicada a la construcción, las exigencias de contar con los avances tecnológicos de mayor actualidad no son, como en el caso de las organizaciones financieras, un factor que determine una ventaja en la competitividad de servicios ofrecidos con respecto a sus competidores, comparado con el riesgo que lleva consigo la falta de solidez y estandarización de una tecnología de esta naturaleza.

Del cuadro comparativo de tecnologías podemos deducir que el esquema de conexión ATM reúne las mejores características que pueden satisfacer las necesidades de la empresa. Además este esquema le ofrecerá las mejores oportunidades de crecimiento y ampliación tecnológica.

4.8 Interfaces

4.8.1 Red WAN

Este esquema se basará en la utilización de canales síncronos dedicados para cada localidad con las siguientes características:

- Existen canales dedicados para voz y datos en cada localidad, básicamente estas señales se conectan directamente al PBX y éste a su vez se encarga de conmutar físicamente la señal para cada extensión ya sea telefónica o de datos. Los canales de datos son principalmente enlaces satelitales, sin embargo también existen enlaces de microondas, de líneas privadas y líneas conmutadas así como la utilización de RDI.

- En la mayoría de los enlaces satelitales de datos la comunicación es punto a punto, centralizada en México.

- Para los casos en que se requiere cambiar los enlaces satelitales, ya sea por cambios en los extremos del enlace, o por cambios en el ancho de banda del enlace esto se hace cambiando ya sea el mapa en el esquema satelital o definiendo un horario para la redistribución del ancho de banda.

Los elementos para conformar la red WAN son :

- Enrutadores
- Concentradores
- VSAT
- Antena
- Modems Satelitales

Cabe destacar que la interconexión entre los equipos relacionados al satélite y su interconexión al Enrutador se pueden llevar al cabo con dos tipos de interface física principalmente:

-RS449

-V.35

Para interconectar ambas redes se pueden contemplar diferentes tipos de interfaces dependiendo de la topología. Estas interfaces se describen como:

ATM está diseñado para WAN, pero necesita como requisito anchos de banda que parten de 34 Mbs para tener un funcionamiento óptimo. En este momento la tecnología instalada para conexiones WAN no permitiría la integración directa de ATM pero dejaría el Backbone de LAN preparado para cuando los enlaces puedan proporcionar los requerimientos mínimos de velocidad. Para la conexión en corto plazo se puede realizar con un Enrutador con interface de ATM. En este punto sólo habrá que revisar que los estándares que se utilicen sean los mismos, ya que la tecnología es relativamente nueva lo que puede originar que en ocasiones existan diferencias de implementación.

4.8.2 Red LAN (ATM)

Los elementos que se conectarán en el Backbone de ATM son :

- Concentradores Ethernet
- Conmutadores ATM
- Concentradores de Fibra óptica
- Equipos de Red (Enrutadores, Servidores, Computadoras personales)

Las interfaces que se utilizarán para los diferentes elementos son:

- ST- SC La conexión de los concentradores de fibra óptica a los equipos
- SC- SC Para la conexión directa de equipos a los conmutadores ATM
- S T-SC Para la conexión de los concentradores de fibra óptica a los conmutadores ATM
- RJ45 Para las conexiones UTP- Nivel 5
- RJ45/DB25 Para las conexiones del Servidor de comunicaciones a los Modems

CAPITULO 5 ANALISIS Y SELECCION DE EQUIPO

En este capítulo se describe en principio el proceso de análisis y selección de equipo en donde se incluyen las pruebas a las que se sometió a equipos de diferentes proveedores, continuando con las consideraciones tomadas para su instalación, para finalizar con una descripción detallada de las características técnicas de cada uno de los equipos seleccionados.

5.1 Justificación de equipos

En esta sección analizaremos las diferentes marcas de equipo que puedan integrar la solución planteada en el capítulo anterior. Para este estudio tomaremos en cuenta comparaciones realizadas por diversas empresas y organizaciones especializadas en este fin.

5.1.1 Justificación de los conmutadores ATM

Con los primeros conmutadores de ATM ya en producción no tiene mucho caso discutir el futuro de esta tecnología. El "Si" y el "Cuando" se han convertido en "Aquí" y "Ahora". Es por esto que DATA COMMUNICATIONS y los Laboratorios Europeos de Redes (ENL, París), realizaron el primer laboratorio de prueba de carga de conmutadores ATM cuyos resultados fueron publicados en la revista DATA COMMUNICATIONS de McGraw- Hill correspondiente al mes de Marzo de 1995. La lista de los 14 proveedores invitados fue la siguiente:

Bay Networks Inc. (Santa Clara California), Cisco Systems Inc. (San Jose California), Digital Equipment Corp. (DEC, Maynard, Mass.), Fore System Inc. (Worrendale, Pa.), Fujitsu Networks Sutching of America Inc. (Raleigh ,N.C.), General Datacomm Inc. (Germantown,Md.), IBM Lightstream Corp. (Billerica Mass.), NEC America Inc. (San Jose California), Newbrige Networks Corp. (Herndon,Va.), Northen Telecom Ltd. (Mississauga, Ontario), y 3Com Corp. (Santa Clara California). Las empresas participantes fueron:

Bay, Cisco, DEC, Fore, Lightstream, Newbridge y 3Com.

ENL realizó 3 evaluaciones de capacidad de manejo de tráfico de cada conmutador bajo las mismas condiciones, utilizando un circuito de servidor virtual como base y un generador-analizador ATM-100 de Wandel & Gotermann para obtener las mediciones. El Analizador compara y calcula el retraso de la celda así como su desviación estándar con lo cual se puede verificar la integridad del encabezado, el contenido del campo y la secuencia de errores. El administrador de tráfico fue deshabilitado en todos los conmutadores excepto en Latiscell, el cual no lo permite.

La prueba 1 produce los valores base para los retardos de las celdas y sus variaciones, la generación del tráfico se trasmite a sólo 7.488 Mbit/s a través del circuito virtual. Las celdas son transmitidas a intervalos regulares de cada 20 celdas, con un tráfico efectivo igual a un flujo CBR (Constant Bit Rate). El tráfico del circuito virtual es conmutado a través de dos de los conmutadores de 4 puertos y ningún otro tráfico corre a través del conmutador mientras se ejecuta la prueba (Figura 5.1).

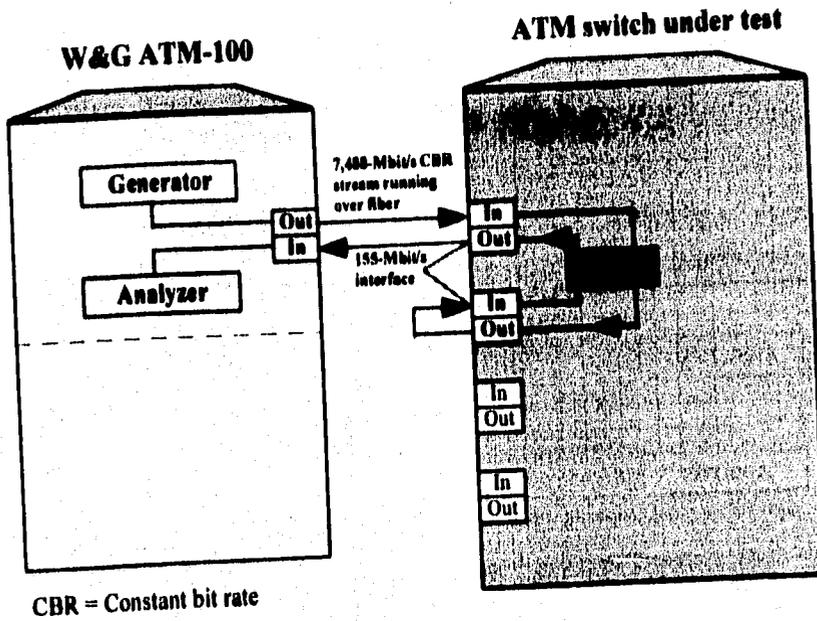


Figura 5.1

Como resultado de la prueba 1 tenemos que el conmutador de Fore desarrolló la latencia más baja, con un retraso de celda de sólo 10.57 microsegundos. El conmutador Cellplex de 3Com obtuvo el segundo lugar con 10.87 microsegundos y el tercero fue para DEC con 11.75 microsegundos (ver Figura 5.2).

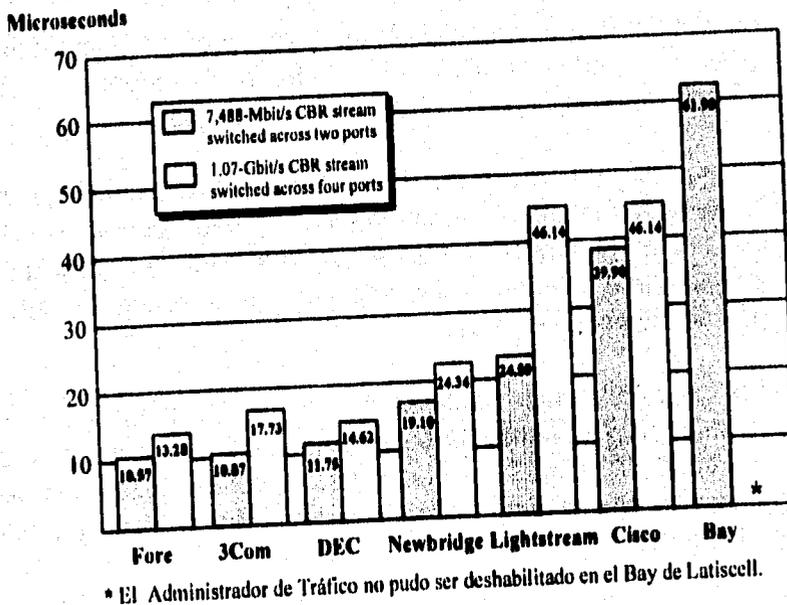


Figura 5.2

En la segunda prueba se incrementó la carga a 1.07 Gbit/s a través de cuatro interfaces full-duplex a 155 Mbit/s, nuevamente con el administrador de tráfico deshabilitado. Se usó el W&G ATM-100 para generar y medir el tráfico (Figura 5.3).

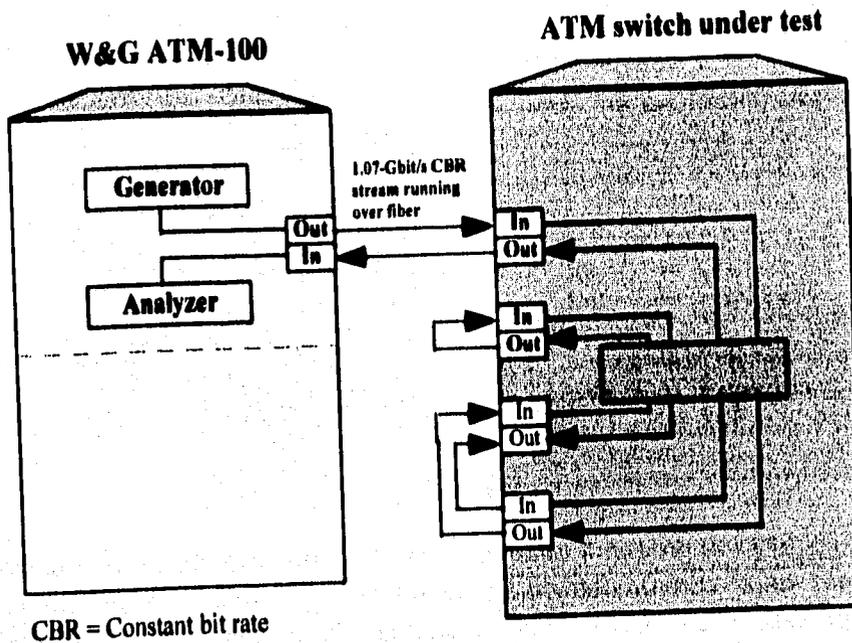


Figura 5.3

Tenemos como resultado que el conmutador de Fore quedó en primer lugar con 13.28 microsegundos de latencia. DEC con 14.62 microsegundos obtuvo el segundo lugar y 3Com el tercero con 17.73 microsegundos.

Pero la latencia no es la única parte importante de la evaluación de las aplicaciones en tiempo real. Los conmutadores deben buscar las celdas rápidamente pero también de manera consistente. Para medir la capacidad de un conmutador deben tomarse en cuenta dos aspectos, la variación de retraso de celda y la variación de intervalo de celda.

Cuando las celdas toman diferentes cantidades de tiempo para pasar a través de un conmutador, la diferencia en latencia es conocida como variación en el retraso de celda. Cuando la latencia permanece constante, las celdas llegan a su destino en intervalos constantes. Pero cuando la latencia varía, los tiempos de intervalo de celda también lo hacen.

Para la prueba se generó un tráfico de 7.488 Mbit/s conteniendo una celda de datos cada 54.6 microsegundos y conmutado a través de dos puertos.

El Cellplex 7000 de 3Com presentó una variación de retraso de celda de 0.96 microsegundos, lo siguió el conmutador ASX-200 de Fore con 1.25 microsegundos y después los conmutadores Gigaswitch ATM de DEC y Bay de Lattiscell con 1.39 y 1.41 microsegundos respectivamente.

Se reportaron variaciones muy bajas en los tiempos de intervalo de celda cuando se conmutaron 7.488 Mbit/s a través de dos puertos. El conmutador 3Com obtuvo una variación de 1.01 microsegundos en dos puertos (Figura 5.4); Fore presentó una variación de 1.54 microsegundos y Lightstream 1.99 microsegundos (por mencionar sólo los tres primeros).

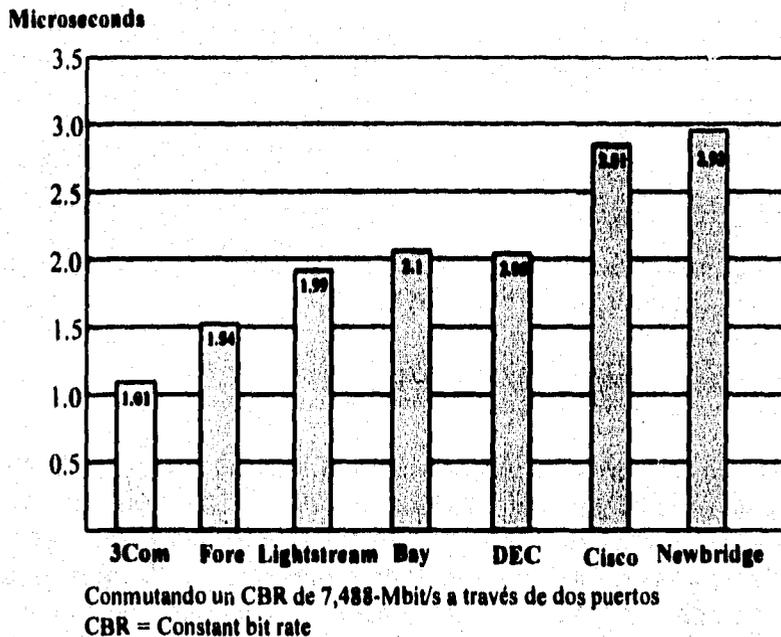


Figura 5.4

ENL también consideró importante la forma en que los conmutadores pueden ordenar el tráfico cuando éste es de diferente tipo, situación con la que se encuentran cotidianamente. Para tal efecto, fueron enviados al mismo puerto un CBR a 7.488 Mbit/s y un tráfico IP (Figura 5.5).

El objetivo fue determinar si el conmutador podía proteger el CBR sin introducir latencia adicional, lo cual afectaría voz y video.

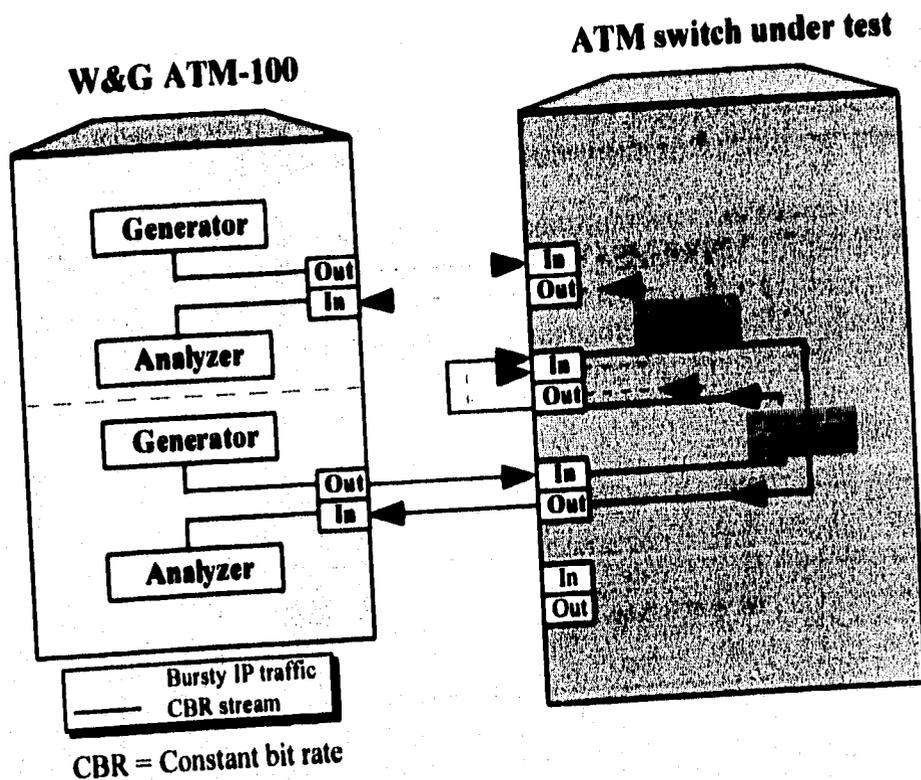


Figura 5.5

Como resultado, el conmutador Fore presentó la latencia más baja (Figura 5.6). Bajo las cargas de trabajo más pesadas la latencia de Fore fue de 77.89 microsegundos. El conmutador DEC mostró un severo incremento en latencia dado que en las cargas de trabajo más ligeras presentó 11.75 microsegundos y en las más pesadas 121.43 microsegundos. Lightstream fluctuó de 24.50 microsegundos cuando se conmutó a través de dos puertos a 89.19 bajo las cargas más pesadas.

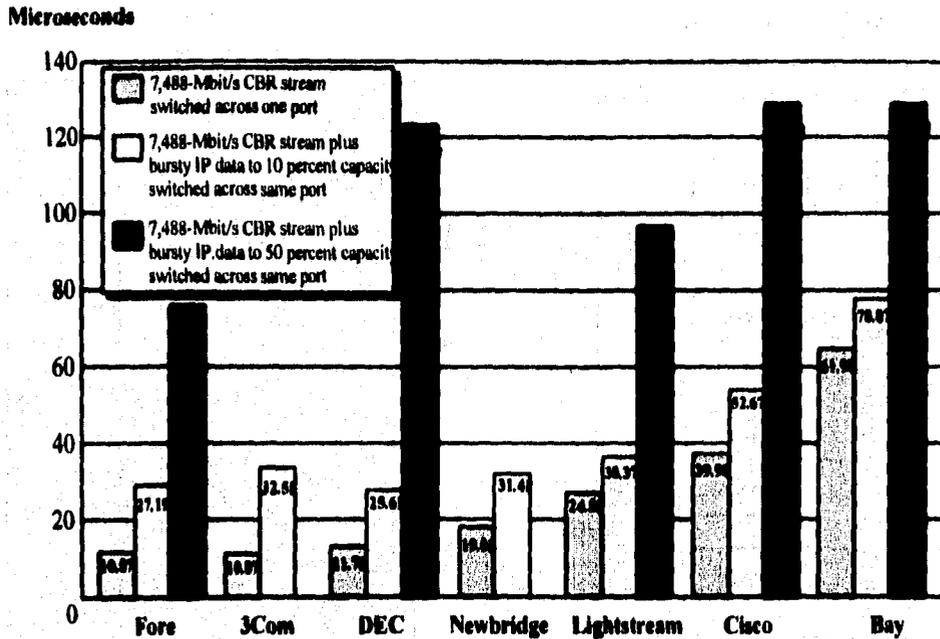


Figura 5.6

Las pruebas del ENL también trataron de comprobar si la congestión en un puerto podría afectar a un puerto no congestionado. Este fenómeno puede indicar las debilidades de una arquitectura.

Para esta prueba se enviaron dos flujos de tráfico a un puerto de entrada (Figura 5.7). Los dos flujos fueron conmutados a diferentes puertos de salida (uno no congestionado y los demás con tráfico de otra fuente).

Cinco de los 7 conmutadores (entre ellos el ASX-200 de Fore) manejaron admirablemente la situación. Los datos que ingresaron al puerto congestionado perdieron celdas, pero la congestión no afectó el tráfico en el puerto no congestionado.

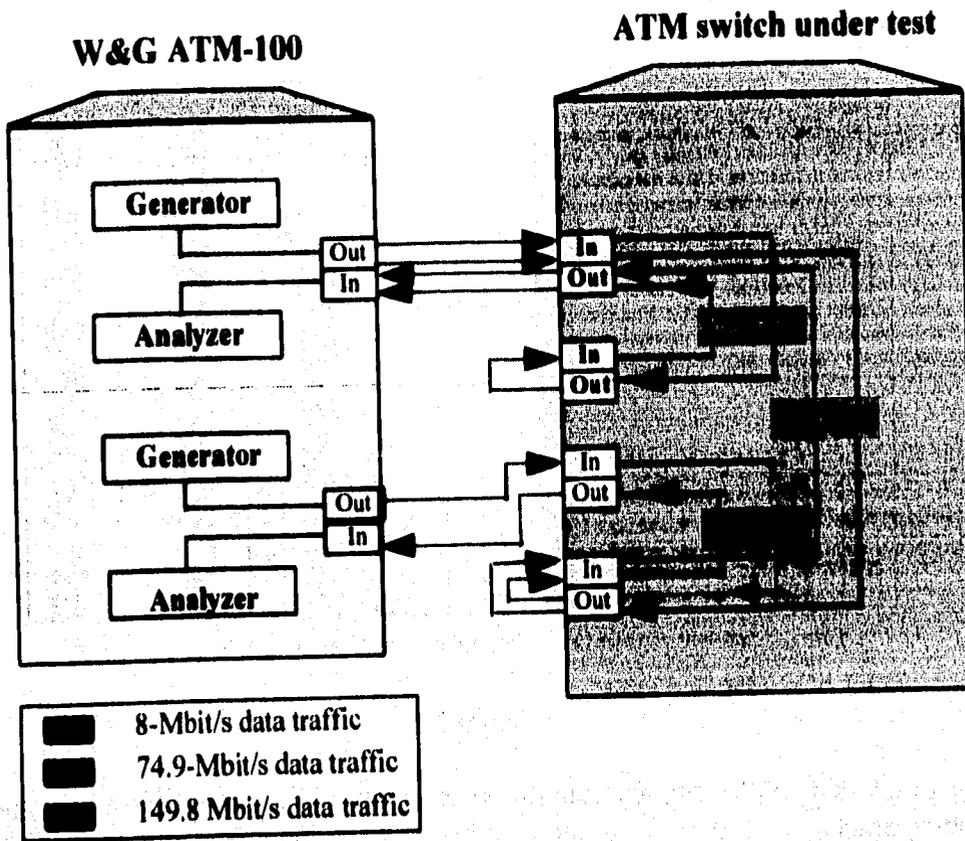


Figura 5.7

5.1.2 Justificación de los concentradores de cableado

VENDEDOR	PRODUCTO	MAX PUERTOS POR HUB	MODULOS	ATM media SOPORTADA	NUM PUERTOS ATM	PROTOCOLO	HOT SWAPPING	ADMON. OUT-OF-BAND	ADMON. REDUN- DANTE	PODER REDUN- DANTE
AT&T Morristown, N.J. 800-747-1212	Star LAN 100 Network Concentrador Círculo No. 463	12	ATM	Multimode fiber	1	agente SNMP	si	si	no	no
Cabletron Systems Inc. Rochester, N.H. 603-3329400	MMACC Círculo No. 464	54	ATM Ethernet, TokenRing, Local Talk	Multimode single mode fiber	1	agente SNMP o SMT	si	si	no	si
Digital Equipment Mayard, Mass. 508-493-5111 800-343-4040	DEC Concentrador 500 Círculo No. 465	8	ATM	Multimode single mode fiber, STP, thin coax	1	agente SNMP	no	no	no	si
Optical Data Systems Inc. Richardson, Texas 214-234-6400	ODS 1090 Círculo No. 466	60	ATM Ethernet, TokenRing,	Multimode single mode fiber	2	agente SNMP proxy o SMT	si	si	si	si
Synemetics Inc. Nhort Billerica, Mass. 508-670-9009	LANplex 5012 Círculo No. 467	40	ATM Ethernet	Multimode fiber	2	agente SNMP proxy o SMT	si	si	si	si
SynOptics Communications Inc. Santa Clara, Calif. 408-764-1013	LattisNet model 3000 Círculo No. 468 Círculo No. 465	40	ATM Ethernet, TokenRing,	Multimode single mode fiber, STP, thin coax	3	agente SNMP	si	si	no	no
	LattisNet model 2914 Círculo No. 469	Nonmodular 12	ATM	Multimode fiber	2	agente SNMP	si	si	no	no
	LattisNet model 2912 Círculo No. 470	Nonmodular 12	ATM	STP	2	agente SNMP	si	si	no	no
3Com Corp. Santa Clara, Calif. 408-764-5000	Link Builder 3GH Círculo No. 471	80	ATM Ethernet, TokenRing,	Multimode fiber	2	agente SNMP	si	si	no	no
Timeplex Inc. Woodcliff Lake, N.J. 201-391-1111	Time/LAN 100 Concentrador Círculo No. 472	30	ATM	Multimode single mode fiber	2	agente SNMP	si	si	no	no
Ungerhann-Bass Inc. Corp. 508-493-5111 800-343-4040	Acces/one Maynard, Mass Círculo No. 473	52	ATM Ethernet, Local Talk	Multimode fiber TokenRing	1	agente SNMP	si	si	no	no

5.1.3 Justificación de los enrutadores

La Universidad de Harvard realizó pruebas para determinar el desempeño de los enrutadores, basados en este estudio determinamos cuál era el mejor proveedor para los servicios a la red WAN.

El desempeño de los enrutadores se analizó desde muchas perspectivas :

- El máximo "throughput" sin tirar paquetes
- El máximo "throughput" sin importar el numero de paquetes tirados (llamado "throughput plano")
- El máximo "throughput" cuando se está filtrando
- El máximo "throughput" en cadenas duales
- Latencia del dispositivo

Como no existe una métrica que indique el desempeño absoluto del enrutador se tienen que considerar todos los aspectos anteriores en conjunto.

El máximo "throughput" sin tirar paquetes. Este parámetro indica el rango máximo al cual el enrutador puede encaminar correctamente todos los paquetes de entrada, éste es de gran utilidad ya que si se tira un solo paquete originará que las puntas tengan que llegar al tiempo de espera para poder pedir una retransmisión lo cual tiene un impacto mayor en el tiempo de respuesta de las aplicaciones.

La prueba comienza al enviar un número de paquetes a través del enrutador, con un tiempo de separación entre paquetes de una duración específica, esto crea alrededor de 20 segundos continuos de transferencia de información. Los paquetes de salida son rastreados por un analizador de red HP LAN. Si todos los paquetes son encaminados sin tirar ninguno la separación entre paquetes se reduce. Así mismo cuando el enrutador tira algún paquete la separación entre paquetes se incrementa. El máximo rango se determina como el punto en el cual un número de paquetes es encaminado dentro de la separación mínima posible. Esto es determinado para cada tamaño de paquete según el protocolo.

El máximo "throughput" sin importar los paquetes tirados ("throughput plano"). Como la carga de tráfico se incrementa en un enrutador, su habilidad para manejar flujos continuos de datos sin tirar paquetes disminuye al llegar a cierto umbral. Para probar la habilidad del enrutador para manejar casos de carga extrema, un conjunto de paquetes fue enviado al máximo rango permitido por equipo de prueba. Para asegurarse que las colas internas se agotaran, un conjunto de paquetes de duración de al menos 20 segundos fue utilizada. Esta prueba también se realizó para diferentes tamaños de paquete según el protocolo.

El "throughput" cuando se está filtrando. El filtrado basado en políticas permite a los administradores instruir a los enrutadores para bloquear o dejar pasar paquetes a ciertos destinos, frecuentemente esta característica es usada con fines de seguridad. Un filtrado típico está basado en direcciones fuente/destino, tamaño de paquete, puertos origen/destino y tipo de protocolo. El proceso adicional en el que el enrutador incurre para realizar tal filtraje puede afectar el rango de manejo de datos. Para medir este efecto, algunos filtros fueron añadidos a la configuración del enrutador y se ejecutó la prueba del máximo rango de datos. Esta prueba sólo se realizó con TCP/IP. Dos condiciones de filtraje fueron utilizadas :

- Un filtro fue agregado a la configuración interna y las pruebas fueron efectuadas

- Nueve filtros más fueron agregados y las pruebas se efectuaron nuevamente

Se buscó hacer los filtros de tal forma que el enrutador revisará las primeras nueve condiciones para poder definir hacia dónde encaminaría los paquetes.

El "throughput" en cadenas duales. Si un enrutador tiene más de dos puertos, y simultáneamente se está moviendo información de datos a través de todos los puertos, esto puede limitar el desempeño del enrutador.

Para probar este efecto, cadenas duales de datos TCP/IP fueron pasadas a través de los enrutadores con más de cuatro puertos, cada cadena direccionada en forma diferente para poder ser enviada a diferentes puertos. Las cargas que se introdujeron fueron con la carga que producía el "throughput plano"

Latencia del dispositivo. Para determinar la latencia interna de un enrutador, paquetes TCP/IP fueron enviados a una baja velocidad. La latencia interna fue establecida al medir el tiempo que pasa desde que la punta inicial del frame entra al dispositivo y la parte final del frame de salida abandona el mismo. Contrariamente a lo que clama la industria en casi todos los casos la latencia del enrutador no causaba problemas de desempeño o confiabilidad. Para casi todos los enrutadores la latencia máxima fue de menos de un milisegundo con una variación de 0.2 ms.

Resultado de las pruebas.

Los resultados de las pruebas son analizados fácilmente en las figuras 5.8 a la 5.11, las cuales grafican el tamaño de paquetes (bytes) contra los paquetes por segundo. Como se puede observar a medida que el tamaño de los paquetes se incrementa, el número de paquetes por segundo que la red puede manejar,

decrece. Otra forma de graficar el desempeño utiliza una métrica basada en bits o bytes por segundo. La métrica pps fue escogida porque la mayoría de los vendedores de enrutadores referencian el "throughput" en esa forma (una medida muy útil siempre y cuando el número de bytes en un paquete sea indicado). Las gráficas de desempeño del dispositivo son más significativas si incluyen una línea de referencia indicando el límite teórico de la red (Ethernet en este caso) en pps. También es interesante una línea que indique la salida máxima de la fuente de prueba para cada tamaño de paquete, en las pruebas de Harvard, la velocidad del dispositivo fuente estuvo cerca de los límites teóricos de Ethernet. Finalmente, estas líneas fueron eliminadas porque uno o más vendedores estuvieron muy cerca de alcanzar los límites teóricos de las pruebas de red.

TCP/IP entre y dentro de una interface. TCP/IP es el protocolo más optimizado en el ambiente de enrutamiento de hoy en día, así como uno de los más comúnmente usados con protocolos de red en interredes corporativas y de investigación.

La figura 5.8 muestra los "throughputs" alcanzados por los enrutadores cuando el tráfico TCP/IP viaja entre puertos de dos diferentes tarjetas de interface. Como se muestra, el Cisco 7000 y el Wellfleet entregan velocidades que están cerca de los límites teóricos de red.

Para el "throughput" con TCP/IP en una tarjeta, el Wellfleet era rápido, excepto para paquetes de 64 bytes. Los paquetes pequeños son normalmente asociados con servidores de terminal y paquetes de reconocimiento.

IPX de Novell entre tarjetas de interface. IPX es una variante del protocolo de servicios de red de Xerox (XNS). Este protocolo ha sido adoptado por Novell para usarlo en sus servidores de archivos. A diferencia de la mayoría de otros protocolos, las implementaciones actuales de IPX no permiten que más de un paquete sea enviado sin un reconocimiento explícito por la otra punta. Esto puede significativamente reducir la carga que los sistemas IPX ponen en una red. El desempeño de Cisco fue equivalente al límite teórico, como lo fue el Wellfleet, excepto para paquetes pequeños. Ver figura 5.10.

Cadenas duales de TCP/IP entre tarjetas de interface. Las pruebas descritas sujetan al enrutador a una sola cadena de paquetes. Pero en el mundo real, los enrutadores deben de manejar múltiples cadenas de paquetes simultáneamente. Las pruebas de multimanejo son complejas y consumen mucho tiempo pero representan el futuro de las pruebas de enrutadores. En un sentido limitado, las pruebas de Harvard exploran las capacidades de multimanejo al enviar cadenas duales de tráfico TCP/IP. El resultado fue medido en términos del agregado de las cadenas de salida en pps.

Por su complejidad, la prueba de cadena dual TCP/IP no fue ejecutada en una forma que de hecho midiera un rango máximo de manejo de paquetes para cada enrutador. Los paquetes fueron enviados al enrutador en el rango máximo que el generador pudiera dar. Como con la prueba de "throughput plano", los enrutadores fueron sobrecargados cuando tiraban paquetes. Considerando que las condiciones de sobre carga tienden a reducir el "throughput" máximo, las pruebas de cadenas duales no deben de ser vistas como un indicador de máximo "throughput" agregado.

Sin embargo la arquitectura del enrutador permite que la prueba de cadena dual sea ejecutada entre tarjetas y en la misma tarjeta. En la prueba entre tarjetas, Cisco tiene el mejor desempeño ya que alcanza el "throughput" teórico. Ver figura 5.11.

En conclusión dedujimos que los equipos con mejor desempeño son Cisco y Wellfleet, pero Wellfleet no tenia servicios de ATM con el RFC 1483 y el 1577 por lo que la decisión del equipo se inclinó al enrutador Cisco 7000.

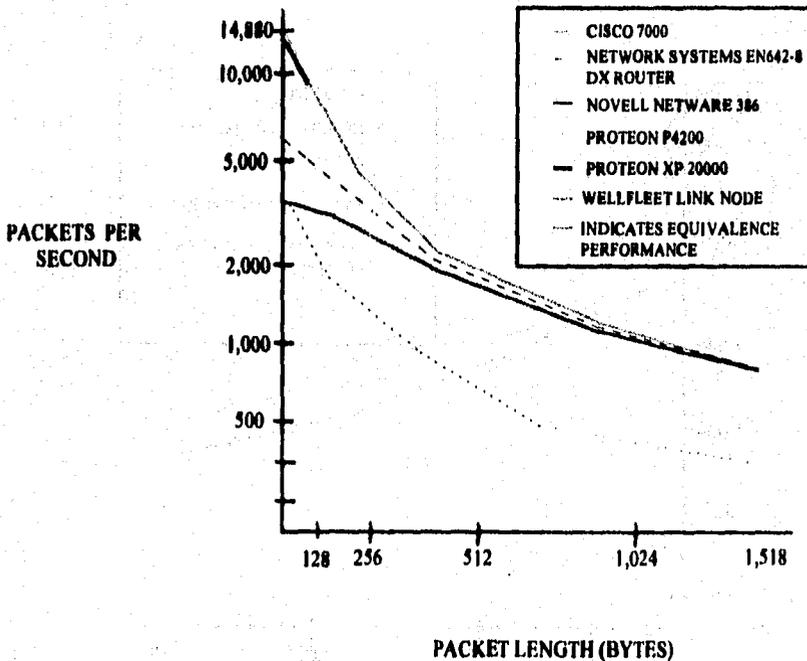


Figura 5.8

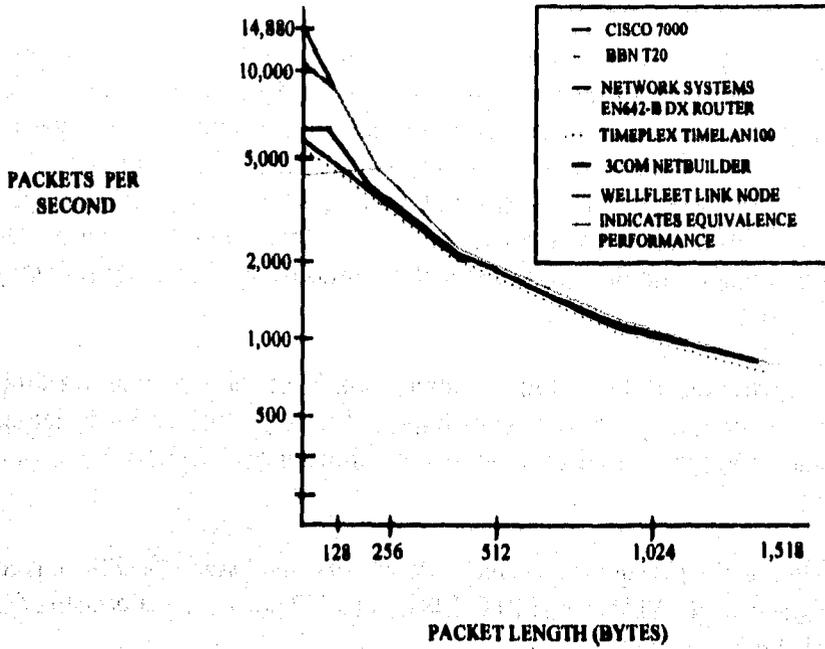


Figura 5.9

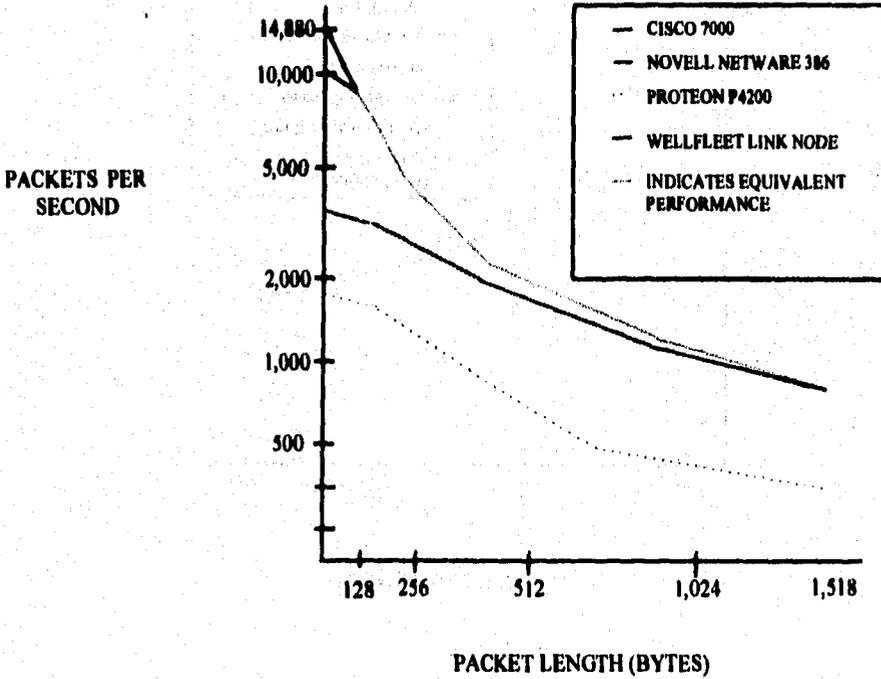


Figura 5.10

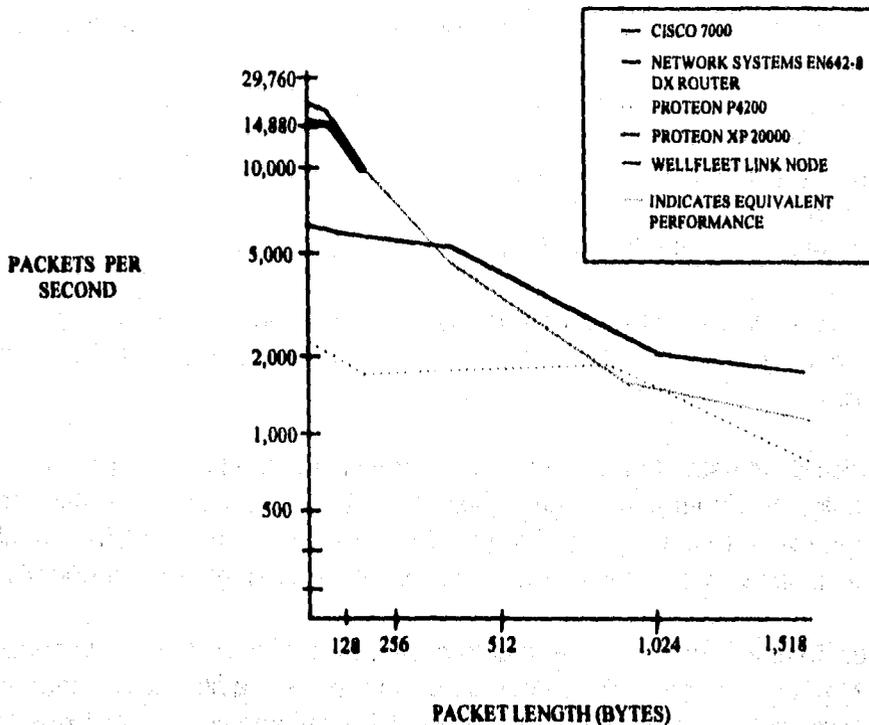


Figura 5.11

5.2 Consideraciones de la instalación

El proyecto de La Empresa comprende la implantación de una red de comunicaciones basada en una arquitectura de sistemas abiertos con los últimos avances en materia de interconectividad e interoperatividad de sistemas y redes de datos.

Como solución a dicho proyecto, se proponen productos como conmutadores ATM marca FORE Systems, enrutadores Cisco Systems, concentradores de cableado CABLETRON Systems.

Con estos productos estamos convencidos de que la integración que pretenden desarrollar cubre y excede las expectativas planeadas por La Empresa, a la vez que ofrece grandes beneficios en funcionalidad, flexibilidad, monitoreo, administración, crecimiento y tendencias hacia tecnologías de vanguardia en este campo.

Esta solución se basa fundamentalmente en el uso de conmutadores de paquetes ATM. Las ventajas principales que presenta esta opción se listan a continuación:

- Se adecúa a las necesidades de comunicación e interoperatividad de La Empresa.
- Cubre las necesidades de desempeño y confiabilidad de la topología propuesta en la sección anterior.
- Representa una mejor alternativa técnica sin representar un gran aumento económico.
- No limita el crecimiento de la red para una aplicación futura.

La red de datos de La Empresa está formada de acuerdo a la infraestructura que se muestra en las figuras del anexo "A" de esta propuesta y se describe a continuación.

La operación de la estructura de la red de informática está integrada por una delta de ATM, unida con la infraestructura propia de La Empresa basada en fibra óptica como medio físico. Esta delta es el medio de transporte de red de alta capacidad e interconecta las tres localidades que están distribuidas en el área metropolitana.

La delta de ATM además de ser el medio a través del cual se efectúa la conexión a nivel metropolitano, también se encarga de unir a los 7 edificios ubicados en la calle "X" como se puede apreciar en la figura 3.1. Aquí se cuenta con 1 enrutador de la familia Cisco 7000 y 5 concentradores de cableado Cabletron MMAC-8FNB, que están conectados al conmutador de paquetes ATM modelo ASX-200 de FORE Systems y que están ubicados en la planta baja de los edificios "RS", "ST",

"VW", "WX" y en el sótano del edificio "U". Las características tanto de los enrutadores como de los concentradores de cableado se mencionan más adelante.

Para proporcionar la conectividad hacia todos los nodos remotos de La Empresa, se utiliza un enrutador Cisco 7000, en el Centro de Control de la Red, mediante el cual se puede establecer comunicación con los 32 sitios remotos utilizando para ello como medio de transporte la red satelital con la que cuenta actualmente La Empresa. En cada uno de estos sitios remotos se cuenta con un enrutador Cisco 2501, para manejar las redes locales requeridas en cada uno de estos centros.

Una funcionalidad de vital importancia en los equipos de enrutamiento propuestos para cada uno de los sitios remotos, es el hecho de que estos equipos pueden llevar a cabo la función de marcaje por demanda mediante uno de sus puertos síncronos o asíncronos, a través de un enlace por medio de línea conmutada. Lo anterior garantiza la conectividad continua, ya que en caso de que se presente una falla en el enlace satelital, se podrá establecer automáticamente un segundo enlace por línea conmutada a través del cual se podrá enrutar todo el tráfico hacia la columna vertebral de la red. Además, esta funcionalidad es útil aun y cuando el

enlace primario permanezca activo, ya que esta funcionalidad se puede configurar para que cuando el enlace primario llegue a cierto grado de saturación, se establezca la segunda conexión y se realice el balanceo de la carga entre ambos enlaces.

5.2.1 Dimensionamiento de Equipos

Edificio Central "D"

En este edificio se encuentra ubicado el centro de control de toda la red. Es aquí donde se concentrará la mayor parte del equipo así como la administración y el control de la misma. Para poder efectuar la comunicación hacia los nodos remotos se contará con un enrutador de la familia Cisco 7000, que se encargará de manejar los 32 enlaces seriales y del acceso de estos mismos a la red de ATM. En esta misma ubicación estarán dos conmutadores de ATM de FORE Systems los cuales forman parte del backbone de ATM. A través de éstos se logra la conectividad de todos los servidores y los concentradores de cableado de Cabletron que a su vez integran a las distintas redes de cada uno de los edificios de la Calle "X".

De esta manera se presenta una solución más robusta y más confiable para La Empresa.

Adicionalmente, se considera la implantación de un concentrador de cableado Cabletron MMAC-8FNB, el cual ofrecerá la capacidad de manejar las redes locales de este edificio en forma independiente. Este concentrador incluye fuente de alimentación y fuente redundante, un módulo de administración Ethernet, y tarjetas con puertos Ethernet con interfaces RJ-45 y una tarjeta para manejar la red TokenRing que se encuentra en el edificio "V".

Acceso Edificios: "RS", "ST", "VW" y "WX"

Para estos edificios proponemos utilizar un concentrador de cableado Cabletron MMAC-8FNB para cada uno, el cual ofrecerá la capacidad de manejar las redes locales de estos edificios. Por otra parte, este concentrador estará conectado al conmutador ATM a través de una Brim para ATM-SONET a 155 Mbps. Este concentrador incluye fuente de alimentación y espacio para fuente redundante, un módulo de administración Ethernet y puertos Ethernet con interfaces RJ-45.

En estos accesos se propone el uso de un UPS de 1250 VA que es montable en rack.

Edificio "Z"

Dentro del edificio denominado "Z" se contará con un conmutador de paquetería de la marca FORE Systems modelo ASX-200, el cual se conectará a otro conmutador igual en el edificio de la Calle "X".

Adicionalmente se propone utilizar cuatro concentradores de cableado Cabletron MMAC-8FNB, los cuales ofrecerán la capacidad de manejar las redes locales de este edificio. Estos concentradores estarán conectados al conmutador ATM a través de una Brim para ATM-SONET a 155 Mbps. Estos concentradores incluyen fuente de alimentación y espacio para fuente redundante, un módulo de administración Ethernet y puertos Ethernet con interfaces RJ-45.

En este mismo edificio se propone el uso de un UPS de 1250 VA para cada uno de los concentradores de cableado.

Edificio "Y"

Para el Edificio "Y" se propone el uso de un LAX-20 de Fore Systems el cual conectará al conmutador ATM ASX-200 que se encuentra en la Calle "X" y que permitirá el acceso de los concentradores de cableado ya existentes, para así poder integrar los equipos actuales al nuevo esquema de red.

Sitios Remotos

Para el caso de los 32 sitios remotos se proponen 32 enrutadores Cisco 2500 con software Desktop, que cuentan con dos puertos Seriales y un puerto Ethernet.

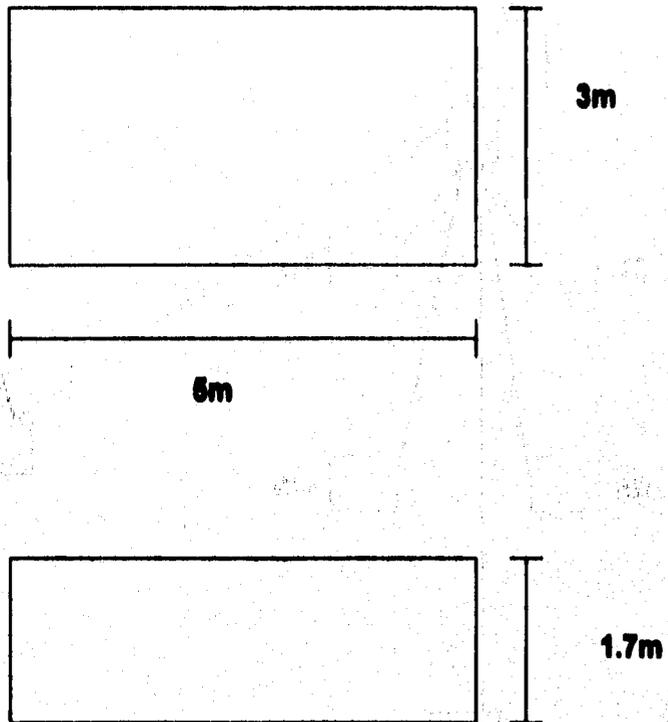
5.3 Inspección del sitio para montaje de estaciones.

Para la inspección del sitio se consideraron los siguientes puntos:

- Descripción física
- Descripción de energía
- Fuentes de interferencia

5.3.1 Descripción física

Para el montaje físico de los equipos se tiene contemplado el siguiente espacio físico en los accesos:

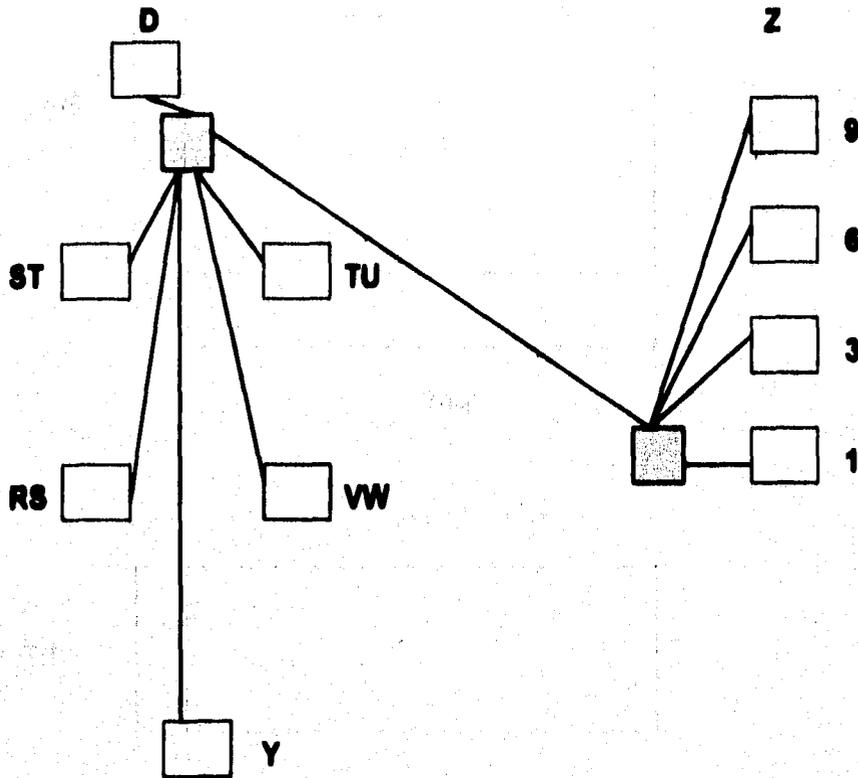


5.3.2 Instalación Eléctrica

EDIFICIOS	VOLTAJE	
	Min	Max
RS	110 V	131 V
ST	112 V	127 V
TV	112 V	128 V
VW	120 V	128 V
WX	113 V	128 V

5.3.3 Fuentes de Interferencia

El medio físico utilizado fue fibra óptica, y ya que ésta no sufre interferencia, se realizó un cálculo de pérdida.



U - TU	EMPALMES	3	CONECTORES	6
U - VW	EMPALMES	3	CONECTORES	6
U - ST	EMPALMES	3	CONECTORES	6
U - RS	EMPALMES	3	CONECTORES	6
Z - 9	EMPALMES	2	CONECTORES	4
Z - 6	EMPALMES	2	CONECTORES	4
Z - 3	EMPLAMES	2	CONECTORES	4

5.4 Características de los equipos

5.4.1 Características técnicas de enrutadores Cisco

5.4.1.1 Arquitectura Modular

El Cisco 7000 tiene 5 ranuras de expansión y dos ranuras más para el procesador de conmutación y el procesador de enrutamiento, tarjetas que ya vienen incluidas en el chasis.

El Cisco 7010 tiene 3 ranuras de expansión y dos ranuras más para el procesador de conmutación y el procesador de enrutamiento, tarjetas que ya vienen incluidas en el chasis.

Crecimiento por Tarjetas

Para el Sistema 7000 y 7010:

- Tarjetas de 4 y 8 puertos seriales que soportan velocidades de hasta 8 Mbps. Las interfaces que manejan son: V.35, RS-232, RS-449 y X.21.
- Tarjetas de 2,4,y 6 puertos Ethernet
- Tarjetas de 2 y 4 puertos Token Ring
- Tarjetas de 1 puerto FDDI, multimodo y monomodo

5.4.1.2 Capacidad de Procesamiento

- Contiene tres tipos de procesadores diferentes: El procesador de conmutación, el procesador de enrutamiento y los procesadores de interface, cada tarjeta de interface contiene su propio procesador.

5.4.1.3 Capacidad de Memoria Real

- 16 MB en memoria RAM (Dynamic Random Acces Memory)
- 2 MB en memoria ROM (Read-Only Memory)
- 4 MB en memoria FLASH para microcódigo y actualizaciones de software
- 128 KB en memoria dinámica de acceso no volátil (RAM no volátil)

5.3.1.4 Capacidad de Memoria Caché

En el Cisco 7000 y el 7010 como se ha mencionado, existen tres tipos de procesadores diferentes. El procesador de conmutación contiene 128 KB de memoria de rápido acceso (Speed RAM), la cual es usada solamente por la unidad lógica del procesador. Asimismo, contiene 512 KB de buffer compartido

entre el procesador de conmutación y los procesadores de interface. Dicho buffer es utilizado para almacenar paquetes de información provenientes de la red así como las estructuras de control de los procesadores de interface. Cuando un procesador de interface recibe un paquete, lo almacena en este buffer para que el procesador de conmutación, posteriormente lo envíe. Esto evita que se tenga información "repetida" en cada procesador, de manera que el desempeño del sistema es más eficiente.

5.4.1.5 Tipo de Microprocesador

El procesador de conmutación está basado en un procesador "bit-slice" que ejecuta 16 millones de instrucciones por segundo (MIPS) con un conjunto de instrucciones especiales. Este procesador tiene una sola función: Decidir el destino de un paquete y enviarlo en base a esta decisión. Modifica la dirección de salida del paquete y almacena los diferentes paquetes destinados a la misma interface de salida. Este procesador es la parte medular del Cisco 7000.

Los procesadores de interface que son el enlace físico inteligente entre el Cisco 7000 y la red utilizan la tecnología "bit-slice", lo que permite ejecutar cierto número de operaciones en paralelo de una sola instrucción dada.

5.4.1.6 Fuente de poder

El Cisco 7000 tiene la capacidad de manejar fuente de poder redundante. El Cisco 7000 es totalmente redundante y "hot-swappable". Cada fuente de poder tiene su propio conmutador de poder y su propio cable. La operación de cada una de las fuentes es visible a través de LED's, localizados en el panel frontal. Cuando los dos sistemas son usados, automáticamente cargan y comparten, cada uno proveyendo el 50% del suministro de energía eléctrica usada por el sistema. Estas fuentes de poder, automáticamente ajustan el voltaje de entrada entre los 100 y los 240 volts y las frecuencias entre los 50 y 60 HZ, lo que permite que este tipo de fuentes, sean usadas en cualquier país.

5.4.1.7 Procesador Central

El Cisco 7000 maneja tres tipos de procesadores: El procesador de conmutación, el procesador de enrutamiento y los procesadores de interface.

El procesador de conmutación es el que ejecuta las funciones principales de enrutamiento está basado en una arquitectura de unidad lógica de 16 bits y contiene 64 registros internos que proveen un poder de procesamiento mucho más eficiente que cualquier otro procesador. El procesador de conmutación contiene 40 KB de memoria de almacenamiento para el conjunto de instrucciones de la unidad lógica, el cual puede ser descargado de la memoria ROM o de la memoria FLASH del procesador de enrutamiento. La memoria de la unidad

lógica está diseñada para considerar cualquier tipo de crecimiento en el conjunto de instrucciones. El procesador de conmutación contiene también 128 KB de memoria de acceso rápido (memoria caché).

Cada tarjeta de interface contiene su propio procesador, llamado procesador de interface. Su arquitectura permite un pre-procesamiento de los paquetes rápido y eficiente, así como el rápido movimiento de la información desde la interface de red hacia el procesador de conmutación. Manejan todas las tareas de nivel de enlace asociadas con la interface física hacia la red. Todas las conexiones de la red están directamente enlazadas a los procesadores de interface.

5.4.1.8 Servicios de conmutación de circuitos

Las velocidades de interface de conexión a TELMEX son :

- 1200 bps (Síncronos y Asíncronos)
- 2400 bps " "
- 9600 bps " "
- 19200 bps " "
- 56/64 bps (Síncronos)
- ISDN Basic Rate ≈ Mbps
- ISDN Primary Rate 64 Kbps

5.4.1.9 Servicios de conmutación de paquetes

Protocolos de conmutación de paquetes que serán soportados:

- X.25
- Frame Relay
- SMDS
- DDN X.25

5.4.1.10 Interfaces Seriales

Interfaces físicas para las localidades remotas:

- RS-232/V.24
- RS-449
- X.21
- V.35
- G.703
- HSSI
- NRZ o NRZI
- DCE o DTE
- Velocidades hasta 8Mbps, 52Mbps

5.4.1.11 Interfaces de Área Local (LAN)

Las interfaces de área local son:

- Ethernet 802.3 y v2: AUI o 10BaseT
- FDDI: Multimodo/Monomodo
- Token Ring IEEE 802.5: 4/16Mbps
- UltraNet

5.4.1.12 Protocolos de Transmisión de Área Extendida (WAN)

Los protocolos de transmisión de área extendida son:

- HDLC (High-level Data Link Control)
- PPP (Point to Point)
- LAPB
- HDH (HDLC Distant Host)
- SMDS
- LAPB
- Frame Relay
- X.25
- T1/E1, T3/E3
- TCP/IP Header Compression
- Priority Output Queuing
- Dial Backup and Load Sharing
- Enrutamiento Dial-on-Demand via V.25bis (para Circuit Switching)

5.4.1.13 Protocolos de Área Local (LAN)

Los protocolos de área local son:

- TCP/IP
- NetBIOS
- SNA
- Transporte SDLC
- Conversión SDLC a Token Ring LLC-2 (SDLLC)
- LAN Network Manager
- Novell IPX
- Apple Talk (Phase I y Phase II)
- Banyan VINES
- DECnet (Phase IV y Phase V)
- 3Com 3+/3+Open
- ISO CLNS (OSI)
- Xerox XNS

- Ungermann-Bass Net/One
- Apollo Domain
- Xerox PUP
- CHAOSnet
- HP Advancenet

5.4.1.14 Protocolos de Enrutamiento

Los protocolos de enrutamiento son:

- Apple Talk Routing Table Management Protocol (RTMP)
- Border Gateway Protocol (BGP)
- DECnet Phase IV Routing
- Exterior Gateway Protocol (EGP)
- Interior Gateway Routing Protocol (IGRP)
Este protocolo optimiza al máximo el rendimiento del ancho de banda de transmisión de datos al menor costo.
- IGRP Intermediate System to Intermediate System (OSI ES-IS)
- IGRP Intermediate System to Intermediate System (IGRP IS-IS)
- Novell IPX RIP
- Open Shortest Path First (OSPF)
- Open System Interconnect End System-Intermediate System (OSI IS-IS)
- Routing Information Protocol (RIP)
- VINES Routing Table Protocol (RTP)
- XNS RIP

5.4.1.15 Protocolos de Administración de Red

Los protocolos de administración de red son:

- Simple Network Management Protocol (SNMP)
- Telnet Remote Acces
- Priority Output Queuing
- Maintenance Operation Protocol (MOP) Remote Acces
- Control de seguridad por nombre de usuario/password
- Listas de acceso por enrutamiento
- Filtraje administrativo (puenteo)
- Comandos "Debug"
- Comandos "Ping"
- Syslog Event Logging
- Acceso remoto y seguridad TACACS
- Performance Tuning

5.4.1.16 Seguridad

Las medidas de seguridad que se consideraron son las siguientes :

- Fuente de poder redundante
- Reemplazo de tarjetas de interface, en operación
- Monitoreo y reporte de las condiciones ambientales
- LED's indicadores por cada una de las tarjetas de interface
- FLASH EPROM. Minimiza el costo de administración de la red, ya que permite tener varias configuraciones ofreciéndole al administrador la posibilidad de escoger la más conveniente. Asimismo, cualquier actualización del sistema operativo de cualquier enrutador remoto, puede realizarse desde un punto centralizado.
- Puerto de consola auxiliar que permite configuraciones remotas vía modem.
- No tienen algún componente eléctrico activo en el bus de datos, es decir, los conectores del backplane son hembras, lo que garantiza que ningún componente del backplane se pueda descomponer.
- Posee un filtro removible que garantiza el constante flujo de aire limpio dentro del sistema.
- Aprobaciones de seguridad y de emisiones manejadas por el enrutador, que incluyen la EN55022 (CISPR Clase B) para Europa y para los estándares japoneses en la VCCI Clase 2.
- Cumple con los estándares para golpes y vibraciones de la IEC.
- Filtraje de paquetes basado en direcciones de anfitriones, direcciones de subred y clase de dirección
- Filtraje de paquetes basado en tipo de protocolo y socket de aplicación
- Listas de acceso
- IPSO (DOD customers only)
- Dos niveles de password
- Encriptamiento de password
- Autenticación de la llamada a nivel PPP
- Prioridades de protocolos

5.4.1.17 Punteo

Las características de punteo son:

- Transparent Bridging
 - * IEEE 802.1 (d) Spanning Tree Algorithm
 - * DEC Spanning Tree
- Source-Route Bridging
- Remote Source-Route Bridging
- Translational Brindging (Ethernet, Token Ring y FDDI)
- Source-Route Transparent Bridging
- FDDI Encapsulation Bridging

5.4.1.18 Soporte TCP/IP cubriendo los siguientes RFC's

*RFC 768	*RFC 877	*RFC 1034	*RFC 1161
*RFC 779	*RFC 879	*RFC 1035	*RFC 1163
*RFC 783	*RFC 891	*RFC 1042	*RFC 1164
*RFC 791	*RFC 894	*RFC 1055	*RFC 1166
*RFC 792	*RFC 896	*RFC 1058	*RFC 1171
*RFC 793	*RFC 903	*RFC 1060	*RFC 1184
*RFC 813	*RFC 904	*RFC 1069	*RFC 1188
*RFC 815	*RFC 906	*RFC 1079	*RFC 1191
*RFC 826	*RFC 919	*RFC 1080	*RFC 1195
*RFC 827	*RFC 922	*RFC 1091	*RFC 1196
*RFC 854	*RFC 925	*RFC 1101	*RFC 1212
*RFC 855	*RFC 950	*RFC 1108	*RFC 1213
*RFC 856	*RFC 951	*RFC 1136	*RFC 1238
*RFC 857	*RFC 982	*RFC 1139	*RFC 1247
*RFC 858	*RFC 994	*RFC 1141	
*RFC 860	*RFC 995	*RFC 1144	
*RFC 862	*RFC 1009	*RFC 1155	
*RFC 863	*RFC 1027	*RFC 1157	

5.4.1.19 Características de mantenimiento de TCP/IP

- Opciones de configuración de TCP/IP para incluir listas de conteo y umbrales, direcciones default de la red, nombres default del servidor y lista de protocolos a manejar por ejemplo: TFPT, DNS y Boot P.
- Comandos de mantenimiento para las estructuras de datos de enrutamiento.
- Monitoreo para poder desplegar información importante de estado y estadística, estado de enlaces e interfaces, procesos de enrutamiento, tabla de enrutamiento y estadísticas de tráfico.
- Desplegado de información de conteo, incluyendo el número de bytes y paquetes conmutados a través del sistema sobre una base fuente y destino.
- Desplegado de información de interface incluyendo la información completa de estados y parámetros con respecto a las interfaces físicas del enrutador. Los elementos incluyen: Dirección de difusión, tamaño MTU, direcciones de ayuda, listas de acceso, nivel de seguridad y otros ajustes de parámetros clave.
- Desplegado de parámetros de enrutamiento para incluir información detallada en el tiempo de espera, filtros y métricas de enrutamiento.
- Desplegado de las tablas de enrutamiento.
- Desplegado de estadísticas de tráfico TCP/IP incluyendo los paquetes enviados o recibidos por los tipos de paquetes IP, ICMP, UDP, EGP, ARP y condiciones de error incluyendo errores de formato, de "checksum" e intentos bloqueados por seguridad.

Nota: Además de estas características de mantenimiento, los enrutadores Cisco cuentan con herramientas "debug":

- Debug de altas para desplegar las transacciones de alta en el enrutador
- Ping TCP/IP
- Discard Service
- TCP/IP Trace para descubrir la trayectoria que tomaron los paquetes al cruzar por la red

5.4.1.20 Características de soporte OSI

- Habilidad de filtraje de información de salida en diferentes máscaras de direcciones (ejemplo: dirección específica de un anfitrión o múltiples direcciones de anfitriones).
- Además, los enrutadores CISCO soportan los siguientes estándares OSI:

- | | |
|--------------------------|---------------------------|
| - ISO 7498/Ad1 | - ISO 8802/3 (IEEE 802.3) |
| - ISO 8208 | - ISO 8802/5 (IEEE 802.5) |
| - ISO 8348/Ad1 | - ISO 8878 |
| - ISO 8348/Ad2 | - ISO 9068 |
| - ISO 8473 | - ISO 9542 |
| - ISO 8473/Ad1 | - ISO 10589 |
| - ISO 8648 | - MAP 3.0 |
| - ISO 8802 | - NIST SP 500-162 |
| - ISO 8802/2(IEEE 802.2) | |

- Habilidad de modificar de manera interactiva los parámetros:

- Métrica de enrutamiento
- Area
- Sin de sistema vecino
- Dirección
- Tiempo de vida de un paquete
- Reporte de errores

5.4.1.21 Características de soporte de Novell IPX

- RIP
- Difusión a todas las redes
- Enrutamiento estático
- Protocolo de datagramas inter-redes (IDP)
- Encapsulamiento de Novell
- Filtraje de paquetes basándose en los criterios de dirección, fuente, destino, y protocolo

- Socket de la aplicación
- Protocolo de aviso de servicio (SAP)
- Habilitación/Deshabilitación del enrutador
- Número máximo de trayectorias alternas
- Establecer actualizaciones de timers y filtros incluyendo actualizaciones RIP y temporizadores SAP en una interface.
- Filtrado por campos SAP y RIP
- Comandos para mantener estructuras de datos de enrutamiento (limpiar interfaces)
- Monitoreo de Novell para desplegar información de la interface, rutas, enrutamiento caché, servidores, mapa de la red y estadísticas de tráfico
- Despliegue de información de la interface para incluir el estado de las interfaces físicas del enrutador
- Despliegue de servidores Novell
- Despliegue de los parámetros de enrutamiento incluyendo cómo se obtuvo la ruta (RIP, estática, conectada o aprendida) y declarar el número máximo o permitido de trayectorias
- Despliegue de estadísticas de tráfico para proporcionar información total de datos, broadcast, petición SAP y paquetes enviados y recibidos desconocidos. Además, errores de formato, errores checksum, paquetes con conteo de saltos erróneos y otros paquetes no válidos.
- Bitácora de tráfico de datagramas y próximo salto a enrutador de cada datagrama.

5.4.1.22 Certificado de Aprobación

Normas de homologación internacionales:

- UL
- CSA
- TUV GS mark
- EN 60 950
- EN 55 022 (CISPR 22 Class B)
- FCC Class A
- VDE
- Canadian DOC Class A

5.4.1.23 Confiabilidad

La siguiente tabla muestra el tiempo promedio entre fallas de los equipos que se seleccionaron (MTBF, Mean Time Between Failure):

PRODUCTO	DESCRIPCION	HRS	AÑOS
<i>Plataforma Cisco</i>			
7000	Backplane	556,178	64.6
	Manejador de Bus	565,490	64.6
	Tarjeta de LED	5,266,497	601.2
PWR-7K	Fuente de poder	171,115	19.5
RP	Procesador de enrutamiento	65,789	7.5
SP	Procesador de conmutación	59,263	6.8
PWR-7K	Fuente de poder primaria	18,541	2.1
PWR-7K/2	Fuente de poder redundante	19,236	2.2
CX-FIP-MM	Tarjeta FDDI con puerto para fibra multimodo	88,650	10.1
CX-EIP2	Tarjeta con 2 puertos Ethernet	95,282	10.9
CX-EIP4	Tarjeta con 4 puertos Ethernet	85,517	9.8
CX-EIP6	Tarjeta con 6 puertos Ethernet	74,337	8.5
PRE-FSIP4-X21	Tarjeta con 4 puertos seriales con interface X.21	2,927,434	334.2
PRE-FSIP4-V35	Tarjeta con 4 puertos seriales con interface V.35	2,828,865	322.9
PRE-FSIP4-232	Tarjeta con 4 puertos seriales con interface RS-232	2,915,672	332.8
PRE-FSIP4-449	Tarjeta con 4 puertos seriales con interface RS-449	2,185,339	249.5
CX-TRIP2	Tarjeta con 2 puertos Token Ring	63,342	7.2
CX-TRIP4	Tarjeta con 4 puertos Token Ring	42,618	4.9
Servidor de Comunicaciones			
ASMn-CS	Servidor de Comunicaciones	259,013	29.6
508-CS	Servidor de Comunicaciones de 8 puertos	8 807,000	92.1

5.4.2 Características técnicas de los equipos Cabletron

5.4.2.1 Arquitectura de red

Arquitectura de Red Integrada (INA), que permite integrar todo tipo de componentes de red, sin importar el medio utilizado y compatibles con los principales estándares internacionales de redes.

Permite la evolución y la expansión de la red en forma transparente de acuerdo a las necesidades del usuario o al ingreso al mercado de nuevas tecnologías.

Conectividad entre redes de Area Local (LAN) y Redes de Area Extendida (WAN) para formar una red global empresarial.

La solución completa de red está basada en tres productos:

- Concentrador de cableado Centro de Acceso a Medios Múltiples (Multi Media Acces Center MMAC).

Cabletron introdujo su tecnología de bus en backplane en 1989, conocido como Bus de Red Flexible (FNB). Desde su introducción, varias tecnologías de red diferentes, incluyendo Ethernet, Token Ring y FDDI pueden ser soportadas y operar en un chasis MMAC. Este soporte se logra con la tecnología avanzada del backplane FNB de 650 Mb/s, que no contiene circuitos activos y por lo tanto no es un punto de falla.

El Bus de Red Flexible (FNB) del concentrador MMAC tiene la capacidad de soportar tecnologías existentes tales como Token Ring, Ethernet, FDDI y conexiones WAN, así como tecnologías en desarrollo como SONET (ATM).

La plataforma de administración de microprocesador RISC ofrece una arquitectura de 32 bits con una velocidad de reloj de 25 MHz que permitirá aplicaciones sencillas y sofisticadas de administración que corran en el panel de cableado. Otros fabricantes utilizan el 80186 que solamente soporta 1 Megabyte de memoria lo cual limitará la administración futura. La implementación de Cabletron con el RISC 1980 permite acceso hasta 1 Gigabyte de memoria.

Poseen una Arquitectura de Red Integrada (INA) con lo cual proporcionan una administración de red centralizada y conectividad para cualquier Red de Area Local (LAN) o Red de Area Extendida (WAN) estándar, que utilice cualquier combinación de medios estándar.

5.4.2.2 Características

- Compatibilidad con productos basados en estándares de cualquier fabricante.
- Conexión y administración de cualquier combinación de redes Ethernet, Token Ring, FDDI y de Redes de Area Local (LAN) o de Redes de Area Extendida (WAN) desde un mismo punto central.
- Modularidad para realizar expansiones y diagnosticar fallas rápida y fácilmente.
- Control y monitoreo completo de toda la red con cualquier sistema de administración que cumpla con el protocolo SNMP.
- Diseño tolerante a fallas.
- Fuentes de alimentación redundantes
- Más de 50 módulos para todas las necesidades.
- Tres tamaños de chasis
- Aceptado por otros fabricantes como el concentrador industrial estándar.

5.4.2.3 Estándares de Red

- Ethernet
- Token Ring
- FDDI

5.4.2.4 Concentradores MMAC's

La línea de concentradores de cableado del centro de acceso a medios múltiples siendo los más recientes para el diseño de INA de Cabletron, proporcionará una administración centralizada, con conectividad para cualquier Red de Area Local (LAN) o Red de alcance remoto (WAN) estándar, que utilice cualquier combinación de tipos de medios estándar.

El MMAC, diseñado para cumplir todos los estándares principales de las industrias para redes Ethernet, Token Ring y FDDI, siendo uno de los concentradores más reconocidos en el mundo.

Los principales fabricantes de redes, tales como Cayman Systems, Novell, SGI, Xyplex y otros, que han reconocido la necesidad de redes con capacidad de extensión y con capacidad de integrar equipo proveniente de múltiples fabricantes, han elegido integrar sus productos standalone en el concentrador MMAC de Cabletron. Más y más fabricantes de redes consideran al MMAC de Cabletron como el concentrador estándar de la industria.

5.4.2.5 Funciones generales

5.4.2.5.1 Interoperabilidad

El MMAC, basado en la INA de Cabletron, es compatible con todos los productos basados en los estándares actuales de cualquier fabricante. Su diseño abierto a las diferentes normas lo hace el candidato ideal para la integración con los productos de otros fabricantes.

5.4.2.5.2 Flexibilidad

La mayoría de los concentradores están diseñados con un papel de interconexiones para una Red de Area Local (LAN) específica, que opera sólo con determinados protocolos. Los concentradores MMAC de Cabletron están diseñados con el exclusivo Bus de red flexible (FNB), un papel de interconexiones independiente del protocolo que permite operar y controlar desde un mismo punto central, cualquier combinación de redes Ethernet, Token Ring, FDDI y Redes de Area Local (LAN) o Redes de alcance remoto (WAN) Local Talk.

5.4.2.5.3 Adaptabilidad

Como la tecnología de redes evoluciona tan rápidamente, las redes instaladas hoy en día experimentarán, inevitablemente, importantes cambios en el futuro próximo. Debido a que el MMAC-8FNB es en realidad independiente del protocolo, permite que se perfeccionen los sistemas a medida que se desarrollen nuevos tipos de redes de área local (LAN), mejores y más rápidas. Ningún otro producto de la industria de redes tiene las capacidades de adaptabilidad que presenta el concentrador MMAC-FNB de Cabletron.

5.4.2.5.4 Modularidad

La modularidad del MMAC permite realizar expansiones y diagnósticos de fallas de manera rápida y fácil. Todos los componentes electrónicos del MMAC se pueden reemplazar localmente sin la necesidad de herramientas o equipos especiales. Los módulos defectuosos se pueden aislar del resto de la red. Debido a que se pueden instalar fácilmente nuevos módulos, la red puede seguir creciendo.

Los usuarios también pueden reemplazar tarjetas de medios y fuentes de alimentación sin tener que desactivar el equipo, para así reducir el tiempo inactivo de la red al expandir o diagnosticar fallas del equipo.

5.4.2.5.5 Redundancia

Cabletron es el único fabricante en todo el mundo que proporciona redundancia de redes en dos formas. La primera asegura que todas las conexiones de datos tengan dos canales de reserva. Este método permite que los servidores críticos, nodos o redes principales tengan múltiples canales de datos en uno o más centros de acceso a medios múltiples (MMAC). En caso de que produzca una falla en el canal de datos, el canal secundario entra en acción (sin que el usuario lo perciba), de modo que no se interrumpen las comunicaciones.

La segunda forma se refiere a la habilidad de los MMAC-5FNB y MMAC-8FNB para repartir la carga de la fuente de alimentación. Ambos concentradores MMAC aceptan múltiples fuentes de alimentación administrables mediante software, lo que asegura que exista una potencia totalmente redundante a lo largo del BUS de red flexible (FNB) del concentrador MMAC. Su capacidad de repetición de carga también prolonga la vida útil de todas las fuentes de alimentación del MMAC, ya que ninguna fuente se verá obligada a funcionar a toda su capacidad.

5.4.2.5.6 Capacidad de Administración

Las verdaderas bases que sustentan el MMAC son sus poderosas capacidades de administración de redes que permiten a los usuarios administrar una red mundial desde un solo punto central. El MMAC proporciona características completas de monitoreo y control al usar cualquier sistema de administración que cumple con el SNMP, incluyendo Remote LANVIEW o SPECTRUM, nuestro sistema avanzado de administración. Al usar estos paquetes, se puede administrar el MMAC desde cualquier conexión de la red en cualquier lugar del mundo.

Los usuarios del concentrador MMAC pueden administrar un gran conjunto de productos administradores de Cabletron, incluyendo puentes locales y remotos, productos de análisis y tarjetas de interface de red de computadoras personales (DNI) que son tarjetas que se enchufan para enlazar estaciones de trabajo a la red. Debido a que todos los productos de Cabletron funcionan con el protocolo simple de administración de red (SNMP), toda la solución de red se puede administrar completamente desde una única estación de administración.

5.4.2.6 Características

- * Es compatible con todos los productos basados en los estándares de cualquier fabricante.
- * Permite conectar y administrar cualquier combinación de redes Ethernet, Token Ring, FDDI y de Redes de área local (LAN) o de redes de alcance remoto (WAN) LocalTalk desde un mismo punto.
- * El diseño modular permite realizar expansiones y diagnosticar de manera fácil y rápida.
- * Proporciona control y monitoreo completo de toda la red al usar cualquier sistema de administración que cumpla con el SNMP.
- * El diseño tolerante a fallas protege las transmisiones de datos.
- * Las fuentes de alimentación redundantes reducen el tiempo inactivo de la red y aumentan la vida útil de cada fuente de alimentación.
- * Actualmente, se ofrecen más de 50 módulos para los concentradores MMAC.
- * Hay tres tamaños de chasis para elegir.
- * Aceptado por otros fabricantes como el concentrador industrial estándar.

5.4.2.7 Descripción

El chasis MMAC-5FNB ofrece muchas características exclusivas. Es capaz de alojar un módulo de administración/repetidor y hasta cuatro módulos de interface de medios (MIM). Funciona con un sólo módulo de alimentación, (MMAC-5FNB) y adquiere capacidad redundante agregándole otro. Todo acceso al MMAC-5FNB se realiza por la parte delantera de la unidad, incluyendo el módulo de

alimentación MMAC-5FNB y la gaveta del ventilador. Al utilizar las tarjetas (MIM) de alta densidad de Cabletron hay capacidad de hasta 131 puertos por chasis MMAC-5FNB. Al igual que todo chasis de MMAC, el bus de red flexible (FNB) permite que se integren, múltiples redes Ethernet, Token Ring y FDDI en un mismo chasis.

5.4.2.8 Capacidades

Concentrador de cableado de 5 ranuras MMAC-5FNB

- * Un módulo de administración/repetidor.
- * Hasta 4 módulos de interface de medios (MIM).
- * Hasta 131 puertos.
- * Fuente de alimentación principal.
- * Fuente de alimentación redundante/repartición de carga.
- * Bus de red flexible.
- * Dimensiones: 33,2 cm de altura x 43,28 cm de ancho x 40,00 cm de profundidad.
- * Peso: (8 kgs.)
- * Tiempo medio entre fallas (MTBF): 4,267,368 horas.

5.4.2.9 Arquitectura del Módulo de Administración

5.4.2.9.1 Procesador RISC i960

- * Boot EPROMS.
- * Memoria no volátil.
- * Memoria Buffer (4 Mb).
- * 4 Memoria de Operación (4 Mb).
- * RAM estática de 256 KB (Fast RAM).
- * Estado del arte en el diseño.

El procesador i960 es 15 veces más poderoso que el 80186.

5.4.2.9.2 Flash EPROMS

- * Imagen guardada en Memoria Flash dentro de los concentradores (dispositivos).
- * Permite nueva funcionalidad siendo fácilmente instalada en cualquier momento.
- * Los usuarios de la red no son interrumpidos al instalar la nueva imagen.
- * No requiere Módulo de Administración para instalar en encendido.
- * Todos los parámetros de configuración son siempre guardados en batería de memoria de respaldo.

5.4.2.10 Estándares de Seguridad

- * UL478
- * UL910
- * NEC 725-2(b)
- * CSA
- * IEC
- * TUV
- * Clase A de VDE
- * Límites de clase A, Sección 15, FCC

5.4.2.11 Fuentes de Alimentación Redundantes

El centro de acceso a medios múltiples MMAC_5FNB ofrece módulos de fuente de alimentación redundantes (Power Supply Modules, PSM). Y el módulo MMAC-5PSM alimenta al chasis respectivamente. Cuando hay dos de estos módulos de fuente de alimentación (PSM) en el chasis, proporcionan una fuente de alimentación redundante. Si una de las fuentes falla, el otro PSM continúa proporcionando potencia al chasis y envía un mensaje a la estación de administración de la red. Esta característica de redundancia asegura que el chasis del MMAC funcione adecuada e ininterrumpidamente.

- * La unidad de redundancia MMAC-5PSM suministra potencia al chasis, la cual cuenta con una conexión en línea de AC individual y con diodos emisores de luz (LED) LANVIEW para verificar a simple vista el estado de la unidad, los módulos se pueden reemplazar sin desactivar el equipo, para así no afectar su funcionamiento.
- * Permiten un máximo tiempo activo de la red.
- * Repartición de carga que prolonga la vida útil de cada módulo de fuente de alimentación.
- * Reemplazo sin desactivar la red.
- * Diagnóstico mediante emisores de luz (LED).

5.4.2.12 Módulos para la administración de redes

Características:

- Proporciona control y estadísticas a nivel de puerto para los módulos de interface de medios de Token Ring Cabletron.

- La CPU I960 RISC de Intel proporciona un procesamiento de alta velocidad de 32 bits para las aplicaciones de administración actuales y futuras.
- La repercusión automatizada de beacon restaura los anillos que tienen adaptadores defectuosos y cables que originan condiciones de beacon.
- Identifica los nodos que causan errores de software que "atascan" el flujo de información de la red y disminuyen el desempeño del sistema.
- Se administra mediante el SNMP con soporte MIB "Standar" y "Enterprise" (de empresa).
- Memoria programable EEPROM tipo Flash permite actualizar fácilmente los módulos.
- Diodos emisores de luz (LED) LANVIEW permiten verificar a simple vista el estado del módulo y de la red.
- Cumple con el estándar IEEE 802.5 y es compatible con redes Token Ring de IBM.
- En forma automática, crea mapas de anillos que señalan las direcciones de la estación, los nombres y la secuencia de anillo.

5.4.2.13 Módulo repetidor multicanal Ethernet.

Estos son módulos integrados de repetidores Ethernet y de conectividad de cable de par trenzado 10 base-T, diseñados para los concentradores MMAC-FNB y equipados con el nuevo Módulo de administración Ethernet (EMME). Estos módulos proporcionan dos canales adicionales Ethernet al panel de interconexiones MMAC-FNB: Los canales B y C. Los módulos se pueden configurar para los canales Ethernet B o C, o bien para el modo standalone.

Cuando se configuran de ese modo, el MMAC-FNB tiene capacidad de hasta siete segmentos repetidos en forma separada.

Cada TRPMIM viene con un módulo de interface de puerto Ethernet (EPIM) que permite a los usuarios configurar el módulo con un puerto único para una variedad de tipos de medio.

5.4.2.13.1 Características

Módulo TPRMIM-20/22/33/36

- * Módulos repetidores Ethernet con conectividad 10 Base-T en par trenzado.
- * Módulos multicanal para conexión a dos segmentos del backplane de los MMAC-FNB o standalone.
- * Dispone de un Módulo de Interface de Puerto Ethernet (EPIM) que permite configurarse para cualquier tipo de medio (ver EPIM).
- * Número de puertos:
 - TPRMIM-20:9 puertos RJ45, 1 EPIM
 - TPRMIM-22:21 puertos RJ45, 1 EPIM
 - TPRMIM-33:13 puertos (1 Telco de 50 pin, 1 EPIM)
 - TPRMIM-36:26 puertos (2 Telcos de 50 pin, 1 AUI, 1 EPIM)

5.4.2.14 Módulos para redes Ethernet

Estos módulos se han diseñado para satisfacer las especificaciones del estándar IEEE 10 BASE-T. El TPMIM se ofrece con tres tipos de conectores de medios: El RJ45, el DB9, y el RJ71 y con 12 ó 24 puertos para conexiones hasta 200 metros de longitud de cable de par trenzado, armado o no.

La serie TPMIM incluye detección automática de polaridad del par de entrada. Al detectarse un error, se corrige la polaridad para obtener una recepción adecuada. Además, todos los módulos TPMIM se han diseñado para eliminar colisiones falsas al filtrar el ruido que se introduce en el par de entrada durante la transmisión.

Características:

Módulo TPMIM-T1//22/32/24/34

- * Cumple las especificaciones IEEE 10 Base-T.
- * Disponible con tres tipos de conectores de medios diferentes: RJ45, DB9, y RJ71.
- * Soporta cable de par trenzado blindado y no blindado.
- * Alcances hasta de 200 metros.
- * Función de detección y corrección de polaridad automática.
- * Número de puertos:
 - TPMIM-T1:12 puertos, conector DB9.
 - TPMIM-22:12 puertos, conector RJ45.
 - TPMIM-32:12 puertos, conector Telco de 50 pin.
 - TPMIM-24:24 puertos, conector RJ45.
 - TPMIM-34:24 puertos, conector Telco de 50 pin.

5.4.2.15 Módulo de administración y puenteo Ethernet (EMME)

Descripción

Módulo EMME

- Módulo de administración que soporta la arquitectura multicanal del MMAC-FNB.
- Permite configurar, monitorear y puentear tres segmentos de red separadamente en el mismo concentrador, así como un cuarto segmento externo para esta última función.
- Ofrece monitoreo y control completo en banda para todos los tres canales Ethernet en el concentrador MMAC.
- Ofrece control y administración de redes múltiples Token Ring y FDDI que operan simultáneamente en el concentrador.

Con el fin de permitir el máximo de canales de información entre los puertos del MMAC y al mismo tiempo proporcionar capacidades de puenteo IEEE 802.1d para impedir que un tráfico de red innecesario pase a través de la MMAC, se ha incorporado en el EMME un repetidor IEEE 802.3. El EMME cumple con los requisitos del SNMP y se puede controlar y monitorear por medio de diversos paquetes de administración de redes que cumplen con el SNMP. Además, el módulo se puede controlar y monitorear mediante la administración local EMME a través de un terminal en forma local o remota mediante un modem.

5.4.2.16 Módulo concentrador activo para Token Ring

TRMIM-22A

Los módulos TRMIM-22A son módulos de interface de medios activos para redes Token Ring diseñados para los Centros de acceso a medios múltiples (MMAC) de Cabletron. Los módulos TRMIM-22A proporcionan 12 puertos de empalme central respectivamente, para conexiones de redes Token Ring con cable de par trenzado no armado (UTP), cableado IBM tipo 3 o el nuevo cableado nivel 4 de gran calidad. Estas tarjetas tienen "Protección de fallas de velocidad de anillo" en cada puerto.

Cada puerto concentrador de los módulos TRMIM-22A tienen circuitos activos que filtran, ecualizan y amplifican la señal recibida para transmitirla a la siguiente estación en el anillo. Esta característica le permite extender el largo del lobe entre una estación conectada y el puerto concentrador con una señal mucho más confiable, cada puerto del TRMIM-22A soporta hasta 200 mts. de cable UTP entre el TRMIM y la estación, permitiendo crear redes autónomas de 4 ó 16 Mbps, nuevas redes integradas o expandir las redes Token Ring ya existentes.

5.4.2.17 Módulos de interface para puertos Ethernet

EPIMS

Estas son interfaces intercambiables y flexibles a la necesidad que tenga con el medio a conectar, éste se integra al concentrador o tarjeta y desde ahí se conecta a diferentes medios coaxial, par trenzado y fibra óptica. Su función es la de la flexibilidad de cambio de medio desde el hub.

Las características de los modelos son:

- Para el EPIMs-A: Son para 10 base 5 y cuenta con conectores AUI que son DB15.
- Para el EIPMs-F2: Son para Fibra Optica multimodo con conectores ST.

5.4.2.18 Concentradores 10 Base-T SNMP MRXI/MRXI-2

Los concentradores MRXI y el MRXI-2 cumplen con los estándares 10 BASE-T y IEEE 802.3 y están equipados con un microprocesador incorporado y una interface Ethernet que se puede administrar mediante cualquier plataforma de administración de redes SNMP. Los concentradores vienen con 12 puertos 10 BASE-T y dos ranuras, que el usuario puede configurar, para módulos de interface de puertos simples opcionales (SPIM). Los concentradores también vienen equipados con los exclusivos diodos emisores de luz (LED) LANVIEW, que proporcionan un diagnóstico de nivel físico incorporado para la rápida detección de problemas de la red.

Especificaciones:

Tipo de conector:	MRXI: Telco (50 pines) MRXI-2: 12 RJ45.
Cables que soporta:	AUI, UTP/STP de fibra óptica.
Longitud de cables:	125 m (común) 200 m (máximo).
Tiempo medio entre fallas (MTBF):	83,133 horas.
Peso:	3.2 Kgs. aprox.

5.4.2.19 Concentrador 10 Base-T MRXI-24

El MRXI-24 proporciona 24 puertos en RJ45 10 BASE-T y dos módulos de interface de puerto Ethernet (EPIM) que el usuario pueda configurar. Los EPIMs ofrecen versiones de RJ45, AUI, de transceiver y de fibra y/o coaxial delgado en el diseño del MRXI-24 se incluye el controlador de interface de repetidores (RIC), que es un repetidor 802.3 completamente funcional integrado a un solo chip, que aumenta el MTBF y proporciona una mayor confiabilidad.

El MRXI-24 proporciona grados variables de capacidad de administración, desde los diodos emisores de luz (LED) LANVIEW para monitorear a primera vista el nivel físico, hasta la pantalla LCD para ver el estado del nivel del sistema. Cada uno de los dos puertos seriales del panel delantero se pueden configurar para soportar una de las siguientes tres capacidades: La interface de administración local, un SNMP "Proxy" para las fuentes inteligentes de alimentación in-interrumpible de conversión de alimentación norteamericana, o el protocolo de inter-red de líneas en serie (SLIP). El MRXI-24 puede administrar totalmente el SNMP desde cualquier sistema de administración de redes. Para poder funcionar como analizador de redes, el concentrador incluye soporte de MIB II y RMON, además del monitor de red área local (LAN) distribuida (DLM).

Especificaciones:

Tipos de conector:	24 RJ45.
Cables que soporta:	AUI, UTP/STP fibra óptica coaxial delgado
Longitud de cables:	125 m (común) 200 m (máximo)
Tiempo medio entre fallas (MTBF):	83,133 horas
Peso:	3.2 Kgs. aprox.

5.5 Características Técnicas de los conmutadores ATM de FORE

Conmutador ATM Modelo ForeRunner ASX-200

5.5.1 Hardware del Sistema

Ensamble del conmutador:	2.5 Gbps sin contención, sin bloqueo
Buffers de salida:	512 Kbytes con prioridad dual
Interface ATM:	Capacidad máxima de 24 puertos
Retraso de tránsito del conmutador:	Menor a 10 microsegundos
Tiempo de conexión inicial:	Menor a 10 millonésimas de segundo
Procesador de Control:	Sistema RISC, DRAM de 16 Mbytes
Velocidad máxima en puertos:	155 Mbps (OC-3c/STM-1)
Interface Ethernet:	622 Mbps (OC-12/STM-4) a futuro Compatible con 802.3, conector hembra DB15
Interface Serial:	Conector DB-9
Indicador de panel frontal:	Detección de portadora, Tx, Rx, Indicadores de diagnóstico

Alimentación eléctrica:	120 VAC 60 Hz., 2.3 amps (máximo) 240 VAC 50 Hz., 1.3 amps (máximo)
Dimensiones:	Altura de 15 cm (5.8 pulgadas) Ancho de 48 cm (19.0 pulgadas) Profundidad de 59 cm (23.3 pulgadas) Peso de 18 kg (40 libras), máximo

5.5.2 Software del Sistema

5.5.2.1 Software de Interconectividad

- Canales virtuales/rutas virtuales
- Circuitos virtuales conmutados (SVCs)
- Circuitos virtuales permanentes (PVCs)
- "Multicast" y "Broadcast"
- Protocolos Q.2931 a SPANS SVC
- Niveles múltiples de prioridad para celdas
- Protocolos Q.2931 a SPANS SVC
- NNI para establecer conexiones interconmutadas
- Emulación de LA
- PI sobre ATM

5.5.2.2 Software de administración de red

- Protocolo simple de administración de red (SNMP v1 & v2)
- Operación Point-and-Click
- Reconocimiento y mapeo automático de redes ATM basadas en ForeRunner
- Integración a plataformas de administración de red

5.5.3 Especificaciones generales

Estándares

- ITU Y.361 capa ATM
- Foro ATM UNI v3.0
- RFC 1483 & RFC 1577
- Q.2931

Emisiones

- FCC parte 68, Subparte 15, Clase A
- VCCI Clase A
- CISPR

Ambientales

- Temperatura de operación: 0°C a 40°C. 0-5000 pies
- Humedad: 0-95% sin condensación

Criterios de Selección para el producto

- Compatibilidad con estándares: Interoperatividad con más de 40 vendedores de equipo; Foro ATM UNI v3.0; CCITT Q.2931; RFC 1483 & 1577
- Confiabilidad: Inteligencia distribuida, Módulos Hot-swappable
- Administración de red: Fore View/SNMP utilizando HP Open View, Sunet Manager, Net View/6000
- Tipos de cable: Cobre y fibra óptica
- Soporte para redes convencionales:
 - * Ethernet, Token Ring y FDDI:
 - * Soporte de aplicaciones:
- Facilidad de uso: Conmutador de acceso LAX-20 LA Emulación de LA, PI sobre ATM, circuitos virtuales, conmutados y grupos virtuales.
- Experiencia del proveedor: Fore Thought, Fore View Software Cuatro años de experiencia en la implementación de redes ATM fuera de laboratorio.

5.5.4 Conmutador de Acceso para LAN Modelo ForeRunner LAX-20**5.5.4.1 Hardware del Sistema****Dimensiones:**

Altura de 5.25 pulgadas,
 Ancho de 17.5 pulgadas
 Profundidad de 15 pulgadas
 Peso de 20 libras
 Con fuente de alimentación redundante

Altura de 8.75 pulgadas
 Peso de 35 libras
 Incluye rack de montaje de 19 pulgadas

Alimentación eléctrica:

115/230 VAC 50/60 Hz (con autoselección)
2.5A y 115 VAC, típico
1.25A y 230 VAC, típico
Con fuente redundante
3.0A y 115 VAc, típico
1.5A y 230 VAc, típico

Procesador base:

Procesador i960 dual de alto desempeño con
arquitectura de memoria compartida.
Backplane de 1.6 Gbps
Latencia menor a 50 microsegundos
4 puertos Ethernet AUI
4 puertos seriales para área amplia
(V.35 o EIA-422)
Módem incluido

Módulos de entrada y salida:

Ethernet 4-AUI, 12-10 BASE-T, 4-BNC,
4-FOIRL
FDDI DAS (MIC, SC, ST)
FDDI SAS (4-ST, 4-SC)
Token Ring (4-DB9)
45 Mbps DS-3 ATM (dual BNC)
155 Mbps SONET OC-3c

Opciones:

Fuentes de alimentación redundante

5.5.4.2 Software del Sistema**Software de interconectividad**

- Soporte de LA virtual
- Emulación ATM LA
- IP-sobre-ATM
- Circuitos virtuales conmutados (SVC), administración
- Circuitos virtuales permanentes (PVC), administración

Soporte de puenteo y enrutamiento

- Soporta "Spanning Tree", "Source Routing" y "Source Routing Transparent"
- Soporta ruteo de PI e IPX

Soporte completo de SNMP MIB (Ethernet, Token Ring, FDDI, ATM)**Software de administración de red**

- HP Open View
- SunNet Manager
- Net View/6000

Criterios de Selección para el producto

- Conmutador de LA para uso completo de ancho de banda sobre cableado.

Elimina los "cuellos de botella" en las redes de comunicación.

- Elección en tipo de medio para LA (Ethernet, Token Ring, FDDI, ATM).

Flexibilidad y protección a la inversión.

- Construcción sobre interface ATM.
- Conmutación local.

Integración sobre ATM. Elimina problemas con la columna vertebral de ATM.

- Software ForeThought.

Brinda comunicación inter-redes transparente y protege la inversión de las aplicaciones existentes.

- Grupos de trabajo virtuales.

Grupos amplios de trabajo con seguridad 'builtin'.

- Administración de red basada en SNMP usando HP Open View SunNet Manager o IBM Net View 6000.

Solución basada en estándar.

6.1 Esquema de la red

Los equipos y las conexiones que se muestran en la figura 6.1, corresponden al nodo central donde se localiza la interface entre la red ATM y la red satelital para comunicar los nodos remotos. También se muestra el equipo de acceso (CS/500) a través del cual se pueden comunicar los usuarios a la red con líneas conmutadas de TELMEX.

Esquema de La Red WAN

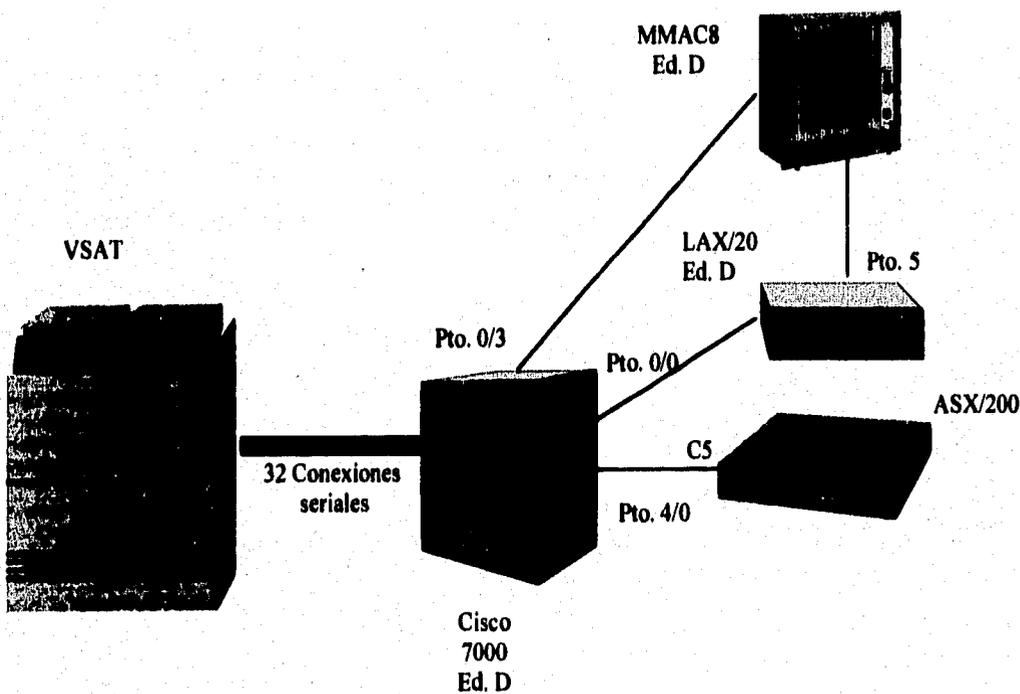


Figura 6.1

Conexion de equipos al Backbone ATM

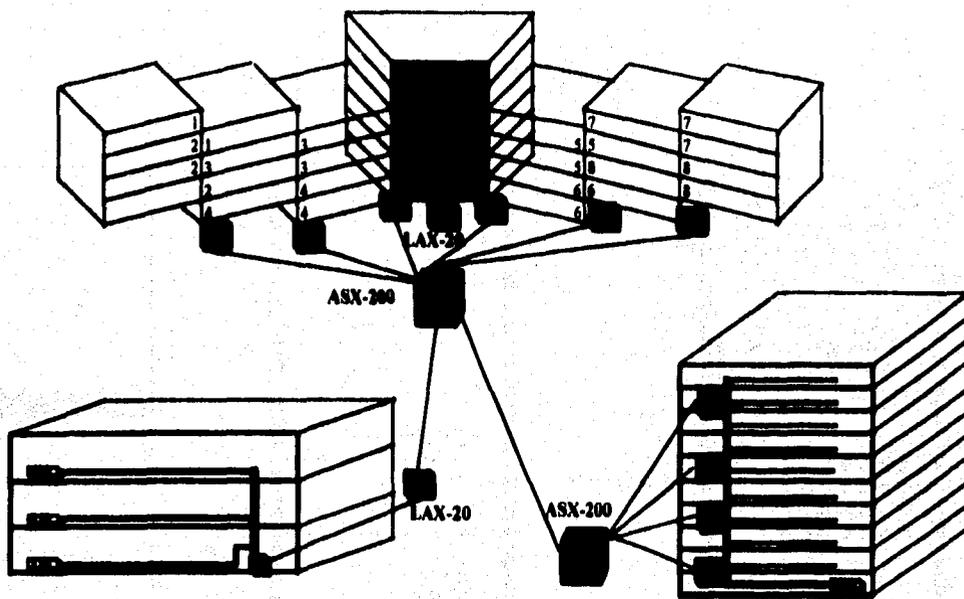


Figura 6.2

6.2 Distribución de los equipos.

De acuerdo a la configuración de los equipos planteada en el capítulo anterior y considerando el espacio con el que se cuenta, se tiene una distribución de equipos como se muestra en las figuras 6.3 y 6.4.

Distribución de equipos

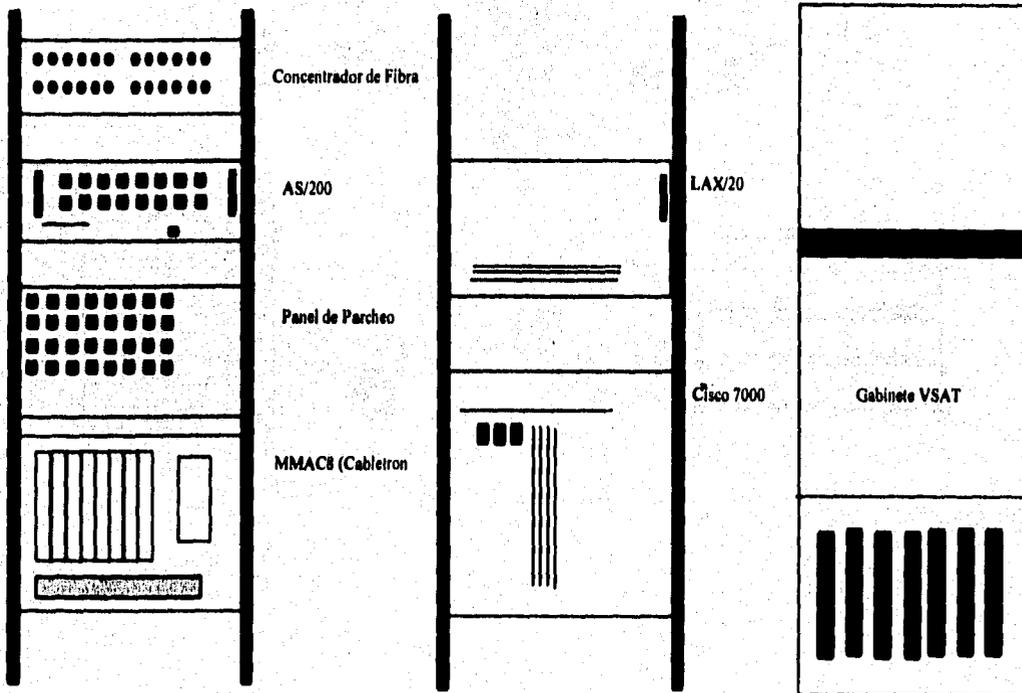


Figura 6.3

Distribución de equipos en los accesos

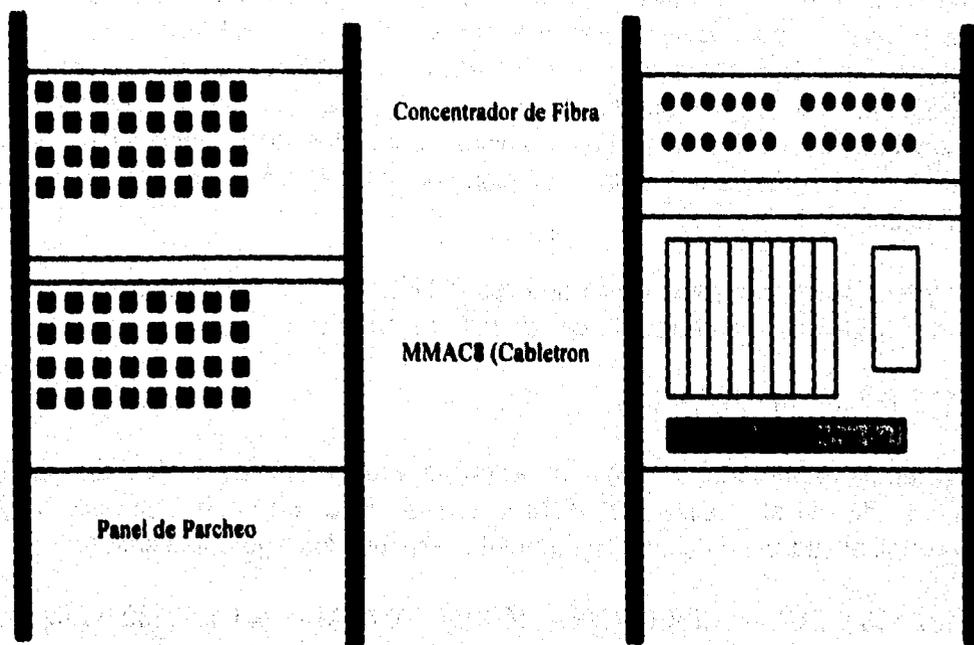


Figura 6.4

6.3 Esquema de direccionamiento lógico

Uno de los primeros aspectos al definir una red es el direccionamiento IP que se va a utilizar. Generalmente se necesita una red de clase que permita tener cuando menos 125 subredes; una clase B brinda 253 subredes las cuales son suficientes para pensar en un crecimiento.

Para definir la máscara a utilizar se consideraron varios aspectos importantes. El punto principal para definir esto fue saber si la red ATM enrutaría o sólo puentearía en los puntos finales, esto lo definió un problema que se enfrentó con un requerimiento de la empresa A, la cual no podía cambiar su esquema de direccionamiento debido a los compromisos derivados de la asociación con la empresa norteamericana. Esta situación derivó el siguiente problema de enrutamiento:

La empresa norteamericana utiliza una red 141.197.0.0 y asigna subredes a las subsidiarias, la empresa A recibió un conjunto de subredes:

141.197.138.0 - 141.197.150.0

El problema se presentó al conectar el enlace proveniente de EUA al enrutador central y de allí al "backbone" ATM y al final a la red de la empresa A. Si analizamos el esquema de direccionamiento tenemos los siguientes saltos:

141.197.138.0 EUA -> CISCO 7000 -> 150.150.0.0 ATM -> 141.197.139.0 Emp. A

Esto viola el concepto de continuidad en redes (el cual es utilizado en RIP) por lo que no se pudo enrutar, en corto plazo, ya que los equipos LAX/20 sólo soportaban RIP en ese entonces, pero soportarían OSPF en un corto plazo. Dada esta situación se definieron las direcciones con una máscara tipo B pero pensando el direccionamiento para sólo cambiar la máscara y enrutar cuando los equipos lo permitieran. El esquema de direccionamiento se muestra en las siguientes tablas:

ASX Edificio D

Piso	Comunicación	Ubicación	Nº de
C1		Edificio D	
C2		Edificio Y	
C3		Edificio Z	
C4		Edificio Z	
D1		Edificio D	
D2		Edificio RS	
D3		Edificio ST	
D4		Edificio UV	
B1		Edificio VW	
B2			
B3			
B4			
A1			
A2			
A3			
A4			

ASX EDIFICIO Z

Piso	Comunicación	Ubicación	Nº de
C1		Piso 9	
C2		Piso 6	
C3		Piso 3	
C4		Piso 1	
D1			
D2			
D3			
D4			
B1			
B2			
B3			
B4			
A1			
A2			
A3			
A4			

LAX Edificio D

Id	Nombre	Comentario	Ubicación	Nota
1			EDIFICIO D	
2			EDIFICIO D	
3			EDIFICIO D	
4			EDIFICIO D	
5			EDIFICIO D	
6			EDIFICIO D	
7			EDIFICIO D	
8			EDIFICIO D	
9			EDIFICIO D	
10			EDIFICIO D	
11			EDIFICIO D	
12			EDIFICIO D	
13			EDIFICIO D	
14			EDIFICIO D	
15			EDIFICIO D	
16			EDIFICIO D	
17			EDIFICIO D	
18			EDIFICIO D	
19			EDIFICIO D	
20			EDIFICIO D	
21			EDIFICIO D	

LAX Edificio Y

Parada	Ubicación	Ubicación	Nº de
1		Edificio Y	
2		Edificio Y	
3		Edificio Y	
4		Edificio Y	
5		Edificio Y	
6		Edificio Y	
7		Edificio Y	
8		Edificio Y	
9		Edificio Y	
10		Edificio Y	
11		Edificio Y	
12		Edificio Y	
13		Edificio Y	
14		Edificio Y	
15		Edificio Y	
16		Edificio Y	
17		Edificio Y	

Direccionamiento IP WAN

CS516

Protocolo	Comando	Redes IP	N.º
0		A7	
1		A8	
2		A9	
3		A10	
4		A11	
5		A12	
6		A13	
7		A14	
8		A15	
9		A16	
10		A17	
11		A18	
12		A19	
13		A20	
14		A21	
15		A22	
16		A23	

Cisco 7000

Port	Connection	Redes IPX	Net
1/0		A24	
1/1		A25	
1/2		A26	
1/3		A27	
1/4		A28	
1/5		A29	
1/6		A30	
1/7		A31	
2/0		A32	
2/1		A33	
2/2		A34	
2/3		A35	
2/4		A36	
2/5		A37	
2/6		A38	
2/7		A39	
3/0		A40	
3/1		A41	
3/2		A42	
3/3		A43	
3/4		A44	
3/5		A45	
3/6		A46	
3/7		A47	
4/0		A48	
4/1		A49	
4/2		A50	
4/3		A51	
4/4		A52	
4/5		A53	
4/6		A54	
4/7			
0/0			
0/1			
0/2		A57	
0/3		2	
0/4			
0/5		A56	

ASIGNACION DE DIRECCIONES IP POR UNIDAD DE NEGOCIO

Unidad de Negocio	Rango Red	Sub Red	Identificador De Red
ICA CP	150.150.106		ICACP
ICA FD	150.150.161		ICAFD
ICA CU	150.150.136		ICACU
ICA ASOCIADOS	150.150.116		
ICA INTERNACIONAL	150.150.96		
ICA CONCESIONES	150.150.76		
SERVICIOS MUNICIPALES	150.150.56		
MAQUINARIA	150.150.46		
BIENES DE CAPITAL	150.150.36		
DIR. ADMINISTRATIVA	150.150.34		
RESERVADA	150.150.32		
ICA SERVICIOS	150.150.30		
RESERVADA	150.150.28		
CONTRALORIA	150.150.26		
RESERVADA	150.150.24		
FINANZAS	150.150.22		
RESERVADA	150.150.20		
RECURSOS HUMANOS	150.150.18		
RESERVADA	150.150.16		
PRESIDENCIA	150.150.14		
RESERVADA	150.150.12		
VICEPRESIDENCIA	150.150.10		
RESERVADA	150.150.8		
JURIDICO	150.150.6		
RESERVADA	150.150.4		
TELECUMUNICACIONES	150.150.2		
RESERVADA	150.150.0		
PARA ASIGNAR A OBRA	150.151.191		

ASIGNACION DE DIRECCIONES IP POR UNIDAD REMOTA

	IP	IP
ICA CP	190.191.168	ICACP
ICA FD	190.191.142	ICAFD
ICA CU	190.191.117	ICACU
ICA ASOCIADOS	190.191.97	
ICA INTERNACIONAL	190.191.77	
ICA CONCESIONES	190.191.57	
SERVICIOS MUNICIPALES	190.191.37	
MAQUINARIA	190.191.17	
BIENES DE CAPITAL		
LIBRES	190.191.0	

Pruebas

Las pruebas realizadas contemplaron únicamente aspectos de conectividad ya que no se contaba con elementos de generación de tráfico para tener elementos cuantitativos. La figura 6.5 muestra los diferentes accesos para las pruebas mostradas en las tablas 6.1, 6.2 y 6.3

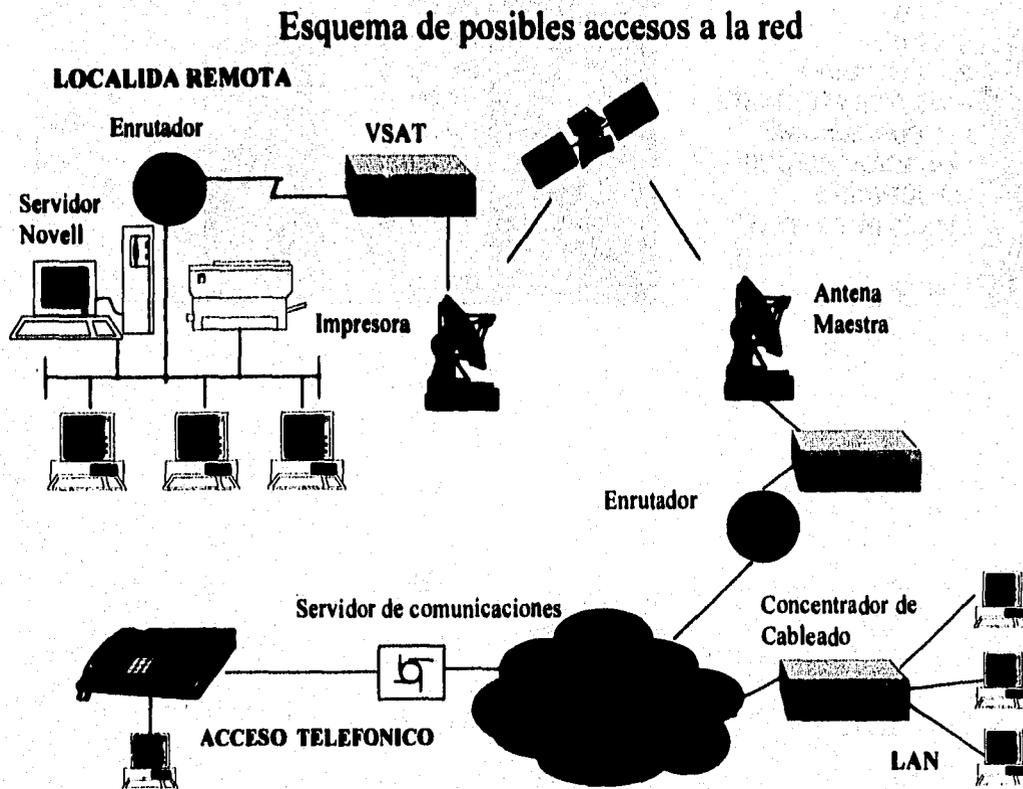


Figura 6.5

Conectividad Servidores UNIX

Accesos

	OK		
	OK	OK	
	OK	OK	OK

Tabla 6.1

Conectividad Servidores NOVELL

Accesos

	OK		
	OK	OK	
	OK	OK	OK

Tabla 6.2

Conectividad Servidores NT (Netbios)

Accesos

	OK		
	OK	OK	
	OK	OK	OK

Tabla 6.3

Conclusiones

Infraestructura de corto, mediano y largo plazo

El diseño e implementación de Red para esta empresa cubre perfectamente sus requerimientos inmediatos, ya que proporciona una red LAN con una estructura que soporta 155 Mbits/seg (ancho de banda necesario como "backbone") que permite, además la interconexión con otras redes de servicios públicos (BANXICO, INDEVAL, etc) y la interconectividad e interoperabilidad con las localidades remotas, satisfacer sus necesidades de comunicación de datos eficientemente. Además soporta la interconexión de conmutadores telefónicos (PBX) utilizando la misma red de datos, Pero además el diseño contempla una visión de mediano y largo plazo ya que como se comento en el trabajo, los requerimientos de la mayoría de las empresas no era de alta velocidad de escritorio, esto es, todavía están evaluando las opciones multimedia o de videoconferencia, pero el diseño de red es tan flexible que permite la migración natural en tres etapas según los requerimientos de las aplicaciones de escritorio lo soliciten :

(1)

En esta etapa tenemos concentradores Ethernet en los nodos finales de red, los cuales convergen a una red ATM, Los principales servidores (Novell y UNIX) así como los servidores de CAD o herramientas que necesitan un gran ancho de banda también están conectados directamente a ATM. Para la interconexión de los nodos remotos se tienen enrutadores.

Las características de trabajo de esta etapa son :

No se tienen aplicaciones que requieran gran ancho de banda en el escritorio y se tienen servidores que, por su volumen de operación necesitan estar conectados directamente al "Backbone". Las transferencias entre las localidades remotas y el campus central no son de gran volumen y no la voz y los datos viajan independientemente por el mismo medio.

(2)

En esta segunda etapa (con el mismo chasis de los concentradores) se cambian, según las necesidades, las tarjetas ethernet por tarjetas de conmutación LAN que permitirán tener conexiones al escritorio de 10 Mbits/s (no colisionados). Casi todos los servidores estarán conectados directamente al "Backbone". Los conmutadores de los principales edificios estarán conectados en ATM y los sitios remotos continuaran con conexión a través de enrutadores pero se realiza un incremento substancial en la capacidad de los enlaces.

Las características de trabajo de esta etapa son :

Los usuarios pueden compartir video, tienen acceso a videoconferencia entre ellos y comparten aplicaciones multimedia, además pueden tener la misma red telefónica en las computadoras de los escritorios. La comunicación con los sitios remotos sigue siendo a través de enrutadores pero el volumen de transferencia es mayor (no se cuenta con videoconferencia en los sitios remotos)

(3)

En esta tercer etapa las computadoras de escritorio están conectadas directamente a los servicios de ATM con conexión UTP nivel 5. La red contempla el aspecto de escalabilidad por lo que "n" conmutadores ATM pueden ser conectados para soportar los requerimientos que provengan de todos los clientes emisores. Las localidades remotas se encuentran conectadas con conmutadores ATM y se cuenta con multimedia y videoconferencia.

Como se puede ver en el trabajo ATM es una realidad HOY , ya que se puede implementar un red que opere y coexista con las arquitecturas de red actual. Los estándares para las interfaces físicas así como para la capa de ATM están terminados por lo que el resto se implementa en software lo que permite instalar una red hoy e instalar nuevas funcionalidades mañana cambiando solamente el software de los equipos.

Un aspecto a considerar es la interoperabilidad ya que, como se muestra en el trabajo, los estándares (de niveles superiores) están abiertos a opciones que pueden conducir incompatibilidades, por lo que es muy conveniente considerar , por lo menos en un corto plazo, instalar equipos del mismo proveedor.

ATM esta lo suficientemente maduro que incluso los grandes "carriers" en EUA empiezan a ofrecer servicios de conexión en ATM, esta madurez (con la capacidad de Gbs) aunada a las nuevas capacidades de procesamiento que las computadoras de escritorio adquieren cada día, impulsaran el desarrollo de nuevas aplicaciones mas orientadas a integrar en un solo componente Voz/Datos/Video.

1BASE Véase StarLAN

10BASE2 Véase Cheapernet

10BASE5 Especificación de capa física (physical layer) de banda base (baseband) IEEE 802.3 similar a Ethernet, que emplea cable coaxial grueso y que funciona a 10 Mbps.

10BROAD36 Especificación de banda amplia (broadband) IEEE 802.3 que emplea cable coaxial grueso y que funciona a 10 Mbps,

10BASET Especificación IEEE 802.3 que emplea cable de par trenzado (twisted pair) simple y que funciona a 10 Mbps.

A & B bit signaling Señalización de bits A & B Procedimiento empleado en la mayoría de los sitios de transmisión TI, en el cual un bit de cada sexto marco o trama (frame) de cada uno de los 24 subcanales se usa para información de señalización de supervisión.

ABM Asynchronous Balanced Mode: Modo balanceado asincrónico. Modo de comunicación HDLC (y su protocolo derivado) que maneja comunicaciones de punto a punto entre nodos equivalentes (peer) para dos estaciones, en donde cualquiera de ellas puede iniciar la transmisión.

abstract syntax Sintaxis abstracta. Descripción de una estructura de datos independiente de la codificación y del tipo de hardware.

access-group Suborden de la interface Cisco que aplica una lista de acceso a una interface.

access-list Lista de acceso. Lista que los enrutadores Cisco emplean para controlar el acceso desde o hacia el enrutador para servicios varios (por ejemplo, para impedir que paquetes con una cierta dirección IP salgan de una interface en particular del servidor de la red).

access method Método de acceso. Software de un procesador SNA que controla el flujo de información a través de la red. En general, se refiere a la forma en que los dispositivos de la red tienen acceso a ella.

accounting management Administración de cuentas. Una de las cinco categorías de administración de redes definidas por ISO para el manejo de redes OSI. Los subsistemas de administración de cuentas son

responsables de recolectar los datos de la red que se refieren al uso de los recursos.

ACF Advanced Communications Function: Función de comunicación avanzada. Conjunto de productos SNA que ofrecen procesamiento distribuido y comparación de recursos.

ACFINCP Advanced Communications Functions/Network Control Program: Función de comunicación avanzada/Programa de control de redes. Programa principal de control de redes SNA. Reside en el controlador de comunicaciones y sirve como interface con los métodos de acceso SNA en el procesador principal para controlar las comunicaciones de la red.

ACK Abreviatura de acknowledgment (acuse de recibo). Normalmente se envían ACKs de un dispositivo a otro de la red para indicar que ocurrió algún suceso (por ejemplo, la recepción de un mensaje).

ACSE Association Control Service Element. Elemento de servicio de control de asociación. Convención OSI empleada para establecer, mantener o terminar una conexión entre dos aplicaciones.

active hub (Véase hub: concentrador). Dispositivo de varios puertos amplifica señales de transmisión de una red local, LAN.

adapter Adaptador. Tarjeta de una PC, normalmente instalada dentro de la máquina, que ofrece capacidades de comunicación de red desde y hacia la computadora. Suele usarse también en lugar del término NIC.

adaptive routing Enrutamiento adaptable. Véase enrutamiento dinámico.

ADCCP Advanced Data Communications Control Protocol: Protocolo de control avanzado para comunicación de datos. Protocolo ANSI estándar para control de enlaces de datos que funciona en el nivel de bits.

address Dirección. Estructura de datos empleada para identificar una entidad única, como algún proceso o la localización de una red.

address mask Carátula o máscara de la dirección. Combinación de bits empleada para designar los bits de dirección de la subred dentro de la dirección del protocolo de una red.

adjacency Adyacencia. Relación formada entre enrutadores cercanos seleccionados y nodos terminales con el propósito de intercambiar información de enrutamiento. La adyacencia se basa en el uso de un segmento físico común.

adjacent nodes Nodos adyacentes. En SNA, nodos conectados a algún otro en forma directa, sin nodos intermedios. En DECnet y OSI, los nodos adyacentes son aquellos que comparten un segmento común (Ethernet, FDDI, Token Ring).

administrative distance Distancia administrativa. Medida de la confiabilidad de una fuente de información sobre rutas. En los enrutadores Cisco, la distancia administrativa se expresa como un valor numérico entre 0 y 255 (mientras más alto sea el valor, menor es la confiabilidad).

ADPCM Adaptive Differential Pulse Code Modulation: Modulación diferencial adaptable codificada por pulsos. Procedimiento mediante el cual se emplea la alta correlación estadística entre muestras consecutivas de voz para crear una escala de cuantización variable (o adaptable). Con ADPCM se pueden codificar muestras analógicas de voz en forma de señales digitales de buena calidad.

advertising Anuncios- Método con el que los enrutadores mantienen listas de rutas utilizables, enviando actualizaciones de enrutamiento o de servicio en períodos especificados de tiempo.

adyacencia Véase adjacency.

agent Agente. Software que procesa pedidos y devuelve respuestas en alguna aplicación. En los sistemas de administración de redes los agentes residen en todos los dispositivos bajo control y reportan los valores de las variables especificadas a las estaciones de administración. En las arquitecturas Cisco un agente es una tarjeta individual de procesador que ofrece una o varias interfaces físicas.

AGS Advanced Gateway Server: Servidor de intercomunicación avanzado. Nombre del enrutador/puente Cisco de 9 ranuras (slots).

AGS + Advanced Gateway Server Plus: enrutador/puente Cisco de 9 ranuras con un módulo cBus de conmutación. Cinco de las ranuras se

conectan al cBus.

AIS Alarm Indication Signal: Señal de alarma. En T1 es una señal de bits en uno que se transmite en lugar de la señal normal para mantener continuidad en la transmisión e indicar a la terminal de recepción que hubo una falla de transmisión localizada en, o antes de, la terminal de transmisión.

alarm Alarma Mensaje que avisa al operador o administrador sobre problemas en la red.

A-Law Ley-A. Estándar de compresión y expansión (companding) empleado por CCITT para la conversión entre señales analógicas y digitales en sistemas PCM. Se usa más bien en las redes telefónicas europeas y es similar al estándar norteamericano mu-law (ley-mu).

alert Alerta. En NetView, es un registro que indica al operador de la red la existencia de un problema que debe ser atendido en el punto de control.

algorithm Algoritmo. Reglas o procesos bien definidos para alcanzar la solución de un problema.

algoritmo Véase algorithm.

alignment error Error de alineación. En las redes IEEE 802.3, es un error que ocurre cuando el número total de bits de un marco o trama (frame) no es múltiplo de ocho. Los errores de alineación normalmente son causados por daños a la trama debidos a colisiones.

ALOHA Técnica de control de accesos para sistemas de transmisión que permite a múltiples estaciones transmitir simultáneamente. En el sistema ALOHA las estaciones transmiten cuando tienen datos que mandar, y las transmisiones que no tuvieron acuse de recibo se repiten.

AM Amplitud modulada. Técnica de modulación en la que la información se conduce mediante la amplitud de la señal portadora.

amplitude Amplitud. El máximo valor de una forma de onda analógica o digital.

analog transmission Transmisión analógica. Transmisión de señales, mediante cables o por el aire, en la cual se conduce la información mediante la variación de alguna combinación de la amplitud de la señal,

su frecuencia y su fase.

ancho de banda Véase bandwidth.

anfitrión Véase host.

ANSI American National Standards Institute: Instituto nacional norteamericano de estándares. Instancia coordinadora de grupos voluntarios de fijación de estándares en los Estados Unidos. ANSI es miembro de ISO (International Organization for Standardization: Organización internacional para la estandarización).

anuncios Véase advertisement.

API Application Programming Interface: Interface para programas de aplicación. Especificación de convenciones de llamadas a funciones para definir la interface con un servicio.

Apollo Domain Conjunto patentado de protocolos de red desarrollados por la compañía Apollo Computer para comunicaciones en redes Apollo.

AppleTalk Serie de protocolos de comunicaciones relacionados, creados y mantenidos por la compañía Apple Computer. Actualmente existen dos fases: 1 y 11. La fase 11, que incluye manejo de interconexión entre redes, es la versión más reciente.

application layer Capa de aplicación. Capa 7 del modelo de referencia OSI. Está implantado en varias aplicaciones de red, como correo electrónico, transferencia de archivos y emulación de terminales.

aplique Aplicación. Placa de montaje que contiene conectores de hardware para fijarse a la red. Las placas traducen y convierten las señales de comunicaciones tipo serie en las que espera el estándar de comunicación escogido (por ejemplo, RS-232. Y35).

APPC Advanced Peer-to-Peer Communications: Comunicación avanzada entre nodos similares o equivalentes. Esquema SNA de comunicaciones de IBM que permite comunicar directamente aplicaciones equivalentes SNA.

APPN Advanced Peer-to-Peer Networking: Redes avanzadas entre nodos equivalentes. Esquema SNA de IBM que ofrece procesamiento distribuido basado en nodos de red de Tipo 2.1 y LU 6.2.

árbol abarcador Véase spanning tree.

area Area. Conjunto lógico de segmentos conectados por enrutadores y que están basados en los estándares ISO CLNS, DECnet u OSPE

ARCNET *Attached Resource Computer Network*: Red de computadoras con recursos asignados. Red local (LAN) de tipo token bus a 2.5 Mbps desarrollada a finales de los años 70 e inicios de los 80 por la empresa Datapoint Corporation. Sus principales características son su sencillez, facilidad de uso y relativa economía.

ARM *Asynchronous Response Mode*: Modo de respuesta asíncrono. Modo de comunicación HDI-C con un primario y al menos un secundario, donde el primario o cualquiera de los secundarios puede iniciar las transmisiones. **ARPA** *Address Resolution Protocol*: Protocolo de resolución de direcciones. Protocolo Internet usado para ligar una dirección IP a direcciones Ethernet/802.2. Está definido en el documento RFC 826.

ARPA Véase DARPA.

ARPANET Red pionera de conmutación de paquetes (*packet switching*) desarrollada al inicio de los años 70 por la empresa BBN y financiada por la agencia ARPA (luego DARPA). ARPANET se convirtió luego en "Internet". El término ARPANET desapareció oficialmente en 1990.

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

AS *Autonomous System*: Sistema autónomo. Conjunto de redes bajo administración común y que comparten una estrategia común de enrutamiento. A un sistema autónomo debe dársele un número único de 16 bits asignado por el Centro de Información sobre Redes (NIC) de la agencia DDN.

ASCII American Standard Code for Information Interchange: Código estándar nortamericano para intercambio de información. Código de ocho bits para representar caracteres que emplea siete bits más paridad.

ASM Servidor de terminales CISCO en chasis A.

ASN.1 Abstract Syntax Notation One: Notación de sintaxis abstracta número uno. Lenguaje OSI para describir tipos de datos en forma independiente de estructuras computacionales y técnicas de representación. Organización Internacional de Estandarización, Estándar Internacional 8824, diciembre, 1987. Véase también BER.

asynchronous transmission Transmisión asincrónica. Operación de un sistema de red en el cual los acontecimientos suceden sin estar sincronizados por un reloj. En tales sistemas, los caracteres individuales suelen estar encapsulados en bits de control llamados de arranque y de parada, que designan el inicio y el final de los caracteres.

ATDM Asynchronous time Division Multiplexing: Multiplexaje asincrónico por división de tiempo. Método de envío de información que emplea el multiplexaje usual por división de tiempo, pero en donde se asignan ranuras de tiempo cuando se requieren, en lugar de preasignarlas a transmisores específicos.

ATG Address Translation Gateway: Intercomunicador traductor de direcciones. Función de software para enrutamiento DECnet que Cisco emplea para lograr que el enrutador maneje varias redes DECnet independientes, y para establecer traducción de direcciones- especificada por el usuario para nodos seleccionados entre redes.

ATM Asynchronous Transfer Mode: Modo de transferencia asincrónico. Estándar CCITT para retransmisión de celdas (cell relay) en el cual la información para diferentes tipos de servicios (voz, video, datos) se transmite en pequeñas celdas de tamaño fijo. También, modo de transmisión BISDN en el cual se usa una versión acelerada del multiplexaje asincrónico por división de tiempo (ATDM) para transferir flujos Múltiples de información en un canal de comunicación.

attenuation Atenuación. Pérdida de energía en la señal de comunicación.

AUI Attachment Unit Interface: Interface de unidad de vinculación.

Cable IEEE 802.3 que conecta la unidad de acceso al medio (MAU: Media Access Unit) al dispositivo en red. El término AUI también se puede usar para referirse al conector del panel trasero principal al que se puede fijar el cable AUI.

authority zone Zona de autoridad. Relativa a DNS, sección del nombre del árbol del dominio en el cual el nombre de un servidor es autoridad.

automatic call reconnect Reconexión automática de llamada. Capacidad de permitir reenrutamiento automático de llamadas en una línea troncal diferente de la que falló.

autonomous confederation Confederación autónoma. Grupo de sistemas autónomos que confían más en su información de red y de enrutamiento que en la que reciben de otros sistemas o confederaciones autónomas.
autonomous switching Conmutación autónoma. Característica de los enrutadores Cisco que ofrece un procesamiento más rápido de paquetes al permitir que el cBus conmute paquetes en forma independiente, sin interrumpir al procesador del sistema.

backbone network Red fundamental. Actúa como conducto primario (o "espina dorsal") de tráfico que usualmente viene de, o va hacia, otras redes.

back channel Canal secundario. Empleado para enviar datos en dirección opuesta a la del canal primario. Los canales secundarios suelen usarse para enviar información de control. Mediante ellos, la información puede enviarse aunque el canal primario falle. También llamado canal en reversa.

back door Ruta secundaria alterna hacia una red no local (especificada por un IPG) que debe ser usada por un enrutador de frontera. Los enrutadores Cisco permiten la especificación de rutas secundarias alternas mediante una variación de la suborden network.

back end Nodo o programa que ofrece servicios a un front end. Véase también cliente y servidor.

backoff El retraso (usualmente aleatorio) en la retransmisión causado por los protocolos de competencia por el control de acceso al medio de transmisión, luego de que un nodo que intentaba transmitir detectó una portadora en el canal físico.

back pressure Propagación en sentido inverso de la información del

congestionamiento de la red en una interconexión.

backward channel Véase back channel.

backward learning Aprendizaje en reversa. Proceso mediante el cual se conjetura la inexistencia de información al suponer condiciones de una red simétrica. Por ejemplo, si se supone que el nodo A recibe un paquete del nodo B mediante el intermediario C, entonces el algoritmo de enrutamiento de aprendizaje en reversa supondrá que A puede, en forma óptima, llegar a B a través del nodo C.

balanced configuration Configuración balanceada. En HDLC, una configuración de red punto a punto con dos estaciones combinadas.

balun **Balanced**, unbalanced: balanceado, desbalanceado. Dispositivo empleado para igualar impedancias entre una línea balanceada y una desbalanceada; normalmente entre par trenzado y cable coaxial.

banda base Véase baseband.

bandwidth Ancho de banda. Diferencia entre la frecuencia más alta y la más baja de las señales de una red. También describe la capacidad establecida de un protocolo o un medio dados para una red.

bandwidth reservation Reservación de ancho de banda. En líneas conmutadas, característica que permite reservar el ancho de banda de la llamada para llamadas de alta prioridad o de alto ancho de banda.

BARRnet Bay Area Regional Research Network: Red para investigación en la región de la bahía de San Francisco. La red fundamental (backbone) BARRnet está compuesta por cuatro campus de la Universidad de California (Davis, Berkeley, Santa Cruz Y San Francisco), por la Universidad de Stanford, el Laboratorio Nacional Lawrence Livermore y por el Centro de Investigaciones Ames de la NASA.

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

basic rate interface Interface de tasa básica. Interface ISDN (Integrated

Services Digital Network: Red digital de servicios integrados) compuesta de 2B + ID canales

baud Unidad de velocidad de señalización igual al número de condiciones discretas o sucesos en la señal por segundo. Los bauds son equivalentes a los bits por segundo cuando cada suceso en la señal representa exactamente un bit.

BBN Bolt Beranek v Newman, Inc. Compañía de Massachusetts, responsable del desarrollo y mantenimiento de los sistemas primarios de enlace de ARPANET (y luego, de Internet).

B Channel Canal B. En ISDN, un canal full duplex de 64 Kbps, empleado para enviar datos de usuarios.

beacon Boya, faro. Marco (frame) de Token Ring de IBM que indica algún problema serio en el anillo (ring), tal como un cable cortado.

Bellcore 1920 Organización que efectúa labores de investigación y desarrollo para las compañías regionales de la empresa Bell.

Bellman-Ford routing algorithm Algoritmo de enrutamiento Bellman-Ford. También conocido como algoritmo de vector de distancias. Clase de algoritmos de enrutamiento que itera sobre el número de saltos (hops) en una ruta para encontrar el árbol abarcador (spanning tree) más corto. El algoritmo pide que cada enrutador envíe únicamente a sus vecinos su tabla de rutas completa cada vez que se actualiza. Estos algoritmos pueden caer en ciclos, pero computacionalmente son más sencillos que los de tipo estado de enlace, link-state.

BER Base Encoding Rules: Reglas básicas de codificación. Reglas para codificar las unidades de datos descritas en ASN. 1. Las siglas también significan bit error rate: tasa de error de bits, que se refiere al número de bits erróneos recibidos.

BERT Bit Error Rate Tester Device: Dispositivo para prueba de tasa de errores de bits- Determina la tasa de error de bits en un canal de comunicaciones.

Best effort delivery Entrega lo mejor posible. Característica de los sistemas de redes que no emplean un sistema elaborado de verificación que garantice el manejo confiable de información.

BGP Border Gateway Protocol: Protocolo de intercomunicación de frontera. Protocolo de enrutamiento de interdominios que es un

reemplazo potencial de EGP (Exterior Gateway Protocol). BGP está definido por el documento RFC 1105, hecho por un empleado de CISCO y uno de IBM.

big-endian Método de almacenar o transmitir información en el cual el bit o byte más significativo se presenta primero. Véase también little-endian.

binary Binarario. Sistema de numeración caracterizado por unos y ceros (on y off, sí y no).

binary synchronous communication Comunicación binaria sincrónica. Protocolo de enlace de datos por caracteres que se emplea en aplicaciones half-duplex. Se conoce simplemente como bisync.

biphase coding Codificación bifase. Esquema de codificación bipolar originalmente desarrollado para su uso en Ethernet. La información del reloj se incluye, y se obtiene, del flujo de datos sincrónico sin necesidad de señales extras de reloj. La señal bifase no contiene energía de corriente directa.

bipolar Bipolar. Que tiene polaridades negativa y positiva.

BISDN Broadband ISDN.- de banda amplia. Estándares de comunicaciones que se desarrollan para manejar aplicaciones de gran ancho de banda, tales como video.

bisync Véase binary synchronous communication.

bit binary digit: dígito binario. Unidades empleadas en el sistema de numeración binario. Pueden ser 0 ó 1.

bit error rate Tasa de error de bits. Porcentaje de bits transmitidos que se reciben con error

BITNET Because It's Time Network: Red de "ya es tiempo". Red académica de baja velocidad y bajo costo que consiste primordialmente en computadoras grandes IBM y líneas dedicadas de 9600 bps. El modo principal de trabajo en esta red es RJE (Remote Job Entry: Entrada remota de trabajos). Recientemente la red se fusionó con CSNET (Computer + Science Network) para formar CREN (Corporation for Research and Educational Networking).

bit-oriented protocol Protocolo por bits. Clase de protocolos de

comunicaciones de la capa de enlace (link layer) que pueden transmitir marcos (frames) sin preocupación de sus contenidos. Comparados con los protocolos por bytes, éstos son más eficientes y contables, y ofrecen operación full duplex.

bit rate Tasa de bits. Velocidad a la que se transmiten los bits, normalmente expresada en bits por segundo (bps).

black hole Agujero negro. Término de enrutamiento aplicado a alguna área de los sistemas de redes a donde entran paquetes pero ya no salen, debido a condiciones adversas o a una mala configuración del sistema en alguna parte de la red. **blocking** Bloqueo. En un sistema de conmutación, condición en donde ya no hay trayectorias para completar un circuito. Generalmente, el término se emplea para describir una situación en la cual una actividad no puede iniciar sino hasta que otra ha terminado.

Block Multiplexer Channel Canal de multiplexaje de bloque. Canal tipo IBM que realiza el estándar norteamericano FIPS-60. También se conoce como el canal OEMI y el multiplexor de bloque 370 o canal mux de bloque.

BNC connector Conector BNC. Conector estándar empleado para ligar el cable coaxial IEEE802.3 IOBASE2 a un receptor o transmisor.

BOC Bell Operating Company, Las compañías telefónicas locales que existían en las siete regiones de los Estados Unidos antes de que se diera la orden legal de que la compañía AT&T se desmembrara.

BootP Protocolo empleado por un nodo de la red para determinar la dirección IP de sus interfaces Ethernet, para poder arrancar con la operación inicial (boot) de la red.

Boot PROM Boot Programmable Read-Only Memory: Circuito de memoria de sólo lectura para iniciar operaciones. Circuito de una tarjeta que contiene las instrucciones ejecutables de arranque (boot) para un dispositivo computacional.

border gateway Intercomunicación de frontera. Enrutador que se comunica con otros en sistemas autónomos (AS).

boundary function Función de límites. Capacidad que tienen los nodos de subárea SNA para manejar protocolos para nodos periféricos asignados. Suele encontrarse en los dispositivos IBM 3745.

BPDU Bridge Protocol Data Units: Unidades de datos para protocolos de puente. Paquete de protocolo hello de árbol abarcador (spanning tree). Véase también PDU.

BRI Véase Interface de tasa básica (Basic Rate Interface).

bridge Puente. Dispositivo que conecta dos segmentos de una red y pasa paquetes entre ellos. Los puentes operan en el nivel 2 del modelo de referencia ISO (capa de enlace de datos: link layer) y no son sensibles a los protocolos de niveles superiores.

bridge-group Suborden de puenteo de Cisco que asigna interfaces de la red a grupos particulares del árbol abarcador. Pueden ser compatibles con los estándares IEEE 802.1 o de DEC.

broadband Banda amplia. En contraposición con la banda base (baseband), es un sistema de transmisión que multiplexa varias señales independientes en un solo cable. En la terminología de las telecomunicaciones, se refiere a cualquier canal que tenga un ancho de banda mayor que el requerido para transmitir voz (4 KHz). En la terminología de las redes locales, se refiere a un cable coaxial que maneja señales de tipo analógico.

broadcast Difusión o mensaje público. Mensaje enviado a todos los destinos dentro de una red.

broadcast address Dirección para difusión. Dirección reservada para realizar envíos simultáneos a todas las estaciones de una red.

broadcast storm Disturbios por difusión. Acontecimiento indeseable en una red, en el cual se envían muchas difusiones a la vez, empleando para ello considerable ancho de banda y, normalmente, causando además interrupciones en la red.

BSC Véase comunicación binaria sincrónica (Binary Synchronous Communication).

buffer Amortiguamiento. Zona temporal de almacenamiento empleada para el manejo de datos transitorios. Los buffers suelen emplearse para

compensar las diferencias de velocidad de procesamiento entre dispositivos de la red. Las emisiones rápidas de datos se almacenan en un buffer hasta que los pueda procesar el dispositivo que funciona más lentamente.

bus topology Topología de bus. Arquitectura LAN lineal en la cual las transmisiones de las estaciones de la red se propagan a lo largo de todo el medio de comunicación y son recibidas por todas las demás estaciones.

bypass mode Modo de operación en redes FDDL y Token Ring en el cual se ha des-insertado (o desviado) una interface del anillo.

byte Término genérico que se refiere a una serie de dígitos binarios consecutivos con los que se trabaja como si fueran una unidad; un ejemplo son los bytes de 8 bits.

byte-oriented protocol Protocolo por bytes. Clase de protocolos de comunicaciones de la capa de enlace que emplean un carácter existente específico para delimitar marcos (frames). Este tipo de protocolos prácticamente ha sido reemplazado por los de manejo de bits.

cable Cable. Medio de transmisión que consiste en alambres o fibras ópticas envueltas por una cubierta protectora.

call priority Prioridad de llamada. Prioridad asignada a cada puerto de origen en los sistemas de circuitos conmutados. La prioridad define el orden en el cual se reconectan las llamadas. También define cuáles llamadas se efectuarán durante una reservación de ancho de banda.

call setup time Tiempo de establecimiento de llamada. Tiempo requerido para establecer una llamada conmutada entre dispositivos DTE.

canal Véase channel.

capa de aplicación Véase application layer.

capa de enlace Véase link layer.

capa de red Véase network layer.

capa de transporte Véase transport layer.

capa física Véase physical layer.

carrier Portadora. Señal propia para ser modulada por otra señal que contiene información a ser transmitida.

catenet Red en la cual las computadoras que actúan como anfitriones están conectadas a diversas redes, que a su vez están conectadas con enrutadores. Internet es un importante ejemplo de una red tipo catenet.

CATV Cable Television: Televisión por cable. Anteriormente llamada Community Antenna Television (televisión por antena comunal). Sistema de comunicaciones en el cual se transmiten varios canales con programación a las casas, empleando cable coaxial de banda amplia.

cBus Tecnología de canal (bus) de medio Gigabit por segundo, patentada, desarrollada y distribuida por Cisco Systems, Inc.

cBus controller Véase switch processor.

CCITT Comité Consultivo Internacional de Telegrafía y Telefonía (siglas en francés). Organización internacional que desarrolla estándares de comunicaciones, como la recomendación X.25.

CCS Common Channel Signaling: Señalización de canal común. Sistema de señalización usado por muchas redes telefónicas, que separa la información de señalización de los datos de usuario.

cell relay Transmisión por celdas. Tecnología de redes basada en el uso de pequeños paquetes de tamaño fijo, llamados celdas. Las celdas contienen un identificador que especifica el flujo de datos al que pertenecen. Como son de tamaño fijo, el hardware puede procesarlas y conmutarlas a muy altas velocidades. Este método es la base de muchos protocolos de red de alta velocidad, incluyendo IEEE 802.6, DQDB,

ATM y el protocolo de interface SMDS.

cellular radio Radio celular. Tecnología que emplea transmisiones de radio para lograr acceso a la red telefónica. El servicio se ofrece en una célula (área) particular mediante un transmisor de baja potencia.

centrex PBX mejorado que también ofrece marcaje directo e identificación automática del PBX que llamó. La palabra se refiere a un producto específico de la empresa AT&T.

CEPT Conference Europeene des Postes et teleconimunications: Asociación de 26 oficinas de correos y telecomunicaciones europeas que hace recomendaciones a la CCITT sobre especificación de comunicaciones.

CERFnet California Education and Research Foundation Network: Red de la fundación para la educación y la investigación del estado de California. Red basada en TCP/IP que opera en el sur de California e interconecta muchos centros de educación superior, diseñada para el avance de la ciencia y la educación mediante las comunicaciones.

CGS Compact Gateway Server: Servidor de intercomunicación compacto. Nombre del enrutador/puente Cisco de 2 ranuras (slots).

chaining Encadenamiento. Concepto de SNA en donde las unidades de pedido/respuesta (RU) se agrupan para propósitos de recuperación de errores.

channel Canal. Línea de comunicaciones. En algunos entornos se pueden multiplexar varios canales en un solo cable. El término también se refiere al conducto específico entre computadoras grandes y sus periféricos.

CHAOSnet Protocolo de redes desarrollado en el MIT (Massachusetts Institute of Technology) y empleado fundamentalmente por la comunidad académica de la inteligencia artificial.

cheapernet Término empleado en la industria para referirse al estándar IEEE 802.3 IOBASE2 o al cable especificado en ese estándar. Thinnet, que también se refiere a ese estándar, especifica una versión más delgada y barata de cable Ethernet.

checksum Suma de control. Método para verificar la integridad de los datos transmitidos. Es un número entero calculado a partir de una secuencia de octetos por medio de una serie de operaciones aritméticas. El valor se recalcula en el lado del receptor y se compara para verificarlo.

choke packet Paquete de sofocamiento. Paquete que se envía a un transmisor para indicar que existe congestión y que se debe reducir el volumen de envíos.

CICS Customer Information Control System: Sistema de control sobre información de clientes. Subsistema de aplicación IBM que permite que las transacciones que llegan de terminales remotas sean procesadas concurrentemente por las aplicaciones de los usuarios.

circuit Circuito. Enlace de comunicaciones entre dos o más puntos.

circuit switching Circuitos conmutados. Sistema de conmutación en el que debe existir un circuito físico dedicado entre el emisor y el receptor durante la llamada. De amplio uso en la red telefónica. Los circuitos conmutados se contrastan con los métodos de competencia (Contention) y token passing para acceso al canal, y con la conmutación de paquetes (packet switching) como técnica de conmutación.

class of service Clase de servicio. En forma general, se refiere a cómo manejar un paquete. El tipo de servicio (TOS) IP es una clase de servicio. En SNA, la clase de servicio es la designación de las características de control de trayectoria de la red, incluyendo la seguridad de la trayectoria, el ancho de banda y las prioridades de transmisión que se aplican a alguna sesión en particular. En telefonía existen varias clases de servicio para los abonados dependiendo del servicio requerido.

client Cliente. Nodo o programa de software que requiere servicios de un servidor. Véase también back end.

cliente Véase client.

client-server computing Computación en modo cliente-servidor. Término empleado para describir sistemas de redes de procesamiento distribuido en donde las responsabilidades de las transacciones se dividen en dos partes: el cliente (front End) y el servidor (back end). Ambos términos se pueden aplicar tanto a programas como a dispositivos de cómputo. Véase también peer- to-peer computing

(computación entre nodos equivalentes)

CLNP/CLNS Connectionless Network Protocol/ Connectionless Network Service
Protocolo de redes sin Conexiones/ Servicio de red sin conexiones. De la capa de red OSI

CO Central Office: Oficina central. Oficina de la compañía telefónica local a la cual se conectan todos los loops (ciclos) de una cierta área y en la cual ocurre la conmutación de los circuitos de las líneas abonadas.

coaxial cable Cable coaxial. Cable consistente en un conductor cilíndrico externo hueco que cubre a un alambre conductor único. Suelen emplearse dos tipos de cable coaxial para las redes locales: cable de 50 Ohms, para señales digitales, y cable de 75 Ohms, para señales analógicas y para señales digitales de alta velocidad.

CODEC Coder-Decoder.- Codificador-decodificador. Dispositivo que normalmente emplea modulación codificada por pulsos para transformar voz analógica en un tren de bits y viceversa.

coding Codificación. Técnicas eléctricas usadas para conducir señales binarias.

common carrier Portador común. Compañía particular que tiene licencia para ofrecer servicios de comunicaciones al público a precios regulados.

common channel signaling Señalización de canal común. Uso exclusivo de algún canal específico para llevar información de señalización a los demás canales del grupo.

communication Comunicación. Transmisión de información.

communication controller Controlador de comunicaciones. En SNA, nodo de subárea que contiene un programa NCP, Normalmente es un dispositivo IBM 3745.

community Comunidad. En SNMP, grupo lógico de dispositivos manejados y de estaciones NMS en el mismo dominio administrativo.

companding Contracción formada con los procesos opuestos *compression* (compresión) y *expansion* (expansión). Parte del proceso PCM en el que los valores de muestras de señales analógicas se redondean en términos lógicos a valores discretos de escala de intervalos

dentro de una escala no lineal. El número de intervalo decimal se codifica entonces en su equivalente binario antes de la transmisión. El proceso se invierte en la terminal receptora empleando la misma escala no lineal.

compression Compresión. Paso de los datos por un algoritmo que reduce el espacio/ancho de banda requerido para almacenar/transmitir el conjunto de datos. Véase también *expansion*.

compuerta Véase *gateway*.

concentrador Véase *concentrator*.

concentrator Concentrador. Dispositivo que sirve como centro de una red con topología tipo estrella. También se refiere a un dispositivo que contiene múltiples módulos de equipos de redes.

configuration management Manejo de configuración. Una de cinco categorías de manejo de redes definidos por ISO para el manejo de redes OSI. Los subsistemas de manejo de configuración son los responsables de detectar y determinar el estado de la red.

congestion Congestionamiento. Tráfico excesivo en la red.

connectionless Sin conexiones. Término empleado para describir transferencias de datos sin la existencia de un circuito virtual.

conmutación de paquetes Véase *packet switching*.

connection-oriented Por conexión. Término empleado para describir transferencias de datos posteriores al establecimiento de un circuito virtual.

CONP/CONS Connection-Oriented Network Protocol/ Connection-Oriented Network Service. Protocolo servicio OSI que ofrece operaciones por conexión a protocolos de las capas superiores.

console Consola. DTE a través del cual se ingresan órdenes a una máquina.

contention Competencia. Método de acceso en el cual los dispositivos de la red compiten por los derechos de acceso al medio físico. Véase también *token passing*.

convergence Convergencia. Capacidad (y velocidad con la cual se logra) de un grupo de dispositivos de interconexión de redes que ejecutan un protocolo específico de enrutamiento, para coincidir en la determinación de la topología de las interconexiones luego de que ésta cambió.

conversation Conversación En SNA, una sesión LU 6.2 entre dos programas de transacciones.

core gateway Servidor de intercomunicación básico. Enrutadores primarios en Internet. El centro de operaciones de red Internet de la compañía BBN les da servicio.

COS Corporation for Open Systems: Corporación para sistemas abiertos. Organización que promueve el uso de protocolos OSI mediante pruebas de aceptación, certificación y otras actividades relacionadas.

COSINE Corporation for Open Systems Interconnection Networking in Europe: Corporación para interconexión de redes de sistemas abiertos en Europa. Proyecto europeo, financiado por la Comunidad Económica Europea, EC, para construir una red de comunicaciones entre entidades científicas e industriales en Europa.

count to infinity Cuenta hasta el infinito. Problema que puede ocurrir en algoritmos de enrutamiento de convergencia lenta, donde los enrutadores incrementan secuencialmente la cuenta de trayectos (hop count) hacia algunas redes específicas hasta que (típicamente) se imponga algún límite arbitrario.

CPE Customer Premises Equipment: Equipo en las instalaciones del cliente. Equipo terminal, tal como terminales, teléfonos y modems, proporcionados por la compañía telefónica, que se instalan en el local del cliente y se conectan a la red de teléfonos.

CPT Cisco Protocol Translator. Traductor de protocolos Cisco. Producto Cisco, en chasis C. que traduce (actúa como intercomunicador) entre protocolos diversos.

CRC Cyclic Redundancy Test: Prueba ciclica de redundancia. Técnica de verificación de errores en la cual el receptor del marco (frame) calcula el residuo de dividir el contenido del marco entre un divisor binario primo (a lo cual a veces también se llama CRC) y lo compara con el valor previo que el nodo emisor almacenó en el marco mismo.

CREN The Corporation for Research and Educational Networking: Corporación de redes educativas y de investigación. Resultado de la fusión de BITNET y CSNET.

cross talk Diafonía. Energía de interferencia transferida de un circuito a otro.
CSC/3 Tarjeta de procesamiento Cisco basada en un microprocesador MC68020 de 30 MHz. Véase procesador de ruta.

CSC-ENVM Cisco environmental monitor card: Tarjeta monitora del entorno, para el chasis AGS+, que detecta las condiciones de voltaje y temperatura para garantizar una adecuada suspensión forzosa de las operaciones en el caso de condiciones anómalas en el sistema.

CSC-FCIT Tarjeta de interface FDDI de Cisco con puenteo con traducción (translational bridging).

CSC-MC Tarjeta de memoria Cisco con 32 kilobytes de memoria. La tarjeta **CSC-MC** proporciona al enrutador Cisco información no volátil de configuración.

CSC-MC+ Tarjeta de memoria Cisco que contiene circuitos de memoria RAM no volátil para almacenar la información de la configuración y que usa tecnología Flash EPROM para guardar el software de sistema operativo.

CSC-MCI Tarjeta de interface Cisco con interfaces para diversos tipos de medios (por ejemplo, Ethernet y líneas serie).

CSC-MEC Tarjeta de interface Cisco con 2, 4 y 6 puertos Ethernet.

CSC-R16 Tarjeta de interface Cisco que maneja Token Ring de 4 ó 16 Mbps.

CSC-SCI Tarjeta de interface Cisco que maneja cuatro puertos de interfaz serie sincrónica con velocidades de transmisión de hasta 4 Mbps cada una.

CSMA/CD Carrier Sense Multiple Access with Collision Detection: Acceso múltiple con detección de portadora y detección de colisiones. Mecanismo de acceso al canal en el cual los dispositivos que desean transmitir primero verifican la existencia de portadora en el canal. Si no se detecta portadora en un cierto lapso, los dispositivos pueden transmitir. Si dos de ellos transmiten a la vez, ocurre una colisión, que es detectada por dispositivos especiales, que entonces retardan la

retransmisión durante un periodo aleatorio. El acceso CSMA/CD es empleado por Ethernet y por IEEE 802.3 .

CSNET Computer+Science Network. Gran inter-red que consiste primordialmente en universidades, centros de investigación e intereses comerciales. CSNET se fusionó con BITNET para formar CREN.

CSU Channel Service Unit. Unidad de servicio al canal. Dispositivo de interface digital que conecta equipos terminales de usuario al ciclo (loop) telefónico digital local.

CTS Clear to Send. Preparado para transmisión. Circuito en la especificación RS-232 que se activa cuando el DCE (equipo de comunicación de datos) está listo para aceptar datos del DTE (equipo terminal).

D4 framing Marcos tipo D4. Formato de los marcos (frames) usados por la mayoría de los sistemas de 1.544 Mbps.

DARPA Defense Advanced Research Projects Agency: Agencia de proyectos avanzados de investigación para la defensa. Agencia de gobierno de los EEUU que financió la investigación y el desarrollo de Internet.

DARPA Interet Véase Internet.

DAS Dual Attach Station: Estación asignada doble. En FDDI, estación conectada a ambos anillos.

data channel Canal de datos. En SNA, dispositivo que conecta el procesador y la memoria central con los periféricos. Véase canal.

dataflow control layer Capa de control de flujo de datos. Capa 5 del modelo de arquitectura SNA.

datagram Datagrama. Agrupamiento lógico de información enviada como unidad de la capa de red (network layer) en un medio de transmisión, sin el establecimiento previo de un circuito virtual.

Los términos paquete, marco, (frame), segmento y mensaje también se emplean para describir agrupaciones lógicas de información en varios niveles del modelo de referencia OSI y en otras áreas de la tecnología. Los datagramas IP son las unidades primarias de información en Internet.

data link control layer Capa de control de enlace de datos. Capa 2 del modelo de arquitectura SNA.

data link layer Capa de enlace de datos. Capa 2 del modelo de referencia OSI, que toma un medio de transmisión de datos y lo transforma en un canal que, desde el punto de vista de la capa de red: network layer, está libre de errores de transmisión. Los servicios principales de la capa de comunicación o enlace de datos son el direccionamiento, la detección de errores y el control del flujo. DATANET IPSN importante de los Países Bajos.

DATAPAC Gran PSN canadiense.

Datapak Red pública de conmutación de paquetes de los países nórdicos.

data sink Sumidero de datos. Equipo de redes que acepta transmisiones de datos.

Datex-1 Red pública alemana de circuitos conmutados.

Datex-p Red pública alemana de conmutación de paquetes.

DCA Defense Communications Agency: Agencia de comunicaciones de la defensa. Organización del gobierno de los Estados Unidos responsable de las redes DDN tales como MILNET.

DCE Data Communications Equipment: Equipo de comunicación de datos (según EIA), o Data Circuit-Terminating Equipment: Equipo terminal de circuitos de datos (según CCITT). Dispositivos y conexiones de una red de comunicaciones que conectan el circuito de comunicación con el dispositivo terminal (DTE). Un modem puede ser considerado como DCE.

D Channel Canal ISDN full duplex de 16 Kbps (tasa básica) o de 64 Kbps (tasa primaria).

DDN Defense Data Network. Red de datos de la defensa. La sección MILNET y otras partes asociadas de Internet que conectan instalaciones militares.

DDN X.25 Protocolo del Departamento de la Defensa de los Estados Unidos muy similar a X.25 y que es empleado en comunicaciones de la red DDN.

DECnet Grupo de productos de comunicaciones (incluyendo protocolos) desarrollados y mantenidos por Digital Equipment Corporation (DEC). La versión más reciente es DECnet Phase V, que está basada fundamentalmente en los protocolos OSI.

DECnet routing Introducido en DECnet Phase M, es el esquema propio de enrutamiento de DEC. En DECnet Phase V, completó la transición a los protocolos de enrutamiento OSI (ES-IS y IS-IS).
dedicated line Línea dedicada. Línea de comunicaciones que no es conmutada. Cuando la línea no es propiedad del usuario suele emplearse el término *leased line*: línea arrendada.

de facto standard Estándar definido por el uso más que por decreto oficial; estándar por omisión o por default.

default route Ruta por omisión. Entrada de la tabla de rutas empleada para dirigir los marcos (frames) para los cuales no existe un trayecto (hop) explícitamente definido.

de jure standard Estándar por decreto oficial.

demarc Punto de demarcación entre equipo de portadora y equipo telefónico privado (CPE).

demodulation Demodulación. Proceso de devolver una señal modulada a su forma original. Los modems hacen la demodulación tomando una señal analógica y regresándola a su forma digital original.

demultiplex Verbo en inglés que denota la acción de separar varios flujos de salida a partir de una entrada común.

DES Estándar de codificación de datos. Algoritmo criptográfico estándar desarrollado por la Oficina Nacional de Estándares de los Estados Unidos.

designated router Enrutador designado. En OSPF, cada red multiacceso con al menos dos enrutadores conectados tiene un enrutador designado, que genera un anuncio de estado de enlace para la red multiacceso y tiene otras responsabilidades especiales en la ejecución del protocolo. El enrutador designado es elegido con el protocolo Hello OSPF. El

concepto de enrutador designado permite una reducción en el número de adyacencias requeridas en una red multiacceso, lo cual a su vez reduce el tráfico de protocolos de enrutamiento y el tamaño de la base de datos de la topología.

destination address Dirección destino. Dirección de un dispositivo de recepción de la red.

device Dispositivo. Entidad que puede tener acceso a la red. Se emplea en forma intercambiable con nodo.

dial backup Respaldo de marcaje. Característica de los enrutadores que ofrece protección contra fallas de la red WAN al permitir que el administrador configure una línea serie de respaldo mediante una conexión de circuito conmutado.

dial-on-demand routing Enrutamiento por llamadas pedidas. Característica de los enrutadores Cisco que ofrece conexiones por pedido a la red en un entorno que use la red pública comutada (PSTN).

dial-up line Línea de llamada. Circuito de comunicaciones establecido con una conexión de circuito conmutado empleando la red telefónica.

different encoding Codificación diferencial. Técnica de codificación digital en la que un valor binario se denota por un cambio de señal más que por un nivel particular de la señal.

Differential Manchester encoding Codificación diferencial Manchester. Esquema de codificación digital en el que se emplea una transición durante el bit para señal de reloj, y donde una transición al inicio del tiempo de cada bit denota un cero. Es el esquema de codificación empleado por las redes IEEE 802.5/Token Ring.

Dijkstra's algorithm Algoritmo de Dijkstra. Algoritmo de enrutamiento de trayectoria mínima que itera sobre la longitud del camino para determinar el árbol abarcador (spanning tree) de trayectoria mínima. Es de uso común en los algoritmos de estado de enlace. Véase también algoritmo de enrutamiento Bellman-Ford.

dirección Véase address.

directory services Servicios de directorio. Servicios para auxiliar a los

dispositivos de la red para localizar proveedores de servicios.

distance vector routing algorithm Algoritmo de enrutamiento de vector de distancias. Véase Bellman-Ford routing algorithm.

DLC Data Link Control Layer. Capa de control de enlace de datos. Capa SNA responsable de la transmisión de datos entre dos nodos, empleando un enlace físico.

DLCI Data Link Connection Identifier. Identificador de conexión de enlace de datos. Valor Frame Relay (retransmisión de marcos) que identifica una conexión lógica.

DNA Digital Network Architecture: Arquitectura digital de red. Arquitectura de las redes de la compañía Digital Equipment Corporation. Se emplea el término DECnet para referirse a los productos DNA (que incluyen protocolos de comunicaciones).

DNS Domain Name System: Sistema de nombre de dominio. Nombre de sistema distribuido usado en Internet.

DoD Department of defense: Departamento (o ministerio) de la Defensa de los Estados Unidos. Organización de gobierno responsable de la defensa del país. El DoD frecuentemente ha financiado desarrollos de protocolos de comunicaciones.

domain Dominio. En Internet, porción de un árbol de jerarquía de nombres. En SNA es un SSCP y los recursos que controla. En IS-IS, un conjunto lógico de redes. "Dominio" hace referencia a un sistema de redes desarrollado por la empresa Apollo Computers (que ahora es parte de Hewlett-Packard) para uso en sus estaciones de trabajo de ingeniería.

DOMPAC Gran PSN de la Guayana francesa.

downlink station Estación de enlace. Véase estación terrena.

DQDB Distributed Queue Dual Bus: Canal dual de cola distribuida. Protocolo de comunicaciones propuesto por el comité IEEE 802.6 para uso en redes metropolitanas (MAN drop Punto de enlace. Lugar de un canal multipunto en donde se hace una conexión a un dispositivo de la red

drop cable Cable de punto de enlace. Cable corto que conecta un

dispositivo de la red (como una computadora) a un medio físico. Véase AUI.

DS-1 Digital (transmission) System 1: Sistema (de transmisiones) digitales

Digital Signal level 1: Señal digital de nivel 1. Término empleado para referirse a la señal digital de 1.56 Mbps (E.E.U.U.) 6 2.048 (Europa) que maneja el sistema de portadora T1.

DS-3 Digital (transmission) System 3: Sistema (de transmisiones) digital 3, o Digital Signal level 3: Señal digital de nivel 3. Término empleado para referirse a la señal digital de 44 Mbps que maneja el sistema de portadora T3.

DSP Domain Specific Part. Parte de dominio específico. Parte de la dirección CLNS que contiene el identificador de área, el identificador de estación y el byte selector.

DSR Data Set Ready: Equipo para datos listo. Circuito de interface RS-232 que se activa cuando el DCE está encendido y listo para usarse, las DSU Data Service Unit. Unidad de servicio de datos. Dispositivo empleado en la transmisión digital para conectar un CSU a un DTE.

DTE Data Terminal Equipment: Equipo terminal de datos. Parte de una estación de datos que sirve como fuente o destino de los datos, o ambos, y que ofrece las funciones de control de comunicación de datos de acuerdo con los protocolos. DTE incluye computadoras, traductores de protocolo y multiplexores.

DTR Data Terminal Ready: Terminal de datos lista. Circuito RS-232 que, se activa para avisar al DCE cuando el DTE está listo para enviar y recibir datos.

dual IS-IS Véase integrated IS-IS.

dynamic address resolution Resolución dinámica de direcciones. Uso de un protocolo de resolución de direcciones para determinar y almacenar información de direcciones que se solicita.

dynamic routing Enrutamiento dinámico. Enrutamiento que se ajusta en forma automática a cambios de tráfico o de topología de la red.

EARN European Academic Research Network: Red Europea de investigación académica. Red que conecta universidades e institutos de investigación.

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

E Channel Canal de control ISDN de conmutación de circuitos de 64 Kpbs.

echoplex Modo en el que los caracteres del teclado se despliegan como eco en la pantalla de la terminal, una vez que la señal apropiada del otro extremo de la línea regresa para indicar que se recibieron correctamente.

ECMA European Computer Manufacturers Association: Asociación de fabricantes europeos de computadoras. Grupo de distribuidores europeos que han hecho trabajo importante de estandarización OSI.

EDI Electronic Data Interchange: Intercambio electrónico de datos. Comunicación electrónica de datos operacionales tales como pedidos y facturas entre organizaciones

error control Control de errores. Técnica para asegurar que las transmisiones de la fuente sean recibidas en el destino sin errores.

error-correcting code Código de corrección de errores. Código con la formación suficiente inteligencia y dotado con la suficiente información de señalización para permitir la detección y corrección de muchos errores en el lado receptor.

error-detecting code Código de detección de errores. Código que puede detectar errores de transmisión mediante el análisis de los datos recibidos, basado en el grado de adhesión a guías estructurales apropiadas que tengan.

ES-IS End System to Intermediate System: De sistema final a sistema intermedio. Protocolo OSI que define la forma en que los sistemas finales (anfitriones) se presentan a los sistemas intermedios (enrutadores).

Ethernet Especificación de red LAN de banda base inventada por la

corporación Xerox y desarrollada en forma conjunta por Xerox, Intel y Digital Equipment Corporation. Las redes Ethernet operan a 10 megabits por segundo utilizando CSMA/CD) sobre cable coaxial. Es similar a una serie de estándares producidos por IEEE y conocidos como IEEE 802.3.

EtherTalk Protocolos AppleTalk que funcionan en Ethernet.

ETSI European Telecommunication Standards Institute: Instituto europeo de estándares de telecomunicaciones. Organización creada por los PTT europeos y la Comunidad Europea para proponer estándares de telecomunicaciones para Europa.

EUnet Red UNIX europea diseñada para ofrecer servicios de interconexión y de correo electrónico que comenzó como extensión de USENET.

Euronet Esquema de redes propuesto por los países del mercado común europeo.

event Suceso, acontecimiento. Mensaje de la red que indica irregularidades operacionales en los elementos físicos de una red, o la respuesta ante la ocurrencia de una tarea significativa, que normalmente es el cumplimiento de un pedido de información.

EXEC Término que Cisco emplea para designar al software que interpreta las órdenes en los productos Cisco.

expansion Expansión. El paso de datos comprimidos a través de un algoritmo que los restituye a su tamaño original. Véase también compression.

expedited delivery En forma general, se refiere a una opción propuesta por una capa específica de un protocolo mediante la cual se pide a otras capas de protocolos (o a la misma capa del protocolo en otro dispositivo de la red) el manejo más rápido de ciertos datos específicos.

explicit route Ruta explícita. En SNA, ruta de una subárea fuente a una subárea destino, especificada por una lista de nodos de subárea y por grupos de transmisiones (transmission groups) que las conectan.

explorer frame Marco de exploración. Marco que envía un dispositivo de la red en un entorno de puenteo de rutas fuente (source route bridging) para determinar la ruta óptima hacia otro dispositivo de la red.

exterior gateway protocol Protocolo de servidor de interconexión externo. Cualquier protocolo de interconexión de redes empleado para intercambiar información de rutas entre sistemas autónomos. No debe confundirse con EGP, que es una instancia particular de uno de ellos.

fan-out unit Unidad de frente de salida. Dispositivo que permite que múltiples dispositivos se comuniquen

fast switching Conmutación rápida. Característica que maneja Cisco, en la cual se usa una memoria rápida caché de ruta para acelerar el paso del paquete a través del enrutador.

fault management Manejo de fallas. Una de cinco categorías de manejo de redes definida por ISO para redes OSI. El manejo de fallas intenta asegurar que las fallas en la red se detecten y controlen.

FC Federal Communications Commission: Comisión federal de comunicaciones. Agencia del gobierno de los Estados Unidos que supervisa, licencia y controla estándares de transmisión electrónica y electromagnética.

FCS Frame Check Sequence: Secuencia de verificación de marcos. Término HDLC adoptado por las siguientes capas de enlace de los protocolos que se refiere a los caracteres extra que se añaden al marco para propósitos de control de errores.

FDI Fiber Distributed Data Interface: Interface de datos distribuidos por fibra. Estándar definido por ANSI que especifica una red token-passing de 100 Mbps empleando cable de fibra óptica.

FD Frequency Division Multiplexing: Multiplexación por división de frecuencia. Técnica en la que en un solo cable se puede asignar a la información de múltiples canales un ancho de banda basado en la frecuencia.

FEP Front End Processor. Procesador frontal. Dispositivo o tarjeta que ofrece a un dispositivo capacidades de interface de red. En SNA, normalmente es un dispositivo 3745.

fiber-optic cable Cable de fibra óptica. Medio flexible y delgado capaz de conducir transmisiones de luz modulada. Comparado con otros medios de transmisión, el cable de fibra óptica es más caro, no es sensible a la interferencia electromagnética y es capaz de mayores velocidades de manejo de datos.

file transfer Transferencia de archivos. Una de las aplicaciones de redes más populares, en la que se llevan archivos de un dispositivo de la red a otro.

filter Filtro. En forma genérica, se refiere a un proceso o dispositivo que filtra la información que le llega, permitiendo sólo el paso de algún subconjunto de ella que tenga ciertas características. En NetCentral de Cisco, se trata de una función que limita los datos que le llegan para transferirlos a NetView.

firmware Instrucciones de software que residen permanente o semipermanentemente en ROM.

flapping Aleteo. Problema de enrutamiento en el que la ruta anunciada entre dos nodos alterna (aletea) de ida y vuelta entre dos trayectorias, debido a un problema que causa fallas intermitentes en la interface.

Flash EPROM Nueva tecnología de PROM (Programmable Read-Only Memory) desarrollada por Intel y licenciada a otras compañías de semiconductores. Es un medio de almacenamiento no volátil que se puede borrar y reprogramar eléctricamente en el circuito. Se emplea en los enrutadores Cisco para lograr la carga inicial y la subsecuente retención de la información de configuración en forma no volátil.

flash update Actualización inmediata. Actualización de enrutamiento enviada asincrónicamente en respuesta a un cambio en la topología de la red. Las actualizaciones de enrutamiento normales se envían a intervalos fijos.

flooding Inundación. Técnica de enrutamiento en la que la información de enrutamiento que recibe el dispositivo enrutador se manda por cada una de sus interfaces, exceptuando (normalmente) la interfaz por la cual se recibió. flow control Control de flujo. Técnica para asegurar que una entidad transmisora no abrume a una entidad receptora con datos.

FNC Federal Networking Council: Consejo federal de redes. Grupo responsable de asesorar y coordinar las necesidades de redes de las agencias federales de los Estados Unidos.

FOIRL Fiber-Optic Inter-Repeater Link: Enlace inter-repetidor de fibra óptica. Metodología de señalización de fibra óptica basada en la especificación de fibra óptica IEEE 802.3.

forward channel Canal de avance. Trayectoria de comunicaciones que lleva información del iniciador de la llamada a quien se llamó.

forwarding Envío. La expedición de un marco (frame) hacia su destino último por medio de un dispositivo de intercomunicación entre redes.

fourier transform Transformada de Fourier. Técnica empleada para evaluar la importancia de diversos ciclos de frecuencia en un patrón de series de tiempo.

fragment Fragmento. Parte de un paquete (packet) mayor que se ha partido en unidades más pequeñas.

fragmentation Fragmentación. Proceso de partir un paquete en unidades menores cuando se transmite en un medio de redes que no maneja el tamaño original del paquete.

frame Marco Agrupamiento lógico de información enviado a un medio de transmisión como una unidad de la capa de enlace (link layer). Los términos paquete, datagrama, segmento y mensaje también se emplean para describir agrupamientos lógicos de información en varias capas del modelo de referencia OSI y en círculos técnicos.

frame relay Retransmisión de marcos. Protocolo empleado en la interface entre dispositivos de usuario (por ejemplo, máquinas anfitriones y enrutadores) y equipo de redes (por ejemplo, nodos de conmutación). Es más eficiente que X.25, protocolo del cual generalmente se considera como reemplazo.

frequency Frecuencia. Medida en Hertz (Hz), es el número de ciclos de una señal de corriente alterna por unidad de tiempo.

front end Nodo o programa que solicita servicios de un back end Véase también cliente y servidor.

FTAM File Transfer, Access and Management: Transferencia, acceso y manejo de archivos. Aplicación OSI desarrollada para intercambio y manejo de archivos en red.

FTP File Transfer Protocol: Protocolo de transferencia de archivos. Protocolo de aplicación IP para transferir archivos entre nodos de la red.

full duplex Capacidad de transmisión simultánea de datos en ambas direcciones.

fuzzball Sistema de cómputo DEC LS- 1 1 que ejecuta software de servidor de intercomunicaciones IR NFSnet usó estos sistemas como conmutadores fundamentales de paquetes.

G.703 Especificación eléctrica y mecánica CCITT para conexiones entre equipo de telecomunicaciones y DTE.

gateway Compuerta o servidor de intercomunicación. En la comunidad IP el término se refería a un dispositivo de enrutamiento. Ahora se prefiere el término enrutador (router) para describir los nodos que hacen esta función, y la palabra gateway se refiere a un dispositivo de propósito especial que efectúa una conversión de información de nivel de capa 7 de una pila de protocolos a otra, como lo hace el producto Cisco CPT.

gateway host Servidor de intercomunicación anfitrión. En SNA, nodo anfitrión que contiene un servidor de intercomunicación SSCR

gateway NCP Servidor de intercomunicación NCP Programa de control de redes (Network Control Program) que conecta dos o más redes SNA y traduce las direcciones para permitir sesiones de tráfico entre redes.

geosynchronous orbit Órbita geosincrónica. Término referido a la órbita de un satélite en la cual su velocidad es igual a la de rotación terrestre, lo cual lo mantiene estacionario relativo a una posición sobre la superficie de la tierra. Las órbitas geosincrónicas requieren una posición de aproximadamente 23,000 millas (37,000 Km) sobre la superficie del globo, sobre el ecuador.

GGP Gateway-to-Gateway Protocol: Protocolo de servidor a servidor de intercomunicaciones. Protocolo MILNET que especifica la forma en que los servidores (o los enrutadores) básicos (core gateway) deben intercambiar información sobre rutas y alcances. El protocolo GGP usa un algoritmo distribuido de camino más corto.

GOSIP Government OSI Profile: Perfil OSI de gobierno. Especificación de gestión para protocolos OSI en el gobierno de los Estados Unidos. A través de GOSIP, el gobierno determina el que todas las agencias

federales se estandaricen en OSI e implanten sistemas basados en esos estándares en la medida en que se puedan obtener en forma comercial.

grade of service Grado de servicio. Medida de la calidad del servicio telefónico basada en la probabilidad de que una llamada reciba señal de ocupado durante la hora pico del día.

ground station Estación terrena. Conjunto de equipo de comunicaciones diseñado para recibir (y usualmente transmitir) señales desde/hacia satélites. También llamada downlink station: estación de enlace.

group address Dirección de grupo. Dirección única que se refiere a múltiples dispositivos de la red. Sinónimo de multicast address (dirección múltiple)

guard band Banda de guardia. Frecuencia libre entre dos canales de comunicaciones, que los separa para prevenir interferencia mutua.

half duplex Capacidad de transmitir datos en sólo una dirección a la vez.

half gateway Medio gateway. Literalmente, dispositivo que efectúa las funciones de medio servidor de intercomunicaciones, pues éstos suelen dividirse en dos mitades funcionales para facilitar su diseño y mantenimiento.

handset Parte del teléfono que contiene el micrófono y la bocina, y que se toma con la mano durante su uso.

handshake Secuencia de mensajes que dos o más dispositivos de la red intercambian para asegurar sincronización en la transmisión.

hardware address Dirección de hardware. También conocida como physical address: dirección física o MAC-layer address: dirección de la capa de control de acceso. Capa de enlace de datos asociada con un dispositivo particular de la red. Contrasta con una dirección o protocolo de red, que es una dirección de la capa de red (network layer).

H Channel Canal H. Canal ISDN primario full duplex que opera a 384 Kbps.

HDH HDLC Distant Host. Anfitrión remoto HDLC. Forma de ejecutar el protocolo 1822 sobre enlaces serie sincrónicos en lugar de sobre hardware especial 1822. HDH es esencialmente headers (encabezados) 1822 y datos encapsulados en paquetes LAPB (X.25 nivel 2).

HDLC High-level Data Link Control: Control de enlace de datos de alto nivel. Protocolo de capa de enlace ISO estándar por bits de uso común, derivado de SDLC. Especifica un método de encapsulamiento de datos en enlaces serie sincrónicos. El servicio HDLC de Cisco sólo maneja la creación de marcos y funciones de suma de control (checksum).

headend El punto terminal de una red broadband (de banda amplia). Todas las estaciones transmiten hacia ese punto, para que luego éste transmita hacia las estaciones destino.

header Encabezado. Información de control que se añade a los datos antes de encapsularlos para su transmisión en la red.

heartbeat Latido Véase SQE.

HELLO Protocolo de enrutamiento empleado principalmente por los nodos NSFnet. Permite a conmutadores contables descubrir rutas de retraso mínimo. Por otro lado, el protocolo Hello (sin relación con HELLO de NSFnet) es empleado por sistemas OSPF para establecer y mantener relaciones de vecindad.

HEMS High-level Entity Management System: Sistema de manejo de entidades de alto nivel. Interesante protocolo de manejo de redes que fue candidato para estandarización en Internet hasta que sus diseñadores lo retiraron durante el proceso de evaluación, en deferencia para SGMP y CMOT.

HEPnet High-Energy Physics network: Red de física de altas energías. Red de investigación originada en los Estados Unidos y que se ha extendido a muchos de los lugares en donde se hace investigación en física de altas energías. Los sitios más conocidos en los que se usa incluyen al Laboratorio Nacional Argonne, al Laboratorio Nacional de Brookhaven, el Laboratorio Lawrence Berkeley y el Centro del Acelerador Lineal de Stanford (SLAC).

Hertz Abreviado como "Hz"; medida de frecuencia o de ancho de banda. Sinónimo de ciclos/segundo.

heterogeneous network Red heterogénea. Red consistente en dispositivos disímiles que ejecutan protocolos disímiles y que en muchos casos manejan funciones o aplicaciones disímiles.

hierarchical routing Enrutamiento jerárquico. Enrutamiento basado en un sistema de direccionamiento jerárquico. Por ejemplo, los algoritmos de enrutamiento IP emplean direcciones IP, que contienen números de la red, números de máquinas anfitriones y (posiblemente) números de subredes.

HIPPI High-Performance Parallel Interface: Interface paralela de alto rendimiento. Estándar de interfaz de alto rendimiento definido en el estándar ANSI X3T9.3/88-023.

holddowns Sujeciones. Característica de algunos protocolos de enrutamiento en los que se impide que las actualizaciones regulares de rutas equivocadamente reinstalen una ruta que ha fallado.

hop count Cuenta de trayecto. Métrica de enrutamiento usada para medir la distancia entre una fuente y un destino. Cada hop equivale al paso de un packet (paquete) por un enrutador.

host Anfitrión. Sistema de cómputo en una red. Es similar a los términos device (dispositivo) o node (nodo), excepto que usualmente implica un sistema de cómputo, mientras que dispositivo y nodo generalmente se aplican a cualquier sistema en red, que incluye terminal servers (servidores de terminales) y enrutadores.

host node Nodo anfitrión. Nodo de subárea SNA que contiene un SSCR

HP Probe Véase probe.

HSCI High-Speed Communications Interface: Interface de comunicaciones de alta velocidad. Controlador desarrollado y distribuido por Cisco. Se trata de una interface de un solo puerto que ofrece capacidades de comunicación sincrónica serie full duplex hasta a 52 Mbps. Se instala en enrutadores Cisco.

HSSI High-Speed Serial Interface: Interface serie de alta velocidad. Estándar de redes para comunicaciones serie de alta velocidad (hasta 52 Mbps) sobre enlaces WAN.

hub Concentrador. En forma genérica, término que describe un dispositivo que sirve como centro de una red con topología de estrella. En la terminología Ethernet/IEEE 802.3 se refiere a un repetidor

multipuerto, que a veces también se conoce como concentrator (concentrador). El término también se usa para el dispositivo de hardware el software que contiene múltiples módulos independientes, aunque conectados, de equipo de redes e interconexión entre redes. Los concentradores pueden ser activos (que repiten las señales que les llegan) o pasivos (que no repiten, sino sólo reparten las señales que les llegan).

hybrid network Red híbrida. Término usado para describir una interconexión entre redes hecha con más de un tipo de tecnología de redes, que incluye LAN y WAN.

IAB Internet Activities Board. Grupo de actividades de Internet. Investigadores de interconexiones entre redes que se reúnen regularmente para discutir asuntos pertinentes de Internet. El grupo define políticas de Internet mediante decisiones y asignación de fuerzas de trabajo para asuntos varios.

ICMP Protocolo Internet de control de mensajes. Protocolo de la capa de red que permite que los paquetes de mensajes reporten errores e información relevante al procesamiento de paquetes IP. Está documentado en RFC 792.

IDD Initial Domain Part. Sección inicial de dominio. Parte de una dirección CLNS que contiene un identificador de autoridad y de formato, y un identificador de dominio.

IDPR Interdomain Policy Routing: Política de enrutamiento interdominios. Protocolo experimental de enrutamiento entre dominios que intercambia políticas entre sistemas autónomos en forma dinámica. IDPR encapsula el tráfico de los sistemas inter-autónomos y lo enruta de acuerdo con las políticas de cada sistema autónomo a lo largo del trayecto. Actualmente es una propuesta de IETF

IDRP IS-IS Interdomain Routing Protocol: Protocolo de enrutamiento interdominios IS-IS. Protocolo OSI que especifica cómo se comunican enrutadores con enrutadores en diferentes dominios.

IEEE Institute of Electrical and Electronic Engineers: Instituto de ingenieros eléctricos y electrónicos. Organización profesional que define estándares de redes. Los estándares LAN de IEEE son los predominantes en la actualidad, e incluyen protocolos similares o virtualmente equivalentes a Ethernet y Token Ring

IEEE 802.2 Protocolo LAN de IEEE que especifica la implantación de

la subcapa de control de enlace lógico de la capa de enlace. Se encarga del manejo de errores, creación de marcos y flujo de control; es interface de servicio con la capa 3. Se emplea en redes LAN tales como IEEE 802.3 e IEEE 802.5

IEEE 802.3 Protocolo LAN de IEEE que especifica la implantación de la capa física y de la subcapa MAC de la capa de enlace. Utiliza accesos CSMA/CD en varias velocidades usando varios medios físicos. Una variante física de IEEE 802.3 (10BASE5) es muy similar a Ethernet.

IEEE 802.4 Protocolo LAN de IEEE que especifica la implantación de la capa física y de la subcapa MAC de la capa de enlace. Utiliza acceso token passing sobre una topología de bus.

IEEE 802.5 Protocolo LAN de IEEE que especifica la implantación de la capa física y de la subcapa MAC de la capa de enlace. Utiliza acceso token passing a 4 ó 16 Mbps sobre cable de par trenzado blindado y es muy similar a Token Ring de IBM.

IEEE 802.6 Especificación IEEE de red de área metropolitana (Metropolitan Area Network: MAN) basada en tecnología DQDB.

IETF Internet Engineering Task Force: Fuerza de trabajo de ingeniería Internet. Equipo de trabajo IAB que consiste en más de 40 grupos responsables de asuntos ingenieriles Internet solubles a corto plazo.

IFIP International Federation for Information Processing: Federación internacional de procesamiento de información. Organización de investigación que realiza trabajos de pre-estandarización OSI. Entre sus logros se encuentra la formalización del modelo original MHS.

IGP Interior Gateway Protocol: Protocolo de servidores de intercomunicación internos. Protocolo Internet usado para intercambio de información de enrutamiento en un sistema autónomo. Ejemplos usuales de IGP Internet son IGRP, RIP y OSPF

IGRP Interior Gateway Routing Protocol: Protocolo de enrutamiento de servidores de intercomunicación internos. IGP desarrollado por Cisco para resolver problemas relativos a enrutadores en redes grandes y heterogéneas.

IGS Integrated Gateway Server: Servidor de intercomunicación integrado. Enrutador/puente Cisco integrado de configuración fija.

IMP Interface Message Processor. Procesador de interface de mensajes. Nombre que anteriormente tenían los conmutadores de paquetes de Internet. Ahora se llaman packet-switched nodes (nodos de paquetes conmutados), packet switches (conmutadores de paquetes) o switches (conmutadores).

in-band signaling Señalización en banda. Transmisión dentro de una gama de frecuencias normalmente empleada para transmitir información. Contrasta con out-of-band signaling (señalización fuera de banda), que usa frecuencias fuera de la gama normal de las empleadas para transferir información.

infrared Infrarrojo. Ondas electromagnéticas con gama de frecuencias por encima de las microondas pero abajo del espectro visible. Recién comienzan a surgir sistemas LAN basados en esta tecnología.

INOC Internet Network Operations Center: Centro de operaciones de redes Internet. Grupo de BBN que, en los inicios de Internet, controlaba y supervisaba los enrutadores y servidores de interconexión primarias.

INTAP Interoperability Technology Association for Information Processing: Asociación de tecnología de interoperatividad para procesamiento de información. Organización técnica creada para desarrollar perfiles OSI japoneses y pruebas de aceptación.

Integrated IS-IS Protocolo de enrutamiento basado en el protocolo OSI de enrutamiento IS-IS y que además se maneja en redes IP u otras. Las implantaciones de IS-IS integrado envían solamente un conjunto de actualizaciones de enrutamiento, por lo cual resulta más eficiente que dos implantaciones separadas. Antes se conocía como Dual IS-IS.

Interface Conexión entre dos sistemas o dispositivos. En la terminología de enrutadores, es una conexión de la red. También se refiere a la frontera entre capas adyacentes del modelo OSI. En telefonía, es una frontera compartida que está definida por características de interconexión física comunes, características de la señal y significados de las señales intercambiadas.

interference Interferencia. Ruido indeseado en el canal de comunicación.

intermediate system Sistema intermedio. Nodo de enrutamiento en una

red OSI.

International Standards Organization Organización internacional de estándares. Expansión errónea del acrónimo ISO.

Internet Término empleado para referirse al sistema de interconexión de redes más grande del mundo, que conecta miles de redes en todo el planeta, y que desarrolló una "cultura" basada en simplicidad, investigación y estandarización fundamentada en el uso real. Buena parte de la tecnología de punta en redes vino de esta comunidad. Internet evolucionó a partir de ARPANET.

Internet address Dirección Internet. También llamada "dirección IP", es una dirección de 32 bits asignada a máquinas anfitrionas que emplean puntos (formato decimal con punto), formados por la sección de la red, una sección opcional de subred y una sección del anfitrión.

internetwork Redes interconectadas. Conjunto de redes interconectadas por enrutadores y que en forma genérica funciona como una sola. A veces se le llama internet, lo cual no debe confundirse con la palabra Internet.

internetworking Interconexión de redes. Término genérico usado para referirse a la industria que surgió alrededor del problema de conectar redes. El término se puede referir tanto a productos como a procedimientos y tecnologías.

interoperability Interoperabilidad. Capacidad para comunicar equipos de computación de diversos fabricantes mediante una red.

intra-area routing Enrutamiento entre áreas. Término empleado en los enrutadores DECnet para describir enrutamiento dentro de un área.

IP Internet Protocol. Protocolo Internet. Protocolo de capa 3 (capa de red) que contiene información de direccionamiento y de control para permitir el enrutamiento de paquetes. Está documentado en R.FC 79 1.

IP address Dirección IP, Véase Internet address.

IPSO IP Security Option: Opción de seguridad IP. Parte del protocolo Internet (IP) que define niveles de seguridad basados en las interfaces.

IPX Internetworking Packet Exchange: Intercambio de paquetes de interconexión de redes. Protocolo Novell de capa 3, similar a XNS e IP que se emplea en redes NetWare.

IRN Intermediate Routing Node: Nodo de enrutamiento intermedio. En SNA, un nodo de subárea con capacidades de enrutamiento intermedio.

IRTF Internet Research Task Force: Equipo de trabajo para investigación en Internet. Comunidad de investigadores en redes con interés en interconexión de redes. Está comandado por el grupo de gobierno en investigación Internet (Internet Research Steering Group: IRSG).

isarithmic flow control Flujo de control isaritmico. Técnica de flujo de control en donde los permisos para transmitir viajan a lo largo de la red. La posesión de uno de ellos posibilita el derecho a transmitir.

ISDN Integrated Services Digital Network: Red digital de servicios integrados. Protocolos de comunicación propuestos por las compañías telefónicas para lograr que las redes de teléfono transmitan datos, voz y otros materiales de la fuente.

IS-IS Intermediate System to Intermediate System: Sistema intermedio a sistema intermedio. Protocolo jerárquico de enrutamiento OSI de estado de enlace (link-state), basado en enrutamiento DECnet Phase V, en donde los sistemas intermedios (enrutadores) intercambian información basada en una sola métrica, para determinar la topología de la red.

ISO International Organization for Standardization: Organización internacional para la estandarización. Organización internacional responsable de una amplia gama de estándares, incluyendo aquellos relevantes para las redes. ISO es responsable del modelo de referencia de redes más popular: el modelo de referencia OSI.

isochronous transmission Transmisión isocrónica. Transmisión asincrónica (start-stop) sobre un enlace de datos sincrónico. En telefonía, isocrónico implica un muestreo de bits de tasa constante, y se conoce como la inversa de la transmisión asincrónica.

ISODE ISO Development Environment: Entorno de desarrollo ISO. Implantación popular de las capas superiores ISO en una pila de protocolo TCP/IP.

jabber Balbuceo. Condición de error en la cual un dispositivo de la red

continuamente transmite "basura" a la red. En IEEE 802.3 se refiere a un paquete de datos cuya longitud excede a la prescrita en el estándar.

JANET Joint Academic Network: Red académica conjunta. Red universitaria en el Reino Unido.

jitter Distorsión de las líneas de comunicación analógicas causada por una variación en las posiciones de referencia temporal de una señal. Puede causar pérdida de datos, particularmente a altas velocidades.

JUNET Japan UNIX Network: Red japonesa de Unix. La red nacional no comercial más grande del Japón, diseñada para promover las comunicaciones entre investigadores japoneses y extranjeros.

JVNCnet John von Neumann Center Network: Centro de redes John von Neumann. Red regional compuesta de enlaces T1 y enlaces serie más lentos, que ofrece servicios de red de nivel medio en localidades del Noroeste de los Estados Unidos.

LAN Local Area Network: Red de área local. Red que cubre un área geográfica relativamente pequeña (usualmente no mayor que un grupo local de edificios). Comparadas con las redes WAN, las redes LAN suelen caracterizarse por velocidades de transferencia de datos relativamente altas y una relativamente baja incidencia de errores.

LAN Manager Sistema de archivos distribuidos desarrollado y manejado por Microsoft.

LAN Network Manager Paquete de manejo Token Ring y source-bridge ofrecido por IBM. Normalmente opera en una PC y verifica los puentes de rutas fuente (source-route bridges) y los dispositivos Token Ring, y puede pasar mensajes de alerta a NetView.

LAN Server Sistema de archivos distribuido derivado de LAN Manager, desarrollado y manejado por IBM.

LAPB Link Access Procedure: Balanced: Procedimiento balanceado de acceso de enlace. Derivado de HDLC, es una versión CCITT X.25 de un protocolo de enlace de datos por bits.

LAPD Link Access Protocol D: Protocolo D de acceso de enlace. Protocolo ISDN de capa de enlace (link layer) para el canal D. Se derivó del protocolo LAPB, CCITT X.25 y está diseñado primordialmente para satisfacer los requerimientos de señalización del acceso básico ISDN. Está definido por las recomendaciones Q.920 y Q.921 de CCITT.

LASER Light Amplification by Stimulated Emission of Radiation: Amplificación de luz por emisión estimulada de radiaciones. Dispositivo analógico de transmisión en el cual un material activo adecuado es excitado por un estímulo externo para producir un estrecho haz de luz coherente, que puede ser modulado en pulsos para transmitir datos. Las redes basadas en tecnología láser están apenas comenzando, pero parecen prometedoras debido a anchos de banda potencialmente amplios y a una relativa resistencia a la interferencia.

LAT Local Area Transport: Transporte de área local. Protocolo de terminal virtual de red desarrollado por Digital Equipment Corporation.

LATA Local Access and Transport Area: Área de transporte y acceso local. Área de marcaje telefónico atendida por una sola compañía telefónica local. Las llamadas dentro de un área LATA se conocen como llamadas locales. Hay más de cien de estas áreas en los Estados Unidos.

leased line Línea arrendada o privada. Línea de transmisión reservada por un portador de comunicaciones para uso privado de un cliente.

level 1 route Ruta de nivel 1. Ruta OSI o DECnet dentro de un área.

level 2 route Ruta de nivel 2. Ruta OSI o DECnet entre áreas.

line Línea. En forma genérica se refiere a lo mismo que link (enlace). En SNA, es una conexión a la red.

line conditioning Acondicionamiento de línea. Uso de equipo, en líneas de voz arrendadas, para mejorar las características analógicas, permitiendo así mayores velocidades de transmisión.

line driver Dispositivo manejador de la línea. Convertidor de señal/amplificador poco costoso que acondiciona las señales digitales para garantizar una transmisión confiable a largas distancias.

line of sight Línea de vista. Característica de ciertos sistemas de transmisión, como el láser, las microondas y los sistemas infrarrojos, en donde no puede existir obstrucción en el camino directo entre el transmisor y el receptor.

line turnaround Tiempo de cambio en la línea. Tiempo requerido para cambiar la dirección de la transmisión de datos en una línea de teléfono.

link Enlace. Canal de comunicaciones de la red consistente en un

circuito o una trayectoria de transmisión, incluido el equipo existente entre el transmisor y el receptor. Suele usarse para referirse a una conexión en una red WAN.

link layer Capa de enlace. Véase data link layer.

Link-state routing algorithm Algoritmo de estado de enlace. Algoritmo de enrutamiento en el que cada enrutador difunde a todos los nodos la información del costo de acceso a cada uno de sus vecinos. Estos algoritmos crean una vista consistente de la red y por ello no son propensos a caer en ciclos de enrutamiento, aunque logran esto a costa de una relativamente mayor dificultad computacional y de un tráfico un tanto más diseminado (en comparación con los algoritmos de enrutamiento de vector de distancias). Véase también Bellman-Ford routing algorithm.

little-endian Método de almacenar o transmitir datos en el cual se presenta primero el bit o byte menos significativo. Véase también big-endian.

LLC Logical Link Control: Control lógico de enlace. Subcapa de la capa de enlace OSI definida la IEEE. Se encarga del control de errores, control de flujo y creación de marcos. El protocolo LLC más usado es IEEE 802.2, que incluye variantes sin y con conexión.

LM/XLAN Manager for UNIX. LAN Manager para entornos UNIX.

LNMLAN Network Manager: Manejador de redes LAN. Producto de IBM para el manejo de un conjunto de puentes de rutas fuente (source-route) y sus entornos Token Ring.

load balancing Balanceo de carga. En enrutamiento se refiere a la capacidad de un enrutador para distribuir el tráfico a todos sus puertos de la red que estén a la misma distancia de la dirección de destino. Los buenos algoritmos de balanceo de cargas usan información sobre la velocidad de la línea y sobre su contabilidad. El balanceo de la carga incrementa la utilización de los segmentos de la red y aumentan el ancho de banda efectivo de la red.

local acknowledgment Acuse de recibo local. Metodo en el cual un nodo intermedio de la red, tal como un enrutador Cisco, termina una sesión de la capa de enlace de datos para una máquina anfitriona final. El uso de estos acuses de recibo locales reduce la sobrecarga de la red y por tanto el riesgo de interrupciones.

local bridge Puente local. Puente que directamente interconecta redes en la misma área geográfica.

local loop Ciclo local. La línea que va de las instalaciones del abonado del teléfono a la oficina central (CO) de la compañía telefónica.

LocalTalk Protocolo de red de banda base CSMA/CA de 230 Kpbs patentado por Apple.

logical channel Canal lógico. Trayectoria de comunicaciones no dedicada, para conmutación de paquetes, entre dos o más nodos de la red. Mediante conmutación de paquetes pueden existir varios canales lógicos simultáneamente en un mismo canal físico.

loop Ciclo. Ruta en la cual los paquetes nunca llegan a su destino, sino que sólo recorren un ciclo o bucle a través de una serie constante de nodos de la red.

loopback test Prueba de ciclos. Prueba en la cual se envían y regresan señales hacia la fuente en algún punto del trayecto de comunicaciones. Suelen emplearse para probar qué tan utilizables son las interfaces de la red.

LU Logical Unit: Unidad lógica. Componente primario de SNA. Tipo de unidad direccionable (NAU) que permite a los usuarios finales comunicarse entre sí y tener acceso a los recursos de la red SNA.

LU 6.2 Logical Unit 6.2: Unidad lógica 6.2. Unidad lógica que gobierna las comunicaciones SNA entre nodos equivalentes (peer-to-peer). Maneja comunicaciones en general entre programas en un entorno de procesamiento distribuido.

MAC sublayer **Media Access Control sublayer**. Subcapa de control de acceso al medio. Como está definida por la IEEE, se trata de la porción baja de la capa de enlace de datos del modelo OSI. La subcapa MAC se encarga de los asuntos de acceso al medio de comunicaciones, como por ejemplo determinar si se usará token passing (paso de estafeta) o contention (competencia).

MAN **Metropolitan Area Network**: Red de área metropolitana. En términos generales se refiere a una red que ocupa un área metropolitana, geográficamente mayor que la ocupada por una red local (LAN), pero menor que la de una red amplia (WAN). Véase también DQDB.

managed object Objeto de manejo. En manejo de redes se refiere a un dispositivo de la red que es tratado por un protocolo de manejo de la red.

management services Servicios de manejo. Funciones SNA distribuidas entre componentes de la red para manejar y controlar una red SNA.

Manchester encoding Codificación Manchester. Esquema de Codificación digital en el que se emplea una transición durante el bit para señal de reloj, y donde una transición a alto durante la primera mitad del tiempo del bit denota un uno. Es el esquema de codificación empleado por IEEE 802.3 Ethernet.

MAP Manufacturing Automation Protocol: Protocolo de manufactura automática. Arquitectura de red creada por la empresa General Motors para satisfacer las necesidades específicas de la fábrica. Especifica una red local (LAN) token-passing similar a IEEE 802.4.

marco Véase frame.

MAU Medium Attachment Unit (IEEE 802.3): Unidad de vinculación, o **Multistation Access Unit (IEEE 802.5):** Unidad de acceso a estaciones múltiples. En el primer caso, es un dispositivo que realiza las funciones de la capa 1 de IEEE 802.3, que incluyen la detección de colisiones y la inyección de bits a la red. Una unidad MAU se conoce como transceiver (transmisor/receptor) en la especificación Ethernet. En el segundo caso (a veces llamadas también MSAU para que no se confundan con las primeras), se trata de concentradores de cables a los cuales se conectan los nodos de Token Ring.

maxdata Tamaño máximo de datos de un marco (frame) en un enlace.

MCI Compañía de telecomunicaciones que compite con AT&T y con U.S. Sprint en el mercado de suscriptores de servicio de larga distancia.

media Medios. Plural de medium, en inglés. Entorno físico mediante el cual pasan las señales de transmisión. Los medios usuales en redes son el par trenzado, el cable coaxial, la fibra óptica y la atmósfera (a través de la cual viajan las microondas, el láser y la transmisión infrarrojo).

mensaje Véase message.

message Mensaje. Agrupamiento lógico de información en la capa de

aplicación (application-layer). Véase también packet, frame, segment y datagram.

message switching Conmutación de mensajes. Técnica de conmutación que transmite mensajes de nodo a nodo en una red. El mensaje se almacena en cada nodo hasta que llega el momento en que se consigue una trayectoria de envío. Véase también packet switching y circuit switching.

MGS Mid-size Gateway Server: Servidor de intercomunicaciones de tamaño medio. Enrutador/puente Cisco de 4 ranuras.

MHS Message Handling System: Sistema de manejo de mensajes. Recomendación CCITT X.400 que ofrece servicios de manejo de mensajes para comunicaciones en aplicaciones distribuidas. NetWare MHS es una entidad diferente (aunque similar) que también ofrece manejo de mensajes y es distribuida por la empresa Novell.

MIB Management Information Base: Base de manejo de información. Base de datos de información sobre manejo de objetos, a la que se puede tener acceso mediante protocolos de manejo de red tales como SNMP y CMIP.

MIC Media Interface Connector. Conector FDDI que es un estándar por default.

microwave Microondas. Ondas electromagnéticas en la gama de 1 a 30 Gigahertz. Las redes basadas en microondas constituyen una naciente tecnología que gana campo debido a su alto ancho de banda y su relativamente bajo costo.

MIDAS PSN australiano.

midsplit Sistema de cable de banda amplia (broadband) en el que las frecuencias disponibles se dividen en dos grupos: uno para transmisión y otro para recepción.

MILNET Military Network: Red militar. Véase DDN.

modelo de referencia OSI Véase OSI Reference Model

MODEM Modulator-Demodulator.- Modulador-demodulador. Dispositivo que convierte señales digitales a una forma adecuada para transmisión sobre medios de comunicación analógicos, y viceversa.

modem eliminator Eliminador de modem. Dispositivo que permite la conexión de dos dispositivos DTE sin el empleo de modems.

modulation Modulación. Proceso por el cual se transforman las características de las señales para representar información. Los tipos de modulación incluyen frecuencia modulada (FM), en donde señales de diferentes frecuencias representan valores de datos diferentes, y amplitud modulada (AM), en donde la amplitud de la señal varía para representar diferentes valores de datos.

MOP Maintenance Operation Protocol. Protocolo de operaciones de mantenimiento. Protocolo DEC, un subconjunto del cual maneja Cisco, que ofrece una forma de realizar operaciones primitivas de mantenimiento en sistemas DECnet. Por ejemplo, puede usarse MOP para pasar una copia de la imagen de un sistema a una estación de trabajo sin discos.

MSAU Multistation Access Unit: Unidad de acceso a estaciones múltiples. Véase MAU.

MSM Servidor de terminales Cisco basado en un chasis M.

MTU Maximum Transmission Unit. Unidad de transmisión máxima. Se refiere al paquete de tamaño máximo, en bytes, que una interface en particular puede manejar.

mu-law Ley mu. Estándar de compresión y expansión (companding) norteamericano usado en conversiones entre señales analógicas y digitales en sistemas PCM.

multicast address Dirección múltiple. Dirección que se refiere a múltiples dispositivos de la red. Sinónimo de group address (dirección de grupo).

multihomed host Anfitrión múltiple. Máquina anfitriona asignada a múltiples segmentos físicos de la red.

multimode fiber Fibra multimodal. Fibra que maneja la propagación de múltiples patrones de campo electromagnético.

multiple domain network Red de dominio múltiple. Red SNA con múltiples SSCP

multiplex La colocación de múltiples señales en un solo canal.

multipoint Line Línea multipunto. También llamada multidrop line: línea de múltiples puntos de enlace. Línea de comunicaciones con múltiples puntos de acceso al cable.

multivendor network Red de varios fabricantes. Red que utiliza equipo de más de un fabricante. Estas redes tienen más problemas de compatibilidad que las de un solo fabricante o distribuidor.

N-1 Red universitaria japonesa que interconecta mainframes (grandes computadoras) mediante X.25 .

NACSIS National Center for Science Information Systems: Centro nacional de sistemas de información sobre ciencia. Red japonesa considerada sucesora de N-1.

Nagle's algorithm Algoritmo de Nagle. Se trata en realidad de dos algoritmos diferentes de control de congestión que se pueden emplear en redes basadas en TCP. Un algoritmo reduce la ventana de envíos mientras que el otro limita los datagramas pequeños.

name resolution Resolución de nombres. En forma general, el proceso de asociar un nombre con una localidad de la red.

name server Servidor de nombres. Servidor que la red ofrece para resolver nombres de la red y asociarlos con localidades (direcciones) de la red.

narrowband Véase baseband.

NAU Network Addressable Unit: Unidad direccionable en la red. Término SNA para las entidades direccionables. Entre los ejemplos se

incluye PU, LU y SSCP

NAUN Nearest Active Upstream Neighbor. Vecino activo más cercano a la fuente. En redes Token Ring o IEEE 802.5 se refiere al dispositivo de la red que aún está activo y que es el más cercano al que actúa como punto de referencia.

NCC Véase NOC.

NCP Network Control Program: Programa de control de la red. En SNA, se refiere a los programas que asignan rutas y controlan el flujo de datos entre un controlador de comunicaciones (en el cual residen) y otros recursos de la red.

NDIS Network Driver/Interface Specification: Especificación de interface del manejador de la red. Producida por Microsoft, es la especificación de un manejador de dispositivos para tarjetas NIC, de tipo general e independiente del hardware y los protocolos.

neighboring routers Rutadores vecinos. En OSPF, se refiere a dos enrutadores que tienen interfaces a una red común. En redes de acceso múltiple, los vecinos se descubren en forma dinámica mediante el protocolo Hello de OSPF.

NET Network Entity Title: Título de entidad de red. Direcciones de la red definidas por la arquitectura de redes ISO y empleadas en redes basadas en CLNS.

NetBIOS Network Basic Input/Output System: Sistema básico de entrada/salida de red. Interface de la capa de sesión para redes de PC, producida por IBM y Microsoft.

NetCentral Producto de software de Cisco que ofrece una herramienta de alto rendimiento para el manejo de interconexión de redes diversas. NetCentral está basado en SNMP y una base de datos relacional de Sybase, y opera en estaciones de trabajo Sun.

NetView Arquitectura y aplicaciones relacionadas con manejo de redes IBM.

NetWare Desarrollado y distribuido por Novell, Inc., se trata del sistema de archivos distribuidos más popular en la actualidad. Ofrece acceso transparente a archivos remotos y muchos otros servicios distribuidos de redes.

network Red. Conjunto de computadoras y otros dispositivos que son capaces de comunicarse entre sí empleando un medio reticular.

network address Dirección de la red. También llamada protocolo de la red (network protocol), es una dirección de la capa de red (network layer) que se refiere a un dispositivo lógico, no físico, de la red.

network administrator Administrador de la red. Persona que ayuda a mantener la red.
network analyzer Analizador de la red. Dispositivo de hardware/software que ofrece algunas características de solución de problemas de la red, incluidos decodificadores de paquetes de protocolos específicos, pruebas de errores preprogramadas, filtrado y transmisión de paquetes.

Network Information Center Centro de información sobre redes. Localidad que controla el acceso a los RFC y más información sobre Internet. Normalmente se conoce como NIC.

Network layer Capa de red. Capa 3 del modelo de referencia OSI. La capa 3 es en donde ocurre el enrutamiento.

network management Manejo de red. Término genérico que describe sistemas o acciones que ayudan a mantener, caracterizar o arreglar una red. Es un tópico importante en el campo más general de las redes.

NFS Network File System: Sistema de archivos en red. Como se emplea normalmente, es un conjunto de protocolos de sistemas de archivos distribuidos desarrollado por la empresa Sun Microsystems, que permite el acceso remoto a archivos en una red. En realidad, NFS es uno de los protocolos del conjunto, que incluye NFS, XDR (External Data Representation: Representación externa de datos), RPC (Remote Procedure Call: Llamada remota a procedimientos), y otros. Esos protocolos son parte de una arquitectura mayor que la empresa Sun nombra como ONC (Open Network Computing).

NIC Network Interface Controller. Controlador de interface de red.

Network Interface Card: Tarjeta de interface de red. Véase adapter.

También es el acrónimo de Network Information Center: Centro de información de redes. Existen muchos centros de información de redes para la comunidad Internet que ofrecen asesoría a usuarios, documentación, capacitación y otros servicios.

N-ISDN Narrow-band ISDN. ISDN de banda angosta.

NIST National Institute of Standards and Technology: Instituto nacional de estándares y tecnología. Anteriormente era el Instituto nacional de estándares (NBS: National Bureau of Standards). Organización del gobierno de los Estados Unidos que respalda y cataloga una variedad de estándares.

NMS Network Management Station: Estación de manejo de red. Sistema responsable del manejo de al menos una parte de la red. Generalmente se trata de una computadora poderosa y bien equipada, como por ejemplo una estación de trabajo de ingeniería, con pantalla de color de alta resolución, gran cantidad de memoria y de espacio en disco y un procesador rápido. Las NMS se comunican con agentes para llevar el control de las estadísticas y recursos de la red.

NMVT Network Management Vector Transport: Transporte vectorial para manejo de red. Mensaje SNA compuesto de una serie de vectores con información específica sobre el manejo de la red.

NOC Network Operations Center: Centro de operaciones de red. Organización o sitio responsable del mantenimiento de una red.

node Nodo. Término genérico que se refiere a una entidad que puede tener acceso a una red. Se usa también el término device: dispositivo.

noise Ruido. Señales indeseadas en el canal de comunicaciones.

Northwest Net Red del noroeste. Red regional financiada por NSF que da servicio al noroeste de los Estados Unidos, Alaska, Montana y Dakota del Norte. Conecta todas las principales universidades de la región y muchas importantes industrias, tales como Boeing y Sequential Computer.

NOS Network Operating System: Sistema operativo de red. Término genérico para referirse a lo que en realidad son sistemas distribuidos de archivos. Ejemplos de esto incluyen NetWare, VINES de Banyan, NFS y LAN Manager.

NPDN Red pública de conmutación de circuitos a baja velocidad en los

países nórdicos.

null modem Modem nulo. Pequeña caja o cable usado para conectar dispositivos directamente más que mediante una red.

Numeris Red pública ISDN en Francia.

Nyquist Sampling Theorem Teorema de muestreo de Nyquist. Teorema demostrado por H. Nyquist que indica que es posible reconstruir señales analógicas a partir de muestras si se toman suficientes de ellas.

NYSER Net Red del Estado de Nueva York con una red fundamental (backbone) T1 que interconecta la NSF, muchas universidades y varios complejos comerciales.

object instance Instancia de objeto. Término de manejo de redes referente a una instancia de un tipo de objeto al que se ha asignado a un valor.

ODA Office Document Architecture: Arquitectura de documentos de oficina. Estándar OSI que especifica cómo transmitir documentos electrónicamente.

OIM OSI Internet Management: Manejo Internet OSI. Grupo de trabajo para la especificación de formas en que pueden usarse protocolos de manejo de red OSI en redes TCP/IP.

ONC Open Network Computing: Computación en redes abiertas. Arquitectura de aplicaciones distribuidas fundada por la empresa Sun Microsystems y actualmente controlada por un consorcio encabezado por Sun. Los protocolos NFS son parte de ONC.

open architecture Arquitectura abierta. Arquitectura para la cual terceros pueden desarrollar productos legalmente, y de la que existen especificaciones de dominio público.

open circuit Circuito abierto. Trayectoria cortada en un medio de transmisión. Normalmente impide la comunicación en la red.

optical fiber Fibra óptica. Véase fiber-optic cable.

OSI Open System Interconnection: Interconexión abierta de sistemas. Programa internacional de estandarización, apoyado por ISO y CCITT, para desarrollar estándares para redes de datos. Facilita la

interoperabilidad de equipos hechos por diversos fabricantes.

OSINET Asociación internacional diseñada para promover a OSI en arquitecturas de diversos fabricantes.

OSI Reference Model Modelo de referencia OSI. Modelo de arquitectura de redes desarrollado por ISO y CCITT. Consiste en siete capas, cada una de las cuales especifica funciones particulares de la red, tales como direccionamiento, control de flujo, control de errores, encapsulamiento, transferencia confiable de mensajes y muchas otras. La capa más alta (application layer: capa de aplicación) es la más cercana al usuario. La capa más baja (physical layer: capa física) es la más cercana a la tecnología del medio físico. El modelo de referencia OSI es universalmente usado como método de enseñar y entender la funcionalidad de las redes.

OSPF Open Shortest Path First: La trayectoria abierta más corta primero. Algoritmo de enrutamiento jerárquico IGP de estado de enlace propuesto como sucesor de RIP en la comunidad Internet. Sus características incluyen enrutamiento de costo mínimo, enrutamiento de camino múltiple y balanceo de cargas. Se deriva de una versión inicial del protocolo OSI IS-IS.

Outframe Outstanding frames: Marcos pendientes. Máximo número de marcos pendientes permitidos en un servidor SNA PU2 en algún momento.

out-of-band signaling Señalización fuera de banda. Transmisión que usa frecuencias o canales fuera de los empleados para transferencia de información. Suele usarse para reporte de errores en situaciones en las que la señalización dentro de banda puede ser afectada por los problemas que la red esté experimentado.

pacing Paso. Término empleado por IBM para el control de flujo. Véase flow control.

packet Paquete. Agrupamiento lógico de información que incluye un encabezado (header) y (normalmente) datos del usuario. Véase también frame, datagram, segment, message.

packet buffer Buffer de paquetes. Véase buffer.

packet switching Conmutación de paquetes. Red en la cual los nodos comparten el ancho de banda porque mandan unidades lógicas de información (packets) en forma intermitente. En contraste, una red de conmutación de circuitos (circuit switching) dedica un circuito a la vez para la transmisión de datos.

PACNET Red de paquetes de Nueva Zelanda.

PAD Packet Assembler/Disassembler.- Ensamblador/ desensamblador de paquetes. Dispositivo usado para conectar dispositivos simples (como por ejemplo, terminales que trabajan en modo de caracteres) que no tienen capacidad de ensamblar ni desensamblar paquetes, a redes X.25. El PAD sirve como buffer para datos enviados entre las máquinas anfitriones y las terminales en una red X.25, como se define en las recomendaciones CCITT X.3, X.28 y X-29.

PAM Pulse Amplitude Modulation: Amplitud modulada por pulsos. Esquema de modulación en el cual se hace que la onda moduladora module la amplitud de un tren de pulsos.

paquete Véase packet.

parallel transmission Transmisión paralela. Transmisión simultánea de todos los bits que forman un byte o un carácter. Véase también serial transmission: transmisión serie.

parity check Verificación de paridad. Proceso para verificar la integridad de un carácter. Consiste en añadir un bit que haga que el número total de bits binarios en '1' en un carácter o en una palabra (excluyendo al bit de paridad) sea impar (en "odd parity": paridad impar) o par (en "even parity": paridad par).

path control layer Capa de control de trayectoria. Capa 3 en el modelo arquitectónico SNA. Se trata de la capa SNA que enruta paquetes en una interconexión entre redes.

path control network Red de control de trayectorias. Concepto SNA consistente en componentes de menor nivel que controlan el enrutamiento y el flujo de datos a través de una red SNA, y que manejan la transmisión física de datos entre los nodos SNA. Contrasta con las NAU, que ofrecen servicios de más alto nivel.

PBX Private Branch Exchange: Conmutador privado. Conmutador telefónico en las instalaciones del usuario.

PCI Protocol Control Information: Información de control de protocolo. El equivalente OSI del término "header": encabezado. Es la información de control que se añade a los datos del usuario para formar un paquete OSI.

PCM Pulse Code Modulation: Modulación por código de pulsos. Transmisión de información analógica en forma digital mediante muestreo y codificación con un número fijo de bits.

PDN Public Data Network: Red pública de datos. Red operada por el gobierno (como en Europa) o en forma privada para ofrecer comunicaciones por computadora al público, normalmente cobrando una cuota. Las redes PDN permiten a las organizaciones pequeñas crear una red WAN sin todo el costo del equipo de circuitos de larga distancia.

PDS Premises Distribution System: Sistema de distribución en las instalaciones. Sistema de cableado desarrollado y distribuido por AT&T.

PDU Protocol Data Unit: Unidad de datos de protocolo. Término equivalente a packet (paquete), definido por OSI. Los dispositivos los intercambian dentro de un nivel específico del modelo de referencia OSI.

peer-to-peer computing Computación entre nodos similares o equivalentes. En contraste con la computación en modo cliente-servidor, la computación entre nodos equivalentes pide a cada dispositivo ejecutar ambas porciones, cliente y servidor, de una aplicación. Véase también client-server computing. La frase también puede emplearse para describir la comunicación entre implantaciones de la misma capa del modelo OSI en dos diferentes dispositivos de la red.

performance management Manejo del desempeño. Una de las cinco categorías de manejo de redes definidas por ISO para el manejo de las redes OSI. Los subsistemas de manejo del desempeño son responsables de analizar y controlar el desempeño de la red, incluyendo su capacidad y las tasas de error.

peripheral node Nodo periférico. En SNA, es un nodo que usa direcciones locales y por tanto no es afectado por cambios a las direcciones de la red. Los nodos periféricos requieren de la asistencia de funciones cercanas de un nodo de una subárea adyacente.

P/F Poll/Final bit: Solicitud de datos/Bit final. Protocolo sincrónico de bit en bit de la capa de enlace que indica la función de un frame o marco. Si el marco es una orden, un " 1 " en ese bit indica una solicitud de datos.

Si el marco es una respuesta, un " 1 " en este bit indica que el marco actual es el último de la respuesta.

phase Fase. Localización de la posición en una forma de onda alterna.

PHY Subcapa física FDDI. Designación de los cables de fibra óptica FDDI-physical address Dirección física. Término empleado algunas veces para referirse a la dirección de la capa de enlace (link-layer) de un dispositivo de la red. Contrasta con una dirección de red o de protocolo (network, protocol), que son direcciones de la capa de red.

physical control layer Capa física de control. Capa 1 en el modelo arquitectónico SNA. Véase physical layer.

physical layer Capa física. Capa 1 del modelo OSI. La capa física define las interfaces eléctricas, mecánicas y físicas a la red, así como los aspectos del medio de red.

Physical mediam Medio físico. Véase media.

PHYSNET Physics Network: Red de Física. Grupo de muchas redes DECnet de investigación en física, incluida HEPnet.

piggybacking Aprovechar el viaje. Transportar acuses de recibo (acknowledgments) con el paquete de datos para ahorrar ancho de banda de la red.

pila de protocolos Véase protocol stack

ping Silbido. Aviso de paquete Internet. Se refiere al mensaje de eco ICMP y a su contestación. Suele usarse para probar el grado de alcance de un dispositivo de la red.

ping ponging Frase usada para describir las acciones de un paquete en un ciclo (loop) de enrutamiento de dos nodos.

poison reverse updates Actualizaciones en reversa. Actualizaciones de enrutamiento que indican específicamente que una red o subred es inalcanzable, en lugar de simplemente implicarlo al no incluirla en las actualizaciones. Estas actualizaciones se envían para acabar con ciclos grandes de enrutamiento. Bajo el supuesto de que mayores métricas de enrutamiento normalmente indican la existencia de ciclos de enrutamiento (loops), los protocolos IGRP de Cisco envían actualizaciones en reversa si una métrica de enrutamiento se ha incrementado en un factor de 1. 1 o más.pollingSolicitud de datos

mediante encuestas. Método de acceso en el cual un dispositivo primario de la red averigua, en orden, si los secundarios tienen datos por transmitir. Las solicitudes, averiguaciones o encuestas suceden en forma de mensajes a cada secundario, lo cual les da el derecho de transmitir.

port Puerto. Interface en un dispositivo de interconexión de redes (como por ejemplo un enrutador). En terminología IP puerto también se usa para especificar el proceso de recepción de las capas superiores.

PPP Point-to-Point Protocol: Protocolo de punto a punto. Sucesor de SLIP, este protocolo ofrece conexiones de enrutador a enrutador y de anfitrión a red empleando circuitos sincrónicos y asincrónicos. Véase también SLIP.

presentation layer Capa de presentación. Capa 6 del modelo de referencia OSI. Esta

intercambiados entre dos entidades de la capa de aplicación.

presentation services layer Capa de presentación de servicios. Capa 6 del modelo arquitectónico SNA. Véase presentation layer.

PRI Primary Rate Interface: Interface de tasa primaria. Interfaz ISDN de acceso a la tasa primaria. Este acceso consiste en un único canal D de 64 Kbps más 23 (en el caso de 1.56 Mbps) ó 30 (en el caso de 2.048 Mbps) canales B para voz o datos.

primary station Estación primaria. En los protocolos sincrónicos por bits de la capa de enlace, tales como HDLC y SDLC, es la estación que controla las actividades de transmisión de los secundarios y efectúa otras funciones, tales como control de errores, mediante encuestas (polling) u otros medios. Los primarios envían órdenes a los secundarios y reciben las respuestas.

print server Servidor de impresoras. Sistema de computación en red que recibe, maneja y ejecuta (o envía para su ejecución) los pedidos de impresión de otros dispositivos de la red.

priority queuing Colas con prioridades. Característica de enrutamiento en la cual a los marcos de la cola de salida de la interface se les da prioridad basada en varias características, como el tamaño del paquete y el tipo de interface.

probe Protocolo de resolución de direcciones desarrollado por Hewlett-Packard.

propagation delay Tiempo de propagación. Tiempo requerido para que los datos en una red viajen desde el origen hasta el destino final.

protocolo Descripción formal de un conjunto de reglas y convenciones que gobiernan la forma en la que los dispositivos de una red intercambian información.

protocol address Dirección de protocolo. Véase network address.

protocol stack Pila de protocolos. Capas de software de protocolo relacionadas que juntas funcionan para realizar una arquitectura específica de comunicaciones. Los ejemplos incluyen AppleTalk, DECnet y muchos otros.

protocol translator Traductor de protocolos. Dispositivo o software de la red que convierte de un protocolo a otro similar. Por ejemplo, el CPT Cisco efectúa conversiones entre X.25, PAD y Telnet.

proxy Apoderad. Entidad que, por motivos de eficiencia, esencialmente ocupa el lugar de otra.

Proxy ARP Variación del protocolo ARP en el que un dispositivo de otro fabricante (por ejemplo, un enrutador) se hace pasar como un nodo final enviando al anfitrión que lo solicita una respuesta ARP a cargo de ese nodo final (que tal vez no sepa cómo usar el enrutador). Esto puede ahorrar costos al disminuir el uso del ancho de banda en recursos caros, tales como los enlaces WAN de baja velocidad.

PSN Packet Switch Node: Nodo de conmutador de paquetes. Conmutador de paquetes Internet. También se refiere a un nodo de conmutación en la arquitectura X.25. Usualmente, el PSN es un DCE (Data Communication Equipment: Equipo de comunicación de datos) que permite conexión a un DTE (Data Terminal Equipment: Equipo terminal de datos). Véase también X.25. El acrónimo también se usa comúnmente como expansión de "packet-switched network": red de paquetes conmutados.

PSTN Public Switched Telephone Network: Red pública telefónica conmutada. Se refiere a la red telefónica.

PU Physical Unit: Unidad física. Componente SNA que maneja los recursos físicos de un nodo, como lo pide un SSCP Existe un PU por nodo.

PU 2.1 Physical Unit 2. 1: Unidad física 2.1. Tipo de PU que se puede conectar directamente a otros nodos PU 2.1 .

puente Véase bridge.

PUP PARC Universal Protocol: Protocolo universal PARC. Protocolo desarrollado en el Centro de Investigaciones Xerox de Palo Alto, California, y que es similar a IP.

PVC Permanent Virtual Circuit: Circuito permanente virtual. En forma genérica se refiere a un circuito virtual establecido en forma permanente. Los PVC ahorran ancho de banda asociado con el establecimiento y eliminación del circuito en situaciones en donde ciertos circuitos virtuales deben existir todo el tiempo.

QOS Quality of Service: Calidad del servicio. Medida del desempeño de un sistema de transmisión que considera la calidad de la transmisión y la disponibilidad del servicio.

query Pregunta. Mensaje usado (usualmente en un protocolo de pregunta-respuesta) para preguntar el valor de alguna variable o serie de variables.

queue Cola. En forma genérica se refiere a una lista ordenada de elementos que esperan procesamiento. En enrutamiento indica un conjunto pendiente de paquetes que esperan ser enviados a una interface del enrutador.

queueing theory Teoría de colas. Principios científicos que gobiernan la formación o falta de formación de congestión en una red o en una interface.

RACE Programa europeo de investigación y desarrollo en comunicaciones avanzadas. Proyecto desarrollado por la comunidad europea para el desarrollo de capacidades de red de banda amplia.

RADIO AUSTRIA PSN austríaco.

RARE Reseaux Associes pour la Recherche Europeene: Asociación europea de universidades y centros de investigación diseñada para

promover una infraestructura de telecomunicaciones avanzada en la comunidad científica europea.

RARP Reverse Address Resolution Protocol: Protocolo inverso de resolución de direcciones. El inverso lógico de ARP, que ofrece un método de encontrar direcciones IP basado en direcciones del medio.

RBOC Regional Bell Operating Company: Compañía operadora regional Bell. Una de las siete compañías telefónicas creadas luego de la separación de AT&T en 1984. A veces también se conocen como Regional Bell Holding Companies. Véase también BOC.

reassembly Reensamble. La reconstitución de un datagrama IP en el destino luego de que se fragmentó en la fuente o en un nodo intermedio.

red Véase network.

redirect Redirigir. Parte de los protocolos ICMP y ES- IS que permite a un enrutador avisar a la máquina anfitriona que sería más efectivo usar otro enrutador.

redirector Redirector. Software que intercepta los pedidos de recursos en una computadora y analiza sus requerimientos de acceso remoto. Si hace falta acceso remoto para satisfacer el pedido, el redirector forma una RPC y la manda al protocolo de software de las capas inferiores para que se transmita en la red hasta el nodo que puede satisfacer el pedido.

redistribution Redistribución. El permitir que la información de enrutamiento descubierta mediante algún protocolo de enrutamiento sea distribuida en los mensajes de actualización de otro protocolo de enrutamiento.

redundancy Redundancia. En telefonía, es la parte de la información total contenida en un mensaje que se puede eliminar sin pérdida de información o significado esencial. En computación, son los elementos múltiples (redundantes) de un sistema que efectúan la misma función.

relay Relevador Terminología OSI para el dispositivo que conecta dos o más redes o sistemas de redes. Un relevador de la capa 2 es un puente. Un relevador de la capa 3 es un enrutador.

remote bridge Puente remoto. Puente que conecta segmentos físicamente diferentes de la red mediante enlaces WAN.

repeater Repetidor. Dispositivo que regenera y propaga señales eléctricas entre dos segmentos de la red.

Request/Response Unit Unidad de pedido/respuesta. Véase RU.

reverse channel Canal en reversa. Véase back channel.

RF Radio Frequency: Radiofrecuencia. Término generico que se refiere a las frecuencias que corresponden a las transmisiones de radio. La televisión por cable y las redes de banda amplia usan tecnología RF.

RFC Request For Comments: Solicitud de comentarios. Documentos empleados como el medio primario de comunicación de información sobre Internet. Algunos RFC son designados por IAB como "Estándares Internet. La mayoría documentan especificaciones de protocolos, como Telnet y FTP aunque algunos son en broma o de carácter histórico. Están disponibles a través de los Centros de Información de la Red Internet.

RG-58 Cable coaxial de 50 Ohms de impedancia. Es empleado por IOBASE2 de IEEE 802.3.

RG-62 Cable coaxial de 93 Ohms de impedancia. Es empleado por ARCnet.

RIF Routing Information Field. Campo de información de enrutamiento. Campo en el encabezado IEEE 802.5 que es empleado por un puente de ruta fuente (source-route bridge) para determinar el segmento de la red Token Ring por el que debe transitar un paquete. El RIF consiste en un número de anillo y de puente, además de otra información.

RIP Routing Information Protocol: Protocolo de información de enrutamiento. IGP proporcionado con los sistemas UNIX de Berkeley. Es el IGP más común en Internet.

ring group Grupo de anillo. Conjunto de interfaces Tóken Ring en uno o mas enrutadores Cisco, que son parte de una red Token Ring con puentes.

ring latency Espera en el anillo. Tiempo requerido para que una señal se propague una vez alrededor de un anillo en una red Token Ring o IEEE 802.5.

ring topology Topología de anillo. Topología en la que la red consiste en una serie de repetidores conectados entre si por enlaces de transmisión

unidireccional para formar un anillo cerrado único. Cada estación en la red se conecta con un repetidor.

RJ-11 Conectores estándar de 4 hilos para líneas telefónicas.

RJ-45 Conectores estándar de 8 hilos para redes 1BASE5 de IEEE 802.3 (StarLAN). También se usan como líneas de teléfono en algunos casos.

RJE Remote Job Entry: Entrada remota de trabajos. Acrónimo ideado por IBM que se refiere a una aplicación por lotes (batch) en lugar de a una de tipo interactivo. En los entornos RJE se someten los trabajos a la computadora y los resultados se reciben después.

rlogin Programa de emulación de terminales, similar a Telnet, que se ofrece en la mayoría de los sistemas UNIX.

ROSE Remote Operations Service Element: Elemento de servicio de operaciones remotas. Es el mecanismo RPC de OSI usado por varios protocolos de aplicación de red OSI. *routeRuta*. Trayectoria o camino a través de una interconexión de redes.

routed protocol Protocolo enrutado. Protocolo que puede ser enrutado por un enrutador. Para enrutarlo, el enrutador debe entender la interconexión lógica entre redes como la percibe el protocolo. Ejemplos de protocolos enrutados incluyen DECnet, Apple Talk e IP

route extension Extensión de ruta. En SNA, trayectoria del nodo de subárea de destino, a través del equipo periférico, a un NAU.

route processor Procesador de ruta. En la arquitectura de hardware Cisco, es una tarjeta de procesador que determina rutas y ejecuta procesos de configuración, seguridad, contabilidad, corrección de errores y manejo de red. También es llamado procesador supervisor. El equipo CSC/3 es un procesador de ruta.

router Enrutador. Dispositivo de la capa 3 OSI que puede decidir cuál de varios caminos debe seguir el tráfico de la red, basándose en alguna métrica óptima. También se conoce como gateway: servidor de intercomunicaciones (aunque esta definición de gateway ya casi no se usa). Los enrutadores envían paquetes de una red a otra, basados en la información de la capa de red.

routing Enrutamiento. Proceso de encontrar un camino hacia el anfitrión

de destino. En las grandes redes el enrutamiento es muy complejo debido a los muchos destinos intermedios potenciales que un paquete puede alcanzar antes de llegar a su anfitrión de destino.

routing bridge Puente enrutador. Puente de la capa MAC que usa métodos de la capa de red para determinar la topología de la red.

routing protocol Protocolo de enrutamiento. Protocolo que hace enrutamiento mediante la implantación de un algoritmo específico. Ejemplos de protocolos de enrutamiento son RIP, OSPF e IGRP

routing table Tabla de enrutamiento. Tabla almacenada en un enrutador o en algún otro dispositivo de las redes, que lleva cuenta de las rutas (y, en algunos casos, de su métrica) hacia destinos particulares en la red.

routing update Actualización de enrutamiento. Mensaje enviado desde un enrutador para indicar el grado de alcance de la red y la información de costos asociada. Las actualizaciones de enrutamiento suelen enviarse a intervalos regulares, y luego de un cambio en la topología de la red.

RPC Remote Procedure Call: Llamada remota a procedimiento. Es la base tecnológica de la computación distribuida (cliente-servidor). Son llamadas a procedimientos construidas o especificadas por los clientes y ejecutadas en los servidores, y los resultados se devuelven a los clientes mediante la red.

RS-232C Interface de capa física bastante popular. Es virtualmente idéntica a la especificación V24 .

RS-422 Realización eléctrica balanceada de RS-449 para transmisión de datos a alta velocidad.

RS-423 Realización eléctrica no balanceada de RS-449 para compatibilidad con RS-232C.

RS-449 Interface de capa física bastante popular. Se trata esencialmente de una versión más rápida (hasta 2 Mbps) de RS-232C con capacidad de manejar cables más largos.

RSRB Remote Source-Route Bridging: Punteo de rutas fuente remotas. Punteo de rutas fuente (source route bridging) sobre enlaces WAN. Los enrutadores Cisco, en la versión 9.0 de software, manejan RSRB.

RTMP Routing Table Maintenance Protocol: Protocolo de

mantenimiento de tablas de rutas. Protocolo de enrutamiento propio de las computadoras Apple. Es un derivado de RIP

RTS Request To Send: Petición de transmisión. Señal de control RS-232 que solicita transmisión de datos en una línea de comunicaciones.

RTT Round Trip Time: Tiempo de viaje redondo. Tiempo requerido para que una comunicación de la red viaje de la fuente al destino y de regreso. Incluye por tanto el tiempo requerido para que el destino procese el mensaje de la fuente y genere una respuesta. Algunos algoritmos de enrutamiento lo emplean como auxilio en el cálculo de las rutas óptimas.

RU Request/response Unit: Unidad de pedido/ respuesta. Mensajes SNA de pedido y respuesta intercambiados entre unidades NAU en una red SNA.

RUB Router Hub: Concentrador-enrutador. Producto que será desarrollado en forma conjunta por Cisco y SynOptics Communications y que combina las capacidades de un enrutador y de un concentrador.

sampling rate Tasa de muestreo. Tasa a la cual se toman muestras de la amplitud de alguna forma de onda en particular.

SAP Service Access Point: Punto de acceso al servicio. Interface entre capas OSI adyacentes. También se refiere a Service Advertisement Protocol: Protocolo de anuncio de servicios, un protocolo Novell mediante el cual se hacen conocidos a los clientes recursos de la red tales como servidores.

SAPONET-PPSN de Sudáfrica.

satellite communications Comunicaciones por satélite. Uso de satélites en órbita geoestacionaria para transmitir datos entre múltiples estaciones terrenas. Las comunicaciones por satélite ofrecen gran ancho de banda, costo no relacionado con la distancia entre las estaciones terrenas, retardos de propagación relativamente grandes, y capacidad de difusión (broadcast).

SO Serial-Port Communications Interface: Interface de puerto serie de comunicaciones. Tarjeta de interface de enrutador Cisco con conexiones tipo serie.

SDLC Synchronous Data Link Control: Control sincrónico de enlace de datos. Protocolo IBM sincrónico por bits de la capa de enlace que ha dado lugar a numerosos protocolos similares, incluyendo HDLC y

LAPB.

SDLC Transport Transporte SDLC. Característica de los enrutadores Cisco mediante la cual es posible integrar diferentes entornos en una sola red empresarial amplia de alta velocidad. Los enrutadores Cisco pueden hacer pasar el tráfico SDLC original a través de enlaces serie de punto a punto, y multiplexan el demás tráfico de protocolo sobre los mismos y enlaces. Esos enrutadores también pueden encapsular marcos SDLC dentro de datagramas IP para transportarlos a redes arbitrarias (que sean SDLC).

SDLLC Característica mediante la cual se realiza una traducción entre SDLC e IEEE 802.2 tipo 2.

secondary station Estación secundario. En protocolos de capa de enlace sincrónicos por bits, como HDLC, es una estación que responde a las ordenes de una estación primaria. Véase primary station.

security management Manejo de la seguridad. Una de las cinco categorías de manejo de redes definida por ISO para el manejo de redes OSI. Los subsistemas de manejo de la seguridad son responsables de controlar el acceso a los recursos de la red.

segment Segmento. Término usado en la especificación de TCP para describir una unidad de información de la capa de transporte.

serial transmission Transmisión serie. Método de transmisión en el cual los bits del carácter de datos se transmiten secuencialmente en un canal. Véase también parallel transmission.

server Servidor. Nodo o programa de software que ofrece servicios a un cliente. Véase también back end y client.

Service Advertisement Protocol Protocolo de anuncio de servicios. Véase SAP.

service point Punto de servicio. Interfaz NetCentral de NetView, capaz de enviar alertas de equipo desconocido para el entorno SNA.

servidor Véase server.

session Sesión. Conjunto de transacciones relacionadas que suceden entre dos o más dispositivos de la red. En SNA, es una conexión lógica

que permite a dos unidades NAU comunicarse entre sí.

session layer Capa de sesión. Capa 5 del modelo de referencia OSI. Coordina las actividades de la sesión entre aplicaciones, incluyendo control de errores del nivel de aplicación, control de diálogos y llamadas remotas a procedimientos.

shielded cable Cable blindado. Cable con una capa de aislamiento para reducir la interferencia electromagnética (EMI).

shortest- routing Enrutamiento de camino mínimo. Enrutamiento que mediante la aplicación de un algoritmo minimiza el costo de la distancia o de la trayectoria.

signaling Señalización. Proceso de enviar una señal de transmisión en un medio físico para propósitos de comunicación.

simplex transmission Transmisión simplex. Transmisión de datos en una sola dirección.

single mode-fiber Fibra de modo único. Fibra de diámetro relativamente angosto, a través de la cual sólo se propaga un modo. Tiene un ancho de banda mayor que la fibra multimodal, pero requiere una fuente de luz de espectro reducido (por ejemplo, un láser).

sistema autónomo Véase AS.

sliding window flow control Control de flujo de ventana móvil. Método de control de flujo en el que el receptor da al transmisor permiso de transmitir datos hasta que la ventana se llene. Cuando esto sucede, el transmisor debe detenerse hasta que el receptor anuncie una ventana mayor. TCP, otros protocolos de transporte y varios protocolos de la capa de enlace usan este método de control de flujo.

SLIP Serial Line IP: IP de línea serie. Protocolo Internet usado para ejecutar IP en líneas tipo serie, como las de los circuitos telefónicos.

slotted ring Anillo ranurado. Arquitectura LAN basada en una topología de anillo en donde éste se divide en ranuras que circulan continuamente.

Las ranuras pueden estar llenas o vacías, y las transmisiones deben comenzar al inicio de una ranura.

SMB ServerMessage Block: Bloque de mensajes de servidor. Protocolo de sistema de archivos usado en LAN Manager y similares para empaquetar datos e intercambiar información con otros sistemas.

SMDS Switched Multimegabit Data Service: Servicio de datos conmutados multimegabit. Tecnología WAN basada en datagramas y que emplea conmutación de paquetes a alta velocidad. Es ofrecida por las compañías telefónicas.

SMI Structure of Management Information: Información de estructura de manejo. Documento (RFC 1155) que especifica reglas usadas para definir manejo de objetos en la base MIB.

SMT Station Management: Manejo de la estación. Parte de la especificación FDDI que maneja estaciones en el anillo, como se define en la especificación X3T9.5.

SMTP Simple Mail Transfer Protocol: Protocolo sencillo de transferencia de correo. Protocolo Internet que ofrece servicios de correo electrónico.

SNA System Network Architecture: Arquitectura de redes de sistemas. Arquitectura grande, compleja y con múltiples características, desarrollada en la década de 1970 por IBM.

SNADS SNA Distribution Services: Servicios de distribución SNA. Junto con Document Interchange Architecture (DIA): Arquitectura de intercambio de documentos, y Distributed Data Management (DDM): Manejo de datos distribuidos, es una de las tres arquitecturas de servicios de transacción SNA. Ofrece distribución asincrónica de información entre usuarios finales.

SNAP Sub Network Access Protocol: Protocolo de acceso a subred. Protocolo Internet que opera entre una entidad de red en la subred y una entidad de red en el sistema final, y especifica un método estándar para encapsular datagramas IP y mensajes ARP en redes IEEE. La entidad SNAP en el sistema final hace uso de los servicios de la subred y efectúa tres funciones clave: transferencia de datos, manejo de conexiones y selección de la calidad del servicio.

SNI SNA Network Interconnection: Interconexión SNA de red. Servidor de intercomunicación (gateway) IBM que conecta múltiples redes SNA.

SNMP Simple Network Management Protocol: Protocolo simple de manejo de redes. El protocolo de manejo de redes Internet. Ofrece medios para seguir y determinar la configuración de la red y los parámetros al tiempo de ejecución.

socket Receptáculo. Estructura de software que opera como punto final de comunicaciones en un dispositivo de red.

SONET Synchronous Optical Network: Red óptica sincrónica. Red sincrónica de alta velocidad (hasta 2.5 Gbps) aprobada como estándar internacional en 1988. Las compañías regionales Bell (RBOC) pueden volverlo popular como el sistema de transmisiones de SMDS.

source address Dirección fuente. Dirección de un dispositivo de la red que hace envíos.

source-route bridging Puenteo de rutas fuente. Método de puenteo originado por IBM en el cual la ruta completa a un destino se predetermina en tiempo real antes del envío de datos al destino. Esto es en contraste con transparent bridging: puenteo transparente, en donde el puenteo ocurre trayecto (hop) por trayecto. También conocido por las siglas SRB, es más popular en las redes TÓken Ring.

source-route translational bridging Puenteo de rutas fuente con traducción. A veces conocido como SRITU, es un método de puenteo en el cual las estaciones de rutas fuente pueden comunicarse con estaciones de puente transparentes con el auxilio de un puente intermedio que traduce entre los dos protocolos de puenteo.

source-route transparent bridging Puenteo transparente de rutas fuente. Esquema de puenteo propuesto por IBM, que intenta reunir las dos estrategias prevaletientes de puenteo (transparente, y de rutas fuente). SRT, como a veces se le conoce, emplea ambas tecnologías en un mismo dispositivo para satisfacer las necesidades de todos los nodos finales. No se hace traducción entre los protocolos de puenteo, a diferencia de lo que sucede con source-route translational bridging (SR/TLB).

SPAN Space Physics Analysis Network: Red de análisis de física espacial. Red de comparación de datos para proyectos e instalaciones de la NASA, con extensiones a Japón, Canadá y muchos países europeos.

span Tramo. Línea de transmisión digital full duplex entre dos medios

digitales.

spanning tree Arbol abarcador. Subconjunto sin ciclos de la topología de una red.

spanning tree algorithm Algoritmo de árbol abarcador. Algoritmo, cuya versión original fue inventada por DEC, usado para impedir ciclos de puenteo mediante la creación de un árbol abarcador. Está documentado en la especificación IEEE 802. 1d, aunque en realidad el algoritmo de DEC y el algoritmo IEEE 802. 1d no son el mismo ni son compatibles.

speed matching Igualación de velocidades. Característica que ofrece capacidades suficientes de almacenamiento (buffer) en el dispositivo destino como para permitir que una fuente de alta velocidad transmita datos a su máxima capacidad, aun cuando el dispositivo de destino sea de menor velocidad.

split horizon updates Actualizaciones en el horizonte. Técnica de enrutamiento en la cual se impide que la información sobre las rutas salga de las interfaces del enrutador a través del cual fue recibido. Esto es útil para prevenir los ciclos de enrutamiento.

spooler Aplicación que maneja pedidos o trabajos que se le pasan para su atención. Los pedidos recibidos se procesan en forma ordenada a partir de una cola. El print spooler (sistema de colas de impresión) es tal vez el ejemplo más común. [N. del T. SPOOL es el acrónimo de Simultaneous Peripheral Operations On Line: Operación simultánea de periféricos en línea.

SQE Signal Quality Error. Error de calidad en la señal. Transmisión enviada por el transceiver (transmisor/receptor) de regreso al controlador para indicarle que los circuitos de colisiones están funcionales. También se conoce como heartbeat (latido). SRB Véase source-route bridging.

SRT Véase source-route transparent bridging.

SR/TLB Véase source-route translational bridging.

SSCP System Services Control Point: Punto de control de los servicios del sistema. Punto focal en una red SNA para el manejo de la configuración, que coordina al operador de la red y los pedidos de determinación de problemas, y que ofrece servicios de directorio y otros servicios de sesión para los usuarios finales de la red.

SSCP-PU session Sesión SSCP-PU. Sesión empleada por SNA para

permitir que un SSCP maneje los recursos de un nodo a través de la PU. Los SSCP pueden enviar pedidos y recibir respuestas de nodos individuales para controlar la configuración de la red.

standard Estándar. Conjunto de reglas o procedimientos comúnmente usados o especificados oficialmente. Véase también de facto standard, y de jure standard.

StarLAN Otro nombre para IBASE5 de IEEE 802.3. Es una red local LAN CSMA/CD promulgada por AT&T.

star topology Topología de red. Topología LAN en la cual los puntos finales de la red se conectan a un conmutador central mediante enlaces de punto a punto.

start-stop transmisión Transmisión de arranque-parada. Véase asynchronous transmission.

static route Ruta estática. Ruta que se ingresa manualmente en la tabla de rutas.

statistical multiplexer Multiplexor estadístico. Equipo de multiplexaje que dinámicamente asigna capacidades troncales tan sólo a los canales activos de entrada, permitiendo así la conexión de más dispositivos que con un multiplexor tradicional. También se conoce como statistical time division multiplexor o stat mux.

store and forward Almacena y envía. Técnica de conmutación de mensajes en la cual éstos se almacenan temporalmente en puntos intermedios entre la fuente y el destino, hasta que llegue el momento en que haya recursos de la red (como por ejemplo enlaces libres) disponibles para su envío.

STUN Serial Tunneling; Túneles serie. Abreviatura empleada por Cisco para la característica del enrutador que permite que dos dispositivos que funcionan con SDLC o HDLC se interconecten mediante alguna topología multiprotocolo arbitraria (empleando enrutadores Cisco), en vez de mediante un enlace serie directo. Esto ofrece al administrador de la red flexibilidad en la configuración.

subarea Subárea. Porción de una red SNA que consiste en un nodo de subárea enlaces y nodos periféricos asociados.

subarea node Nodo de subárea. Controlador de comunicaciones o

anfitrión SNA que maneja direcciones completas de la red.

subchannel Subcanal. En la terminología de banda amplia (broadband), es una subdivisión basada en la frecuencia, que crea un canal separado de comunicaciones.

subnet mask Máscara de subred. Máscara de direcciones de 32 bits usada en IP para especificar una subred en particular. Véase también address mask.

subnetwork Subred. Término empleado a veces para referirse a un segmento de la red. En redes IP es una red que comparte una dirección de subred particular. En redes OSI es un conjunto de ES e IS bajo el control de un dominio administrativo único, y que emplea un único protocolo de acceso a la red.

subvector Subvector. Segmento de datos de un vector en un mensaje SNA. Consiste en un campo de longitud, una llave que describe el tipo del subvector, y sus datos específicos.

SURAnet Southeastern Universities Research Association Network: Red de la asociación de investigación de las universidades del sureste [de los Estados Unidos]. Red que interconecta máquinas anfitriones en doce estados del sureste de los Estados Unidos.

SVC Switched Virtual Circuit: Circuito virtual conmutado. Circuito virtual que puede establecerse en forma dinámica por demanda. Se contrasta con PVC.

switch processor Procesador de conmutación. En la arquitectura de hardware Cisco, es una tarjeta de procesador de un bit (bit-slice) que actúa como administrador de todas las actividades del cBus. También se conoce como cBus controller.

synchronization Sincronización. El establecimiento de tiempos en común para el emisor y el receptor.

synchronous transmission Transmisión sincrónica. Operación de un sistema de red en donde los acontecimientos suceden en tiempos precisos.

T1 Terminología Bell que se refiere a un sistema de portadora digital usada para la transmisión de datos a través de la jerarquía telefónica. La velocidad de transmisión es de 1.544 Mbps.

T3 Servicio digital WAN que opera a 44 megabits por segundo.

TAC Terminal Access Controller: Controlador de acceso a las terminales. Anfitrión Internet que acepta conexiones terminales de líneas conmutadas.

TACACS Terminal Access Controller Access System: Sistema de acceso al controlador de acceso a las terminales. Sistema desarrollado por la comunidad de la red de datos de la defensa de los EEUU para controlar el acceso a sus TAC. Los productos Cisco lo manejan.

T-carrier Portadora-T. Método de transmisión de multiplexación por división de tiempo que usualmente se refiere a una línea o cable que lleva una señal DS-1.

T-connector Conector-T. Dispositivo en forma de T con dos conectores BNC hembra y uno macho.

TCP/IP Transmission Control Protocol/Internet Protocol: Protocolo de control de transmisiones/Protocolo Internet. Los dos protocolos Internet más conocidos, que erróneamente suelen confundirse con uno solo. TCP corresponde a la capa 4 (capa de transporte) del modelo de referencia OSI y ofrece transmisión confiable de datos. IP corresponde a la capa 3 (capa de red) del modelo de referencia OSI, y ofrece servicios de datagramas sin conexión. TCP/IP fue desarrollado por el Departamento de la Defensa de los Estados Unidos en los años 70 como apoyo a la construcción de interconexión de redes a escala mundial.

TCU Trunk Coupling Unit: Unidad de acoplamiento troncal. En redes Token Ring, es un dispositivo físico que conecta una estación al cable troncal.

TDM Time Division Multiplexing: Multiplexaje por división de tiempo. Técnica en la que puede asignarse ancho de banda a información de múltiples canales en un solo cable, basándose en distribución de intervalos de tiempo.

TDR Time Domain Reflectometer: Reflectómetro, en dominio de tiempo. Dispositivo capaz de enviar señales a través de un medio de red para verificar la continuidad del cable y otros atributos. Se emplean para

localizar problemas de la capa física de la red.

telecommunications Telecomunicaciones. Término referido a las comunicaciones (que normalmente involucran sistemas de cómputo) en la red telefónica.

TELENET PSN público importante en los Estados Unidos.

telex Télex. Servicio de telemecanografía que permite a los abonados enviar mensajes en la red telefónica pública (PSTN).

Telnet Protocolo estándar Internet de emulación de terminales.

termid También llamado Xid, es la identificación de un cluster controller (controlador de cúmulos) SNA. Sólo tiene sentido en líneas conmutadas.

terminal emulation Emulación de terminales. Aplicación usual de redes en la cual una computadora ejecuta programas que la hacen aparecer, ante una máquina anfitriona de la red, como si fuera una terminal simple conectada directamente.

terminal server Servidor de terminales. Procesador de comunicaciones que conecta dispositivos asincrónicos a una red LAN o WAN mediante software emulador de terminales y de redes.

terminator Terminador. Resistencia eléctrica al final de una línea de transmisión, que absorbe las señales, evitando así que reboten y sean oídas de nuevo por las estaciones de la red.

TFTP Trivial File Transfer Protocol: Protocolo trivial de transferencia de archivos. Versión simplificada de FTP que permite transferencia de archivos de una computadora a otra de la red. **THC over X.25** THC sobre X.25. Característica que ofrece compresión de encabezados TCP/IP en líneas X.25 para propósitos de eficiencia en los enlaces.

THEnet Texas Higher Education Network: Red de educación superior de Texas. Red regional compuesta de más de 60 instituciones académicas y de investigación del estado de Texas.

Thinnet Véase Cheapernet.

throughput Producción, trabajo útil. Cantidad de información que llega, y posiblemente pasa, a un punto en particular en un sistema de red.

time-out Suspensión por tiempo terminado. Acontecimiento que ocurre cuando un dispositivo de la red espera escuchar a otro dentro de un período especificado, pero eso no sucede. La suspensión resultante retransmisión de la información o bien la normalmente causa una disolución del circuito virtual entre los dos dispositivos.

TN3270 Software de emulación de terminales que hace que una terminal aparezca ante un anfitrión IBM como si fuera una terminal 3278, modelo. La realización TN3270 de Cisco permite al usuario el acceso a una máquina IBM sin tener que usar un servidor especial IBM o una máquina UNIX que actúe como servidor.

token Ficha. Marco (frame) de información de control cuya posesión da a un dispositivo de la red el derecho a transmitir.

token bus Arquitectura de red LAN que emplea acceso tipo token passing en una topología de bus. Esta arquitectura es la base de la especificación LAN IEEE 802.4.

token passing Paso de fichas. Método de acceso en el cual los dispositivos de la red tienen acceso al medio físico en un orden definido por la posesión de un pequeño marco (frame) llamado token (ficha). Véase también contention y circuit switching.

Token Ring Red LAN tipo token-passing desarrollada y manejada por IBM. Es muy similar a la red LAN IEEE 802.5.

TOP Technical Office Protocol: Protocolo técnico de oficina. Arquitectura para comunicaciones de oficina basada en OSI y desarrollada por la compañía Boeing.

topología de bus Véase bus topology.

TOS Type of Service: Tipo de servicio. Véase class of service.

TPO Transport Protocol Class 0: Protocolo de transporte de clase 0. Protocolo de transporte OSI sin conexiones para uso en subredes contables definidas por ISO 8073.

TP4 Transport Protocol Class 4: Protocolo de transporte de clase 4. Protocolo de transporte OSI con conexiones definido por ISO 8073.

trailer Elemento de la cola. Información de control añadida a los datos en un paquete.

transaction Transacción. Unidad de procesamiento de comunicaciones orientada hacia los resultados.

transaction services layer Capa de servicios de transacciones. Capa 7 en el modelo de arquitectura SNA. Véase application layer.

transceiver Transmisor/receptor. Véase MAU.

transceiver cable Cable Transmisor/receptor. Véase drop cable y AUI.

transit bridging Puenteo de tránsito. Puenteo que emplea encapsulamiento para enviar un marco (frame) entre dos redes similares, pasando por una red diferente.

translation bridging Puenteo con traducción. Puenteo entre redes con protocolos de subcapa MAC diferentes.

transmisión analógica Véase analog transmission

transmisión asincrónica Véase asynchronous transmission.

transmission control layer Capa de control de transmisiones. Capa 4 del modelo de arquitectura SNA. Es la responsable de establecer, mantener y terminar las sesiones SNA, de secuenciar los mensajes de datos, y del flujo de control de la sesión.

transmission group Grupo de transmisión. En enrutamiento SNA, es uno o más enlaces paralelos de comunicación que se tratan como una entidad de comunicaciones.

TRANSPAC Red importante de paquetes de datos francesa.

transparent bridging Puenteo transparente. Esquema de puenteo preferido por redes Ethernet y IEEE 802.3, en el cual los puentes pasan los marcos un trayecto (hop) a la vez, basados en tablas que asocian nodos terminales con puertos del puente. Se llama así porque la presencia de los puentes es transparente para los nodos terminales de la red.

transport layer Capa de transporte. Capa 4 del modelo de referencia OSI. Es la responsable de la comunicación confiable entre nodos terminales de la red. Realiza los controles de flujo y de errores y suele usar circuitos virtuales para asegurar entrega confiable de datos.

traps Trampas. Mensajes no solicitados enviados por un agente SNMP a un sistema de manejo de red (NMS) que indican la ocurrencia de un acontecimiento significativo.

tree topology Topología de árbol. Topología LAN similar a la de bus, excepto que las redes tipo árbol si pueden contener ramas. Como en la topología de bus, las transmisiones de una estación se propagan por todo el medio y son recibidas por todas las otras estaciones.

TRouter Producto de Cisco capaz de dar servicio de enrutador y de terminal.

trunk Troncal. Canal de transmisión que conecta dos dispositivos de conmutación.

twisted pair Par trenzado. Medio de transmisión de relativa baja velocidad que consiste en dos cables aislados, en forma de espiral. Los cables pueden o no estar blindados. Es muy común en aplicaciones de telefonía y cada vez más usual en redes de datos.

TYMNET PSN público importante en los Estados Unidos.

Type 1 operation Operación tipo 1. Operación sin conexiones IEEE 802.2 (LLC).

Type 2 operation Operación tipo 2. Operación con conexiones IEEE 802.2 (LLC).

type of service routing Enrutamiento de tipo de servicio. Esquema de enrutamiento en el cual se escoge una trayectoria en la interconexión de redes dependiendo de las características de las subredes involucradas y de los paquetes, además del camino -más corto al destino.

UDP User Datagram Protocol: Protocolo de datagrama de usuario. Protocolo sin conexión de la capa de transporte que pertenece a la familia de protocolos Internet.

ULP Upper Layer Protocol: Protocolo de nivel superior. Protocolo que

está más arriba en el modelo de referencia OSI que el punto actual de referencia. Suele usarse para referirse al siguiente protocolo más alto en una cierta pila de protocolos.

UltraNet Red de muy alta velocidad (1 25 Mbps) desarrollada y distribuida por Ultra Network Technologies.

unbalanced configuration Configuración desbalanceada. Configuración HDLC con una estación primaria y múltiples estaciones secundarias.

unicast address la red.

unipolar Unipolar. Literalmente significa una sola polaridad. Es la característica eléctrica fundamental de las señales internas en los equipos de comunicaciones digitales. En contraste con bipolar.

unity gain Ganancia unitaria. En redes de banda amplia (broadband), es el balance entre pérdida y ganancia de señal a través de los amplificadores.

UNMA Unified Network Management Architecture: Arquitectura unificada de manejo de redes. Arquitectura de manejo de redes de AT&T.

unnumbered frames Marcos sin numeración. Marcos HDLC usados para propósitos de mantenimiento, incluyendo el arranque y terminación de enlaces y la especificación de modos.

USENET Iniciada en 1979, es una de las redes cooperativas más antiguas y grandes, con más de 10,000 anfitriones y un cuarto de millón de usuarios. Su principal servicio es news, un servicio de conferencias distribuidas. **UUCP** UNIX-to-UNIX Copy Program. Programa de copias de UNIX a UNIX. Protocolo empleado para comunicaciones entre sistemas UNIX que cooperan. También se refiere a una red basada en UNIX, cercanamente asociada con USENET.

V.24 Interface de capa física comúnmente empleada en muchos países. Muy similar a EIA-232D y RS-232C.

vector Vector. Segmento de datos de un mensaje SNA. Está compuesto por un campo de longitud, una llave que describe el tipo de vector, y los datos específicos del vector.

VINES Virtual Network System: Sistema de red virtual. NOS

desarrollado y distribuido por Banyan Systems.

virtual circuit Circuito virtual. Circuito lógico formado para asegurar comunicación confiable entre dos dispositivos de la red.

virtual route Ruta virtual. Terminología SNA para circuito virtual. Es una conexión lógica entre dos nodos de subárea que se realiza físicamente o como una ruta explícita particular.

VTP Virtual Terminal Protocol: Protocolo de terminal virtual. Aplicación ISO para establecer una conexión de terminal virtual en una red.

WAN Wide-Area Network: Red de área amplia. Red que ocupa un área geográfica amplia. Véase también LAN y MAN.

wideband Banda amplia. Véase broadband.

wiring closet Cuarto de conexiones. Cuarto diseñado específicamente para el cableado de redes de voz y datos. Sirve como punto de unión para los cables y equipo que se usan para interconectar dispositivos.

WISNET Red TCP/IP en Wisconsin, E.E.U.U., que conecta 27 instalaciones de la Universidad de Wisconsin, además de varias instituciones privadas. Los enlaces son a 56 Kbps y T1.

X.21 Recomendación CCITT que define un protocolo de comunicaciones entre redes de circuitos conmutados y dispositivos de usuario.

X.25 Recomendación CCITT que define el formato de los paquetes para transferencias de datos en redes públicas de datos. Muchos establecimientos tienen redes X.25 que les dan acceso a terminales remotas. Esas redes se pueden usar para otros tipos de datos, incluyendo los protocolos Internet, DECnet y XNS.

X.28 Recomendación CCITT que define la interface terminal-PAD.

X.29 Recomendación CCITT que define la interface PAD-computadora.

X.3 Recomendación CCITT que define varios parámetros PAD.

X3T9.5 Número asignado al grupo de trabajo del comité de acreditación de estándares para su documento interno de trabajo que describe la interfaz de datos distribuida por fibra. Véase FDDI.

X.400 Recomendación CCITT que define y especifica un estándar para transferencias de correo electrónico.

X-500 Recomendación CCITT que define y especifica un estándar para el mantenimiento de archivos y directorios distribuidos.

Xid Véase *termid*.

XDMCP Protocolo de control de X Display Manager: Protocolo usado para comunicación entre terminales X y estaciones de trabajo que ejecutan UNIX.

XNS Xerox Network Systems: Sistemas de red Xerox. Grupo de protocolos originalmente diseñados por Xerox PARC. Muchas compañías de redes de PC, como Ungermann-Bass, Novell, Banyan y 3Com, usaban o actualmente usan variantes de XNS como pila de protocolos primarios de transporte.

XRemote Protocolo desarrollado específicamente para optimizar el manejo de X Windows en enlaces de comunicación serie.

X Windows Sistema gráfico y de ventanas distribuido, multitarea, independiente de los dispositivos, y transparente a la red, originalmente desarrollado por el MIT para comunicaciones entre terminales X y estaciones de trabajo UNIX.

Bibliografía

Gigabit Networking
Craig Partridge
Addison-Wesley
Mayo 1994

Networking Standars
William Stallings
Addison-Wesley
Enero 1994

ATM networks
Rainer Handel
Addison-Wesley
Second edition
Enero 1994

ATM Theory and application
David E. McDysan
McGraw Hill
Enero 1994

ATM & CELL RELAY SERVICES FOR
CORPORATE ENVIROMENTS
Daniel Minolli
McGraw Hill
Enero 1994

Intenetworking with TCP/IP
Volume I Principles, Protocols, and Architecture
Second edition
Douglas E. Comer
Prentice Hall
Marzo 1991

ATM
User-Network Interface especification Version 3.0
ATM Forum
Prentice Hall
Abril 1993
