UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

NUEVAS TECNOLOGÍAS APLICADAS AL DISEÑO DE REDES DE TELECOMUNICACIONES MODERNAS

T E S I S

QUE PARA OBTENER EL TÍTULO DE :

INGENIERO ELÉCTRICO ELECTRÓNICO

P R E S E N T A :

ISMAEL MANUEL JUÁREZ SÁNCHEZ

E

INGENIERO EN TELECOMUNICACIONES

P R E S E N T A N :

JUAN FRANCISCO CATALÁN ORTEGÓN

QUETZALCOATL LANDAVERDE VENEGAS

DIRECTOR DE TESIS: ING. ISAAC MENDOZA GÓMEZ

CIUDAD UNIVERSITARIA NOVIEMBRE 2004

INTRODUCCIÓN

El desarrollo tecnológico que se ha presentado durante las últimas décadas ha sido sumamente sorprendente, ya que a finales del siglo pasado y a principios de este, la tecnología ha logrado avanzar de manera vertiginosa en comparación con los anteriores.

En nuestros días, una de las áreas en donde se ha reflejado esta modernización tecnológica han sido las telecomunicaciones, las cuales se encuentran en una acelerada evolución, esto ha generado que los sistemas de telecomunicaciones modernos hayan alcanzado cierto nivel de inteligencia, lo cual ha producido que sean mas confiables, eficientes y mas accesibles.

Las redes modernas de telecomunicaciones así mismo, son de gran importancia en nuestros días, ya que gracias a ellas se ha logrado aumentar la productividad y disminuir los costos de producción de una gran cantidad de negocios; los adelantos tecnológicos han sido un factor decisivo para apoyar las actividades industriales, comerciales y financieras, por lo que ocupan un lugar preponderante en el desarrollo de las naciones.

El objetivo de esta tesis es el de presentar un panorama general del estado actual de las redes de telecomunicaciones, haciendo un énfasis en las ultimas tecnologías que se han desarrollado en este campo, teniendo como idea fundamental el estudio de las telecomunicaciones modernas desde un punto de vista práctico, tratando de aportar un diseño con el cual se maximice el rendimiento de las redes de datos a un menor costo y generando una mayor productividad.

La primera parte de la tesis (Capitulo 1), describe los elementos fundamentales de las redes de telecomunicaciones, como lo son la definición de una red, tipos de redes, topologías, importancia de las redes en la actualidad, describe una a una las siete capas que conforman el modelo OSI etc., que son los conocimientos básicos necesarios con los cuales se realizará un estudio más avanzado en la segunda parte (Capitulo 2), en la cual se describe mas detalladamente las cuatro primeras capas del modelo OSI, mencionando en cada capa las tecnologías actuales de las redes de datos así como sus principales características.

El Capitulo 3, se dedica al estudio de las técnicas utilizadas en las redes de alta disponibilidad, en esta parte se destacan las principales ecuaciones y características para lograr que una red este casi al 100% de disponibilidad, con lo cual se puede asegurar que dichas redes van a dar un servicio eficiente a la gente antes de que se empiece la construcción de estas, y por otra parte se asegura que los usuarios puedan utilizar en cualquier momento los beneficios y recursos que dichas redes ofrecen.

Como se menciono al principio la tecnología ha ido avanzando a pasos agigantados debido a las necesidades que surgen en los diferentes sectores de la sociedad, los cuales conforme pasa el tiempo exigen mayores tasas de transmisión a mayores velocidades pero a costos moderados, así como un sinnúmero de aplicaciones necesarias para su funcionamiento, en el Capitulo 4 se describen dichas necesidades y las razones por las cuales es necesario implementar nuevas tecnologías las cuales solucionaran dichos problemas. Descritas las necesidades, en el Capitulo 5 se dan a conocer las nuevas tecnologías existentes para las redes de datos y se da una descripción detallada de su funcionamiento y aplicación, las cuales solucionan muchas de las necesidades antes descritas.

Finalmente en el Capitulo 6 en base a toda la información recabada a lo largo de la tesis y a la necesidad de redes mas eficaces y robustas, se da una propuesta de una red de telecomunicaciones moderna en la cual se implementan las nuevas tecnologías existentes, y se hace una comparación con una red actual tanto tecnológica como económicamente.

El carácter introductorio, el contenido, así como la forma con la que se presentan los temas, hacen que la tesis sea útil para todas aquellas personas que tengan el deseo de tener un panorama general acerca de las redes de telecomunicaciones modernas, y así conseguir mejores y mayores recursos en lo respectivo a la planeación, administración y operación de redes de telecomunicaciones.

ÍNDICE

INTRODUCCIÓN IX

CAPITULO I FUNDAMENTOS DE REDES DE DATOS

I.1 LAS REDES Y SUS ORÍGENES 1
I.2 OBJETIVO DE LAS REDES 4
I.3 REDES DE TELECOMUNICACIONES 4
I.3.1 PROTOCOLOS 6
I.4 ELEMENTOS DE UNA RED 6
I.4.1 CANALES 6
I.4.2 NODOS 10
I.5 CLASIFICACIÓN DE LAS REDES 12
I.5.1 REDES CONMUTADAS 12
I.5.2 REDES DE DIFUSIÓN 17
I.6 TOPOLOGÍAS DE UNA RED 19

I.6.1 CONCEPTOS BÁSICOS 19
I.6.2 TOPOLOGÍA FÍSICA 20
I.6.3 TOPOLOGÍA LÓGICA 25
I.7 INTERCONEXIÓN DE REDES 27
I.8 JERARQUÍAS DE LA RED 29
I.8.1 PAN 30
I.8.2 LAN 31
I.8.3 MAN 32
I.8.4 WAN 34
I.8.5 INTERNET 38
I.9 MODELO OSI 39
I.9.1 CARACTERÍSTICAS 39
I.9.2 PROTOCOLOS 40
I.9.3 MODELO OSI Y COMUNICACIÓN ENTRE SISTEMAS 41
I.9.4 INTERACCIÓN ENTRE LAS CAPAS DEL MODELO OSI 42
I.9.5 SERVICIOS DE CAPA 42
I.9.6 CAPAS DEL MODELO OSI E INTERCAMBIO DE INFORMACIÓN 43
I.9.7 PROCESO DE INTERCAMBIO DE INFORMACIÓN 45
I.9.8 CAPA1: FÍSICA 45
I.9.9 CAPA2: ENLACE 46
I.9.10 CAPA3: RED 48
I.9.11 CAPA4: TRANSPORTE 48
I.9.12 CAPA5: SESIÓN 49
I.9.13 CAPA6: PRESENTACIÓN 49
I.9.14 CAPA7: APLICACIÓN 50
I.9.15 FORMATOS DE APLICACIÓN 51

CAPITULO II TECNOLOGÍAS ACTUALES DE UNA RED DE DATOS

II.1 CAPA FISICA 55
II.1.1 SEÑALES ELÉCTRICAS 55
II.1.2 CAPACIDAD DE CANAL Y SISTEMAS DE COMUNICACIÓN IDEALES 59
II.1.3 TECNOLOGÍAS DE COBRE 60
II.1.4 TECNOLOGÍAS DE FIBRA ÓPTICA 89
II.1.5 TECNOLOGÍAS DE MEDIOS INALÁMBRICOS 106
II.2 CAPA 2: ENLACE 131
II.2.1 TÉCNICAS DE ACCESO AL MEDIO 131
II.3 CAPA 3 : RED 156
II.3.1 IP 156
II.3.2 IPX 162
II.3.2 APPLE TALK 163

II.4 CAPA 4 : TRANSPORTE 165
II.4.1 DATAGRAMAS 165
II.4.2 TCP 169
II.4.3 UDP 173

CAPITULO III REDES DE ALTA DISPONIBILIDAD

III.1 INTRODUCCIÓN A LAS REDES DE ALTA DISPONIBILIDAD 180
III.1.1 POR QUE NECESITAMOS LA ALTA DISPONIBILIDAD 180
III.1.2 MAYOR CONFIABILIDAD DE REDES EN LA ACTUALIDAD 181
III.1.3 COSTOS REALES POR LOS DESPERFECTOS DE REDES 181
III.1.4 PRESENTANDO Y DESCRIBIENDO LOS MÉTODOS DE ALTA DISPONIBILIDAD 182
III.1.5 EL MÉTODO DEL PORCENTAJE 182
III.1.6 EL MÉTODO DE DEFECTOS POR MILLÓN 186
III.1.7 MTBF, MTTR Y DISPONIBILIDAD 186
III.1.8 RELACIONANDO EL PORCENTAJE Y MÉTODOS DE DPM 187
III.1.9 ANALIZANDO EL TIEMPO PERDIDO EN LOS PASOS DE LA RED 187
III.2 MATEMÁTICAS BÁSICAS DE LA ALTA DISPONIBILIDAD 188
III.2.1 DETERMINANDO LA DISPONIBILIDAD DE LOS DISPOSITIVOS 189
III.2.2 DETERMINANDO LA DISPONIBILIDAD DE UN SOLO COMPONENTE 190
III.2.3 DETERMINANDO LA DISPONIBILIDAD DE COMPONENTES MÚLTIPLES 191
III.2.4 DETERMINANDO EL FLUJO DE DATOS EN UNA RED: ANÁLISIS DEL CAMINO 195
III.3 TOPOLOGÍAS FUNDAMENTALES DE RED 197
III.3.1 TOPOLOGÍA SERIE 198
III.3.1 TOPOLOGÍA PARALELA 198
III.3.3 TOPOLOGÍA SERIE/PARALELO 199
III.4 PREDICIENDO LA DISPONIBILIDAD 200
III.4.1 FACTORES QUE AFECTAN LA DISPONIBILIDAD 201
III.4.2 COMO DISEÑAR UNA RED CONFIABLE 203
III.4.3 HARDWARE 204
III.4.4 EVENTOS DINÁMICOS 205
III.4.5 INSTALACIONES 206
III.4.6 EN EL DISEÑO DE RED, SIMPLE SIGNIFICA CONFIABLE 207
III.4.7 VERIFICACIÓN DEL PRODUCTO 208
III.4.8 RECUPERACIÓN DE ERRORES 209
III.4.9 INSTALACIÓN Y CONFIGURACIÓN DE UNA RED CONFIABLE 210
III.4.10 SEGURIDAD DE RED 210
III.4.11 MANTENIMIENTO Y OPERACIONES PROGRESIVAS

"El mayor riesgo de la Confiabilidad" 211
III.4.12 Errores humanos y procesos de administración y mantenimiento 212
III.4.13 El algoritmo para mejora la Disponibilidad de red 215
III.5 Prediciendo Punto a Punto la Disponibilidad de la Red , el Método de "Divide y Vencerás" 219
III.5.1 Pasos de método Divide y Vencerás 219

Capitulo IV NECESIDADES DE MAYORES TASAS DE TRANSMISIÓN Y LIMITACIONES ACTUALES DE UN SISTEMA DE TELECOMUNICACIONES

IV.1 Sistemas Multimedia 223
IV.1.1 Redes Multimedia 224
IV.1.2 Requerimientos en Comunicaciones Multimedia 225
IV.1.3 Voz IP 226
IV.1.4 Banda Ancha 227
IV.1.5 Limitantes 229

Capitulo V NUEVAS TECNOLOGÍAS EN SISTEMAS DE TRANSMISIÓN DE INFORMACIÓN

V.1 IPv6 233
V.1.1 Descripción de Paquete de Encabezado 235
V.1.2 Hexadecimal "Hex" 235
V.1.3 La Autenticación y Capacidades de Retiro 236
V.1.4 Las capacidades de QoS 236
V.1.5 Extensiones de IPv6 236
V.1.6 Descripción e Direccionamiento 237
V.1.7 Métodos de Broadcasting 237
V.1.8 IPv6 en México 239
V.2 MPLS 242
V.2.1 Utilizando Multiprotocolo de Conmutación de Etiquetas para entrega de Servicios IP 242
V.2.2 El concepto de utilizar etiquetas como envio de información 243
V.2.3 Definición de Términos utilizados por MPLS 244
V.2.4 Arquitectura de MPLS 244
V.2.5 Aplicaciones Basadas en MPLS 245

V.3 PWE3 247
V.3.1 FUNCIONES ESPECÍFICAS 248
V.3.2 ARQUITECTURA DE LA RED ACTUAL 248
V.3.3 PWE3 COMO UN CMINO A LA CONVERGENCIA 249
V.3.4 APLICACIONES ADAPTABLES PARA PWE3 250
V.3.5 REFERENCIA DEL MODELO E PWE3 250
V.3.6 PROCESAMIENTO DEL PAQUETE 251
V.3.7 CONSIDERACIONES EXTRAS 254
V.3.8 RESUMEN 254
V.4 OFDM 254
V.4.1 DESCRIPCIÓN DE OFDM 257
V.4.2 MODULACIÓN OFDM 259
V.4.3 OPERACIÓN DE CANAL PARA OFDM 261
V.5 VPNS (REDES PRIVADAS VIRTUALES) 261
V.5.1 INTRODUCCIÓN 261
V.5.2 PORQUE UTILIZAR UNA VPN 261
V.5.3 QUE ES UNA VPN 262
V.5.4 TECNOLOGÍA DE TUNEL 263
V.5.5 REQUERIMIENTOS BÁSICOS DE UNA VPN 264
V.5.6 COMPONENTES DE UNA VPN 265
V.5.7 VENTAJAS DE UNA VPN 265
V.5.8 CONCLUSIÓN 265

CAPITULO VI DISEÑO Y PROPUESTA DE IMPLANTACIÓN DE UNA RED DE TELECOMUNICACIONES MODERNA

VI.1 ANÁLISIS DE RED CONVENCIONAL 268
VI.1.1 SITIO LOCAL 269
VI.1.1.1 ELEMENTOS DE CORE 270
VI.1.1.2 DISTRIBUCIÓN 270
VI.1.1.3 ACCESO 271
VI.1.2 SITIO REMOTO 1 272
VI.1.3 SITIO REMOTO2 272
VI.2 ANÁLISIS DE RED PROPUESTA 273
VI.2.1 SITIO LOCAL 275
VI.2.1.1 ELEMENTOS DE CORE 275
VI.2.1.2 DISTRIBUCIÓN 276
VI.2.1.3 ACCESO 277
VI.2.1.4 VOZ SOBRE IP 277
VI.2.1.5 VPN´S 278
VI.2.2 SITIO REMOTO 1 279

VI.2.3 SITIO REMOTO 2 279
VI.3 DISPONIBILIDAD RED FRAME RELAY 280
VI.3.1 DETERMINAR ESENARIOS Y RBD 280
VI.3.2 CALCULAR LA DISPONIBILIDAD DE LOS COMPONENTES DE RED 281
VI.3.3 CÁLCULOS DE REDUNDANCIA DE CADA ESCENARIO 281
VI.3.4 CÁLCULOS DE DISPONIBILIDAD PUNTO A PUNTO PARA CADA ESCENARIO 282
VI.4 DISPONIBILIDAD RED MPLS 283
VI.4.1 DETERMINAR ESENARIOS Y RBD 283
VI.4.2 CALCULAR LA DISPONIBILIDAD DE LOS COMPONENTES DE RED 283
VI.4.3 CÁLCULOS DE REDUNDANCIA DE CADA ESCENARIO 285
VI.4.4 CÁLCULOS DE DISPONIBILIDAD PUNTO A PUNTO PARA CADA ESCENARIO 285
VI.5 CONSIDERACIONES EXTRAS 286
VI.6 VENTAJAS EXTRAS DE MPLS 287
VI.7 COMPARACIÓN DE GASTOS DE LA RED FRAME RELAY Y MPLS 288

CONCLUSIONES 291

ANEXO 295

INDEX 331

BIBLIOGRAFÍA 337

I

FUNDAMENTOS DE REDES DE DATOS

I.1 LAS REDES Y SUS ORIGENES

Cada uno de los tres siglos pasados ha estado dominado por una sola tecnología: el siglo XVIII fue la etapa de los grandes sistemas mecánicos que acompañaron a la Revolución Industrial, el siglo XIX fue la época de la máquina de vapor y durante el siglo XX y principios del siglo XXI, la tecnología clave ha sido la recolección, procesamiento y distribución de información, de los cuales, hemos presenciado la instalación de redes telefónicas en todo el mundo, la invención de la radio y la televisión, el nacimiento y crecimiento sin precedente de la industria de las computadoras, así como la puesta en orbita de los satélites de comunicación.

A medida que avanzamos en el presente siglo, se ha dado una rápida convergencia de estas áreas, por lo que las diferencias entre la captura, transporte, almacenamiento y procesamiento de información están convergiendo con rapidez. Organizaciones con centenares de oficinas dispersas en una amplia área geográfica,

esperan tener la posibilidad de examinar en forma habitual el estado actual de todas ellas, a través de una sola computadora. A medida que crece nuestra habilidad para recolectar y distribuir información, la demanda de más sofisticados métodos de procesamiento de información crece todavía con mayor rapidez.

La industria de las computadoras ha mostrado un progreso espectacular en muy corto tiempo. El solo tener una sola computadora para satisfacer todas las necesidades de procesamiento y análisis de información de una organización se ha reemplazando por otro que considera un número grande de computadoras físicamente separadas, pero interconectadas que efectúan el mismo o inclusive mayor trabajo de una manera más rápida y eficiente. Estos sistemas, se conocen con el nombre de redes de computadoras, estas, nos dan a entender una colección interconectada de computadoras autónomas y se dice que las computadoras están interconectadas, si son capaces de intercambiar información, esta conexión no necesita hacerse a través de un hilo de cobre, sino puede hacerse mediante el uso del fibra óptica, láser, microondas y/ó satélites de comunicaciones.

Los orígenes de las redes de computadoras se remontan a los primeros sistemas de tiempo compartido, al principio de los años sesenta, cuando una computadora era un recurso caro y escaso.

Puesto que muchas tareas requieren sólo una pequeña fracción de la capacidad de una gran computadora, se sacará mayor rendimiento de ésta, si presta servicios a más de un usuario al mismo tiempo.

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

Con base a estas inquietudes surgieron redes de datos públicos como Tymnet[1] y Telenet[2]. Las redes de las grandes corporaciones (Xerox, General Motors, IBM, Digital Equipment Corporation, AT&T y Burroughs), y las redes de investigación (SERCnet y NPL, inglesas de 1966-1968; HMI-NET de Berlín 1974; CYCLADES, Francia 1972), las redes comerciales, los sistemas de conferencia y las comunidades virtuales (especialmente USENET y FIDOnet).

A medida que las redes de computadoras fueron captando más adeptos, compañías tales como XEROX e IBM comenzaron a desarrollar su propia tecnología en redes de computadoras, comenzando por lo general, con redes de área

[1] Tymnet: Red pública de datos
[2] Telnet: Red pública conmutada de datos que usa los protocolos CCITT y X.25

local. Las redes de amplio alcance entonces, pasaron a ser usadas no solo para la comunicación entre computadoras conectadas directamente sino también para comunicar las redes de área local.

Con el establecimiento de ARPAnet, en E.U (1968), comenzó a entreverse el impacto social de la telemática, la tecnología de ARPAnet fue utilizada para construir en 1976, la red comercial Telenet.

En 1987 la red ARPAnet (dependiente del Departamento de Defensa Norteamericano) utilizada al principio, exclusivamente para la investigación y desbordada por el interés demostrado por sus usuarios por el correo electrónico, necesitó transmitir datos que usaban gran espectro de banda (sonidos, imágenes y videos) y sufrió tal congestión que tuvo que declarar obsoletas sus redes de transmisión de 56000 baudios por segundo. Posteriormente, una vez que quedo demostrada la viabilidad de las redes de paquetes conmutados de alta velocidad, estas se convirtieron en la espina dorsal de las telecomunicaciones en E.U. bajo su forma actual de INTERNET.

Los servicios comerciales que concentraron una gran cantidad de bases de datos como DIALOG, empezaron alrededor de 1972, los sistemas de conferencia computarizada comenzaron en 1976 y posteriormente encontraron viabilidad comercial en servicios centralizados como Delphi así como en sistemas algo mas distribuidos como Compuserve[1].

Mientras tanto, se fue desarrollando otra tecnología basada en conexiones por líneas telefónicas en lugar de conexiones dedicadas; dos de los primeros productos de esta tecnología fueron ACSNET y UUCP[2], que sobreviven en una forma modificada. Las redes a través de líneas telefónicas produjeron el más distribuido de los sistemas de conferencia: USENET[3], también BITNET[4] puso a disposición de la comunidad académica la tecnología en redes de computadoras de IBM y lo difundió aun entre computadoras de otras marcas.

Los servicios prestados por las redes de computadoras se han difundido ampliamente y alcanzan ya a la mayoría en las naciones, a medida que su diversidad continua en aumento, la mayoría de las redes académicas, se conectan entre si, por lo menos con el propósito de intercambiar correo electrónico.

Por ultimo la comunicación mediante computadoras es una tecnología que facilita el acceso a la información científica y técnica a partir de recursos

[1] Compuserve: Prestador de servicios de información en línea
[2] UUCP: Programa de Copia de Unix a Unix (*Unix to Unix Copy*)
[3] USENET: Es una de las primeres redes cooperativas más antiguas e importantes.
[4] BITNET: Red de bajo costo y baja velocidad con líneas dedicadas de 9600 bps

informáticos y de telecomunicaciones, por eso, se dice que una red es fundamentalmente, una forma de trabajo en común, en la que son esenciales tanto la colaboración de cada miembro en tareas concretas, como un buen nivel de comunicación que permita que la información circule con fluidez y que pueda llevarse a cabo el intercambio de recursos.

I.2 OBJETIVO DE LAS REDES

Las redes en general, consisten en "compartir recursos", y uno de sus objetivos es hacer que programas, datos y equipo puedan estar disponibles para los usuarios de la red que así lo requiera, sin importar la localización física del recurso y del usuario.

Un segundo objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro, por ejemplo todos los archivos podrían duplicarse en dos o tres máquinas, de tal manera que si una de ellas no se encuentra disponible, podría utilizarse una de las otras copias, además, la presencia de múltiples computadoras significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque se tenga un rendimiento global menor.

Otro objetivo es el ahorro económico, las computadoras pequeñas tienen una mejor relación costo/rendimiento comparada con la ofrecida por las máquinas grandes; estas son a grandes rasgos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es varias veces mayor. Este desequilibrio ha ocasionado que muchos diseñadores de sistemas construyan sistemas compuestos por poderosas computadoras personales, uno por usuario, con los datos guardados una o más máquinas que funcionan como servidor de archivos compartidos.

Otro objetivo del establecimiento de una red de computadoras, es que puede proporcionar un poderoso medio de comunicación entre personas que se encuentran muy alejadas entre si; con la infraestructura de una red es relativamente fácil para dos o mas personas que viven en lugares separados, escribir informes juntos. Esta rapidez hace que la cooperación entre grupos de individuos que se encuentran alejados, (y que anteriormente era difícil establecer), pueda realizarse hoy en día con relativa facilidad.

I.3 REDES DE TELECOMUNICACIONES

Un sistema de telecomunicaciones consiste en una infraestructura física a través de la cual se transporta la información desde la fuente hasta el destino, y con base en

esa infraestructura se ofrecen a los usuarios los diversos servicios de telecomunicaciones, en general se denomina ***Red de Telecomunicaciones*** a la infraestructura encargada del transporte de la información. Para recibir un servicio de telecomunicaciones, un usuario utiliza un equipo terminal a través del cual obtiene entrada a la red por medio de un canal de acceso. Cada servicio de telecomunicaciones tiene distintas características, puede utilizar diferentes redes de transporte y, por tanto, el usuario requiere de distintos equipos terminales. Por ejemplo, para tener acceso a la red telefónica, el equipo terminal requerido consiste en un aparato telefónico; para recibir el servicio de telefonía celular, el equipo terminal consiste en teléfonos portátiles con receptor y transmisor de radio, etcétera.

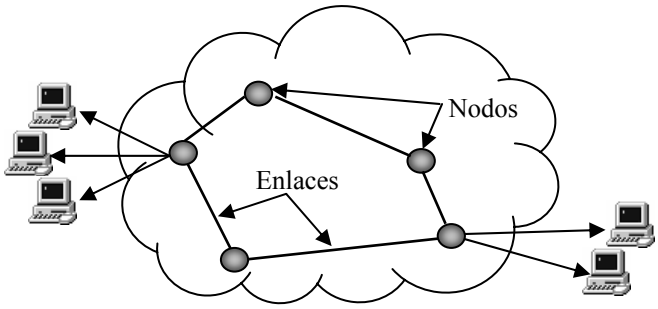


Figura I.1 *Red y equipo*

Para fines ilustrativos, se puede establecer una analogía entre las telecomunicaciones y los transportes: en los transportes, la red está constituida por el conjunto de carreteras de un país y lo que en ellas circulan son vehículos, que a su vez dan servicio de transporte a personas y/ó mercancías y en las telecomunicaciones, se transporta información a través de redes de transporte de información.

La principal razón por la cual se han desarrollado las redes de telecomunicaciones es que el costo de establecer un enlace dedicado entre cualesquiera dos usuarios de una red sería elevadísimo, sobre todo considerando que no todo el tiempo todos los usuarios se comunican entre sí. Es mucho mejor contar con una conexión dedicada para que cada usuario tenga acceso a la red a través de su equipo terminal, pero una vez dentro de la red los mensajes utilizan enlaces que son compartidos con otras comunicaciones de otros usuarios.

Comparando nuevamente con los transportes, a todas las casas llega una calle en la que puede circular un automóvil y a su vez conducirlo a una carretera, pero no todas las casas están ubicadas en una carretera dedicada a darle servicio exclusivamente a un solo vehículo, las calles desempeñan el papel de los canales de acceso y las carreteras el de los canales compartidos.

I.3.1 PROTOCOLO

Un protocolo es la descripción general de un conjunto de reglas y convenciones que rigen la forma en que los dispositivos de una red intercambian información.

I.4 ELEMENTOS DE UNA RED DE TELECOMUNICACIONES

En general se puede afirmar que una red de telecomunicaciones está formado por los siguientes componentes: *a)* un conjunto de nodos en los cuales se procesa la información, y *b)* un conjunto de enlaces o canales que conectan los nodos entre sí y a través de los cuales se envía la información desde y hacia los nodos.

I.4.1 CANALES

El canal es el medio físico a través del cual viaja la información de un nodo a otro, las características de un canal son de fundamental importancia para una comunicación efectiva, ya que de ellas depende en gran medida la calidad de las señales recibidas en el destino o en los nodos intermedios dentro de una ruta. Los canales se pueden clasificar en dos grupos:

1) Medios cableados; son aquellos que guían las señales las cuales contienen información desde la fuente hasta el destino, por ejemplo: Cables o par trenzado cables coaxiales y fibras ópticas. Debido a estas características, cada uno de estos tipos de canales son capaces de transmitir las siguientes tasas de información digital:

Cables o par trenzado	1000 Mbps (1000 millones de bits por segundo)
Cable coaxial	500 Mbps (500 millones de bits por segundo)
Fibra óptica	2 Tbps (2 "Tera" bps) aprox.

Tabla I.1 *Canales alámbricos*

Los cables de cobre son el medio más utilizado en transmisiones tanto analógicas como digitales; siguen siendo la base de las redes telefónicas urbanas, el material del que están formados produce atenuación en las señales, de manera tal que a distancias de entre 2 y 6 Km., dependiendo de la aplicación, deben ser colocados repetidores; los cables coaxiales tienen un blindaje que aísla al conductor central del ruido en la transmisión; han sido muy utilizados en comunicaciones de larga distancia y en distribución de señales de televisión, así como en redes de área

local; finalmente, las fibras ópticas transmiten señales ópticas en lugar de las eléctricas de los dos casos anteriores, son mucho más ligeras que los cables metálicos y permiten transmitir tasas muchísimo más altas que los primeros, además, aunque las señales se ven afectadas por ruido, no se alteran por ruido de tipo eléctrico y pueden soportar distancias mayores entre repetidoras (del orden de 100 Km.). Sus aplicaciones principales son enlaces de larga distancia, enlaces metropolitanos y redes locales de alta velocidad.

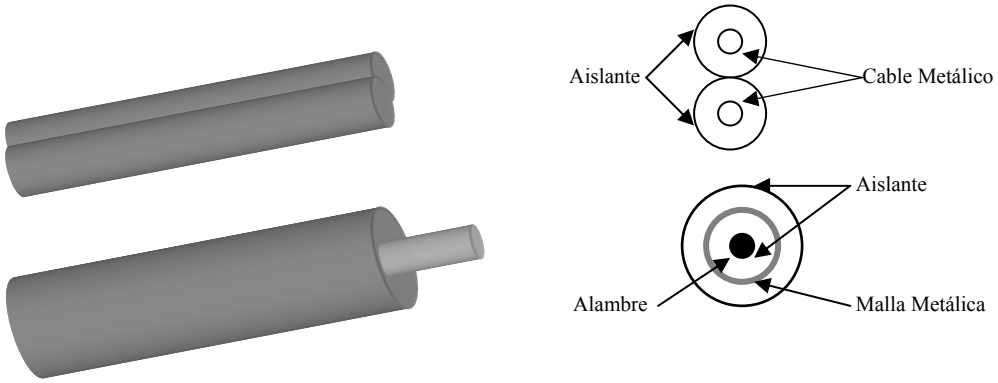


Figura I.2 *Tipos de cables*

La diferencia fundamental entre las transmisiones que utilizan fibras ópticas y las de naturaleza puramente eléctrica, está en el hecho de que en las primeras la información se sobrepone a señales ópticas, es decir, la información modula alguna característica de una señal óptica. Las ventajas de este tipo de transmisiones son múltiples: son mucho menos sensibles a ruido de tipo eléctrico y por el espacio que ocupan en el espectro las señales ópticas, la capacidad de estas transmisiones es mucho mayor que las de los sistemas basados en cables metálicos. Un área en la cual las fibras ópticas han sido de extraordinaria importancia es la de transmisiones transoceánicas; la demanda de este tipo de transmisiones ha crecido en el Atlántico, penetrando asimismo el Pacífico, el Caribe y el Mediterráneo. La clave para este tipo de aplicaciones está en disponer de dispositivos de alta confiabilidad, grandes anchos de banda y pocas pérdidas; esto originó que, alrededor de 1980, surgiera la primera propuesta de un sistema transoceánico basado en fibras ópticas, lo cual, a su vez, permitió instalar en 1988 el primer sistema de este tipo.

2) Canales inalámbricos; son aquellos que difunden la señal sin la necesidad de algún cable. A este tipo de canales pertenecen los canales de radio, que incluyen tanto las microondas como los enlaces satelitales y enlaces mediante dispositivos infrarrojos.

Los medios infrarrojos permiten la transmisión de información a velocidades de hasta 10 Mbps, consiste en la emisión/recepción de un haz de luz infrarroja; por lo

que el emisor y receptor deben tener contacto visual (la luz viaja en línea recta). Debido a esta limitación pueden usarse espejos para modificar la dirección de la luz transmitida.

La banda de frecuencias en la que operan estos dispositivos está ubicada entre los 300GHz y los 400 THz.

La tecnología de microondas encuentra su principal aplicación en las comunicaciones móviles y de banda ancha, con capacidades de transmisión de decenas de Mbps, dentro de la banda espectral que va de los 30 a los 300 Ghz. Debido a la variedad de sistemas que operan en la banda de las microondas, es posible encontrar una gran diversidad de dispositivos y configuraciones de antenas, como son los arreglos Yagi, Logoperiódicas, Cornetas, Cornetas Cónicas y arreglos con Platos Parabólicos.

Los enlaces satelitales son una aplicación de los enlaces de microondas. Un satélite recibe en una banda señales de una estación terrena, las amplifica y las transmite en otra banda de frecuencias. El principio de operación de los satélites es sencillo, aunque al transcurrir los años se ha ido haciendo más complejo: se envían señales de radio desde una antena hacía un satélite estacionado en una orbita fija alrededor de la Tierra (llamado geoestacionario). Los satélites tienen un reflector orientado hacia los sitios donde se quiere hacer llegar la señal reflejada. Y en esos puntos también se tienen antenas cuya función es precisamente captar la señal reflejada por el satélite. De ese punto en adelante, la señal puede ser procesada para que por último sea entregada a su destino.

En la tabla I.2 se encuentran mostradas las bandas de frecuencias en las que operan los satélites:

		Banda de Frecuencia (GHz)		
Banda	Subida		Bajada	Ancho de Banda (MHz)
C	5.9 – 6.4		3.7 – 4.2	500
X	7.9- 8-4		7.25 – 7.75	500
Ku	14 – 14.5		11.7 – 12.2	500
Ka	27 – 30		17 – 20	-
	30 – 31		20 – 21	-
V	50 – 51		40 – 41	1000
Q	-		41 – 43	2000
V		54 – 58		3900
(ISL)		59 – 64		5000

Tabla I.2 *Bandas de frecuencias en las que operan los satélites.*

Las ventajas de las comunicaciones vía satélite son evidentes: se pueden salvar grandes distancias sin importar la topografía o la orografía del terreno, y se pueden usar antenas que tengan coberturas geográficas amplias, de manera tal que muchas estaciones receptoras terrenas puedan recibir y distribuir simultáneamente la misma señal que fue transmitida una sola vez, es por ello que las comunicaciones vía satélite han servido para una gran variedad de aplicaciones que van desde la transmisión de conversaciones telefónicas, la transmisión de televisión, las tele conferencias, hasta la transmisión de datos. Las tasas de transmisión pueden ser desde muy pequeñas hasta del orden de los Mbps. Los requerimientos en cuanto a acceso múltiple, manejo de diversos tipos de tráfico, establecimiento de redes, integridad de los datos, así como seguridad, se satisfacen con las posibilidades ofrecidas por la tecnología VSAT[1].

Entre los servicios que pueden ser ofrecidos por medio de la tecnología VSAT se encuentran: radiodifusión y servicios de distribución, bases de datos, información meteorológica y bursátil, inventarios, facsímiles, noticias, música programada, anuncios, control de tráfico aéreo, televisión de entretenimiento, educación, climatología, mapas, telemetría, transacciones financieras, servicios de bases de datos, servicios de reservaciones, servicio a bibliotecas, interconexión de redes locales, correo electrónico, mensajes de emergencia, videoconferencias, etcétera.

Cabe destacar, que la diferencia principal entre emisiones de radio y de microondas está en que las primeras son omnidireccionales (en todas las direcciones), mientras que las segundas son unidireccionales: por lo tanto, la radio no requiere antenas de alta directividad. Aunque, estrictamente hablando, el término radio incluye todas las transmisiones electromagnéticas, las aplicaciones de la radio se asignan de acuerdo con las bandas del espectro en que se realizan las transmisiones. En la Tabla I.3 se presentan las aplicaciones de los distintos rangos del espectro. Esta clasificación es muy burda, ya que dentro de cada uno de los rangos anteriores existen muchísimas más aplicaciones que no serán mencionadas aquí.

Finalmente, cabe hacer hincapié en que una red moderna de telecomunicaciones normalmente utiliza canales de distintos tipos para lograr la mejor solución a los problemas de telecomunicaciones de los usuarios; es decir, con frecuencia existen redes que emplean canales de radio en algunos segmentos, canales vía satélite en otros, microondas en algunas rutas, radio en otras y, desde luego, en muchos de sus enlaces, la red telefónica pública.

[1] VSAT: Terminales de apertura muy pequeña (*Very Small Aperture Terminals*)

Banda	*Nombre*	*Aplicaciones*
30-300 Khz.	LF (low frecuency) - baja frecuencia	navegación aérea y marítima
300-3000 Khz.	MF (médium frecuency) - frecuencia media	navegación, radio, comercial AM, enlaces privados fijos y móviles
3-30 Mhz	HF (high frecuency) - alta frecuencia	radiodifusión onda corta, enlaces fijos y móviles
30-300 Mhz	VHF (very high frecuency) - muy alta frecuencia	televisión, radio FM, enlaces fijos y móviles
300-3000 Mhz	UHF (ultra high frecuency) - frecuencia ultra alta	televisión y microondas, navegación meteorología
3-30 Ghz	SHF (super high frecuency) - frecuencia super alta	Microondas y satélite, radionavegación
30-300 Ghz	EHF (extra high frecuency) - frecuencia extra alta	experimental

Tabla I.3 *Aplicaciones del espectro electromagnético*

I.4.2 NODOS

Los nodos, parte fundamental en cualquier red de telecomunicaciones, son los equipos encargados de realizar las diversas funciones de procesamiento que requieren cada una de las señales o mensajes que circulan o transitan a través de los enlaces de la red. Desde un punto de vista topológico, los nodos proveen los enlaces físicos entre los diversos canales que conforman la red. Los nodos de una red de telecomunicaciones moderna son equipos que realizan las siguientes funciones:

a) Establecimiento y verificación de un protocolo. Los nodos de la red de telecomunicaciones realizan los diferentes procesos de comunicación de acuerdo con un conjunto de reglas que les permiten comunicarse entre sí. Este conjunto de reglas se conoce con el nombre de protocolos de comunicaciones, y se ejecutan en los nodos para garantizar transmisiones exitosas entre sí, utilizando para ello los canales que los enlazan.

b) Transmisión. Existe la necesidad de hacer un uso eficiente de los canales, por lo cual, en esta función, los nodos de la red adaptan al canal la información o los mensajes en los cuales está contenida, para su transporte eficiente a través de la red.

c) Interfase. En esta función el nodo se encarga de proporcionar al canal las señales que serán transmitidas, de acuerdo con el medio de que está formado el canal. Esto es, si el canal es de radio, las señales deberán ser electromagnéticas a la salida del nodo, independientemente de la forma que hayan tenido a su entrada y

también de que el procesamiento en el nodo haya sido por medio de señales eléctricas.

d) Recuperación. Cuando durante una transmisión se interrumpe la posibilidad de terminar exitosamente la transferencia de información de un nodo a otro, el sistema, a través de sus nodos, debe ser capaz de recuperarse y reanudar en cuanto sea posible la transmisión de aquellas partes del mensaje que no fueron transmitidas con éxito.

e) Formateo. Cuando un mensaje transita a lo largo de una red, pero principalmente cuando existe una interconexión entre redes que manejan distintos protocolos, puede ser necesario que en los nodos se modifique el formato de los mensajes para que todos los nodos de la red (o de la conexión de redes) puedan trabajar exitosamente con dicho mensaje; esto se conoce con el nombre de formateo (o, en su caso, de reformateo). En la Figura I.3 se muestra el formato típico de un paquete.

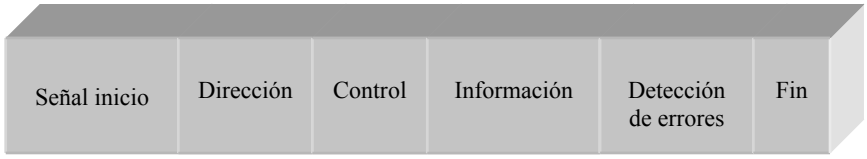


Figura I.3 *Formato típico de un paquete.*

f) Enrutamiento. Cuando un mensaje llega a un nodo de la red de telecomunicaciones, forzosamente debe tener información acerca de los usuarios de origen y destino; es decir, sobre el usuario que lo generó y aquel al que está destinado. Sin embargo, cada vez que el mensaje transita por un nodo y considerando que en cada nodo hay varios enlaces conectados por los que, al menos en teoría, el mensaje podría ser enviado a cualquiera de ellos, en cada nodo se debe tomar la decisión de cuál debe ser el siguiente nodo al que debe enviarse el mensaje para garantizar que llegue a su destino rápidamente. Este proceso se denomina enrutamiento a través de la red. La selección de la ruta en cada nodo depende, entre otros factores, de la situación instantánea de congestión de la red, es decir, del número de mensajes que en cada momento están en proceso de ser transmitidos a través de los diferentes enlaces de la red.

g) Repetición. Existen protocolos que entre sus reglas tienen una previsión por medio de la cual el nodo receptor detecta si ha habido algún error en la transmisión. Esto permite al nodo destino solicitar al nodo previo que retransmita el mensaje hasta que llegue sin errores y el nodo receptor pueda, a su vez, retransmitirlo al siguiente nodo.

h) Direccionamiento. Un nodo requiere la capacidad de identificar direcciones para poder hacer llegar un mensaje a su destino, principalmente cuando el usuario final está conectado a otra red de telecomunicaciones.

i) Control de flujo. Todo canal de comunicaciones tiene una cierta capacidad de manejar mensajes y cuando el canal está saturado ya no se deben enviar más mensajes por medio de ese canal, hasta que los mensajes previamente enviados hayan sido entregados a sus destinos.

Dependiendo de la complejidad de la red, del número de usuarios que tiene conectados y a quienes les proporciona servicio, no es indispensable que todas las redes de telecomunicaciones tengan instrumentadas todas las funciones precedentes en sus nodos. Por ejemplo, si una red consiste solamente en dos nodos a cada uno de los cuales están conectados una variedad de usuarios, es evidente que no se requieren funciones tales como direccionamiento o enrutamiento en los dos nodos que forman la red. Se han descrito aquí, sin embargo, las funciones más importantes que deben tener instrumentadas los nodos de una red compleja.

Una vez expuestas las componentes de una red de telecomunicaciones, a través de la cual se transmite información entre los usuarios, cabe mencionar que lo que realmente da valor a las telecomunicaciones es el conjunto de servicios que se ofrecen por medio de las redes y que se ponen a disposición de los usuarios. Es decir, el valor depende del tipo de comunicación que puede establecer un usuario y del tipo de información que puede enviar a través de la red.

I.5 CLASIFICACIÓN DE LAS REDES

Dependiendo de su arquitectura y de los procedimientos empleados para transferir la información las redes de comunicación se pueden clasificar en:

- Redes conmutadas
- Redes de difusión

I.5.1 REDES CONMUTADAS

Consiste en una sucesión alternante de nodos y canales de comunicación, es decir, después de transmitir la información a través de un canal, llega a un nodo, y éste a su vez la procesa la información para poder transmitirla por el siguiente canal para llegar al siguiente nodo, y así sucesivamente.

Los nodos interconectados entre sí, forman la mayoría de las veces una topología de malla, donde la información se transfiere encaminándola del nodo de origen al nodo destino mediante conmutación entre nodos intermedios. Una transmisión de este tipo tiene 4 fases:

1. Establecimiento de la conexión.
2. Confirmación de la conexión.
3. Transferencia de la información.
4. Liberación de la conexión.

Se entiende por conmutación en un nodo, a la conexión física o lógica, de un camino de entrada al nodo con un camino de salida del nodo, con el fin de transferir la información que llegue por el primer camino al segundo. Un ejemplo muy común del uso de redes conmutadas son las redes de área amplia.

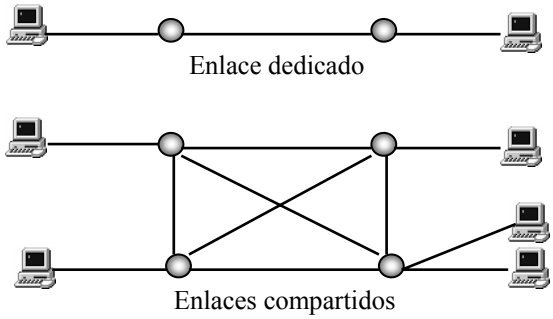


Figura I.4 *Red conmutada.*

Dentro de las redes conmutadas se encuentran los siguientes tipos de conmutación:

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

I.5.1.1 CONMUTACIÓN DE CIRCUITOS

Es el procedimiento por el que dos nodos se conectan, permitiendo la utilización de forma exclusiva del circuito físico durante la transmisión. En cada nodo intermedio de la red se cierra un circuito físico entre un cable de entrada y un cable de salida de la red (Figura I.5).

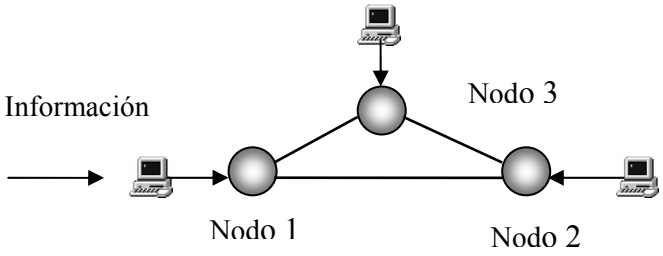


Figura I.5 *Conmutación de circuitos.*

Para establecer una comunicación con esta técnica se requiere de una señal que reserve los diferentes segmentos de la ruta entre ambos usuarios, y durante la comunicación el canal quedará reservado precisamente para esta pareja de usuarios.

Características de la conmutación de circuitos:

- La conexión es permanente durante la llamada.
- El circuito debe establecerse antes de transmitir (servicio orientado a la conexión).
- No hay problema de congestión una vez se establece.
- La única demora es la propagación.
- Reserva recursos anticipadamente.
- Para transmisión de datos hay desperdicio de ancho de banda.
- La forma más utilizada de compartir canales entre conmutadores es TDM[1].

I.5.1.2 CONMUTACIÓN DE MENSAJES

En la conmutación de mensajes en lugar de tener las líneas dedicadas desde un origen hasta un destino, lo que se va a hacer es que cada mensaje sea conmutado a un circuito. El mensaje va a llegar al conmutador, y el conmutador le va a asignar el mensaje a su nodo correspondiente, de esta manera podemos tener varios mensajes, pero cada mensaje tiene que llevar un identificador de encabezado del nodo destino para que pueda ser reconocido por el conmutador (figura I.6).

Sin embargo, el agregar un encabezado a cada mensaje ocasiona un decremento en el desempeño, ya que el encabezado es información adicional y si el encabezado es comparable ó muy grande con respecto a la información, el servicio va a ser menos eficiente.

[1] TDM Multiplezación por División de Tiempo *(Time Division Multiplexing)*

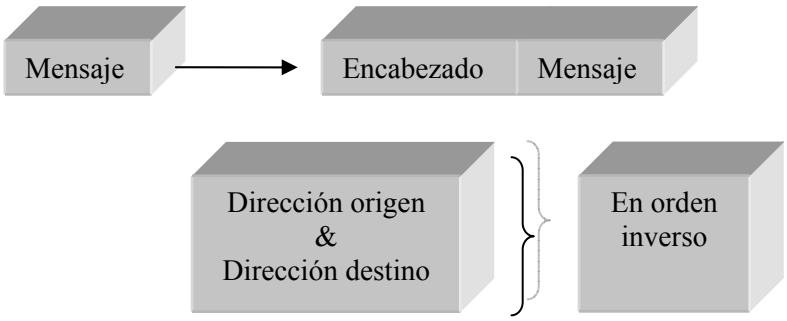


Figura I.6 *Mensaje con información de encabezado*

Para asegurar un desempeño óptimo es necesario procurar que el encabezado sea lo más pequeño posible. Además, por cada encabezado que se encuentre, el conmutador necesita analizarlo y procesarlo (lo cual lleva tiempo); por eso los conmutadores de mensajes deben de ser muy buenos.

I.5.1.3 CONMUTACIÓN DE PAQUETES

En este tipo de conmutación cuando un nodo quiere enviar información a otro, la divide en una serie de paquetes. Cada paquete al igual que en la conmutación de mensajes es enviado por el medio con información de cabecera, y a su vez en cada nodo intermedio por el que pasa el paquete se detiene el tiempo necesario para procesarlo.

Una ventaja de la conmutación de paquetes (además de la seguridad en la transmisión de datos) es que el mensaje es ensamblando de una manera más rápida en el nodo destino, debido a que los paquetes son enviados por varios caminos, produciéndose un fenómeno conocido como transmisión en paralelo. Además, si un mensaje tuviera un error en un bit de información y estuviésemos usando la conmutación de mensajes, tendríamos que retransmitir todo el mensaje; mientras que con la conmutación de paquetes solo hay que retransmitir el paquete con el bit afectado, lo cual es mucho menos problemático. Lo único negativo quizás, en el esquema de la conmutación de paquetes es de que su encabezado es más grande.

Características de la conmutación de paquetes

- En cada nodo intermedio se apunta una relación que establece las reglas de reenvío del paquete con base a su procedencia y a su destino.
- Los paquetes se numeran para poder saber si se ha perdido alguno en el camino.
- Los bloques de información se dividen en unidades de longitud variables.

- El canal se comparte dinámicamente por los usuarios.
- No se dedica un canal permanentemente para un usuario.
- Hay mayor retardo en el tránsito de los paquetes.
- Puede presentar problemas de congestión.
- Adecuado para tráfico de datos.
- Puede soportar servicios orientados o no a la conexión.

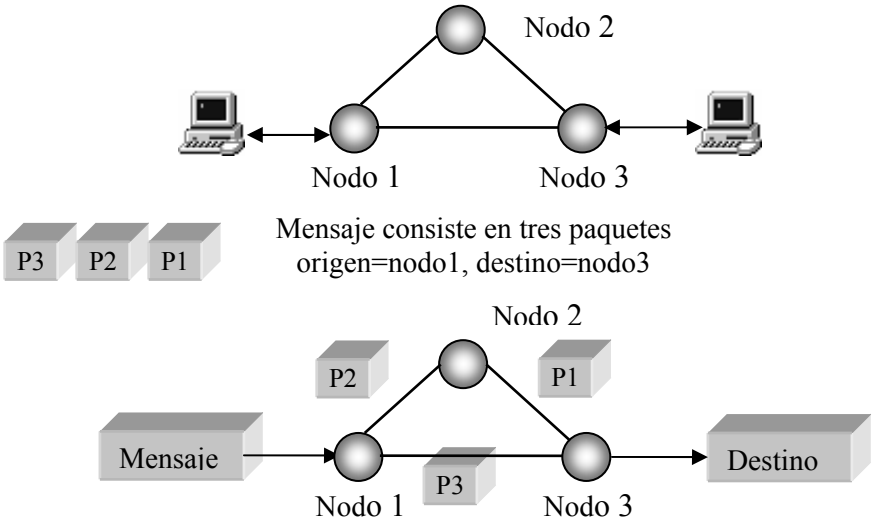


Figura I.7 *Conmutación de paquetes.*

I.5.1.4 CONMUTACIÓN DE CELDAS

Al igual que en conmutación de paquetes cuando un nodo quiere enviar información a otro, este también divide la información en paquetes, pero con la diferencia de que estos son tamaño fijo llamados celdas. En conmutación de celdas el circuito se mantiene permanentemente abierto con la estación destino hasta que termina la comunicación, aun y cuando no haya transmisión de datos.

La ventaja principal de la conmutación de celdas es que los paquetes son mucho mas pequeños y además la conmutación puede ser realizada a nivel hardware y no software, por lo que dichos paquetes pueden ser analizados mediante procesadores dedicados (ASICs[1]), lo cual reduce el tiempo de retardo de la celda en cada nodo.

[1] ASIC Circuitos Integrados de Aplicación Específica *(Application Specific Integrated Circuit)*

Características de la conmutación de celdas:

- Unidad de información de longitud fija.
- La celda de longitud muy corta (53 octetos para ATM[1]).
- La conmutación se realiza por hardware.
- Apta para altas velocidades.
- Bajos tiempos de retardo.
- Aunque principalmente optimiza el tráfico de voz y video, también se utiliza para tráfico de datos.

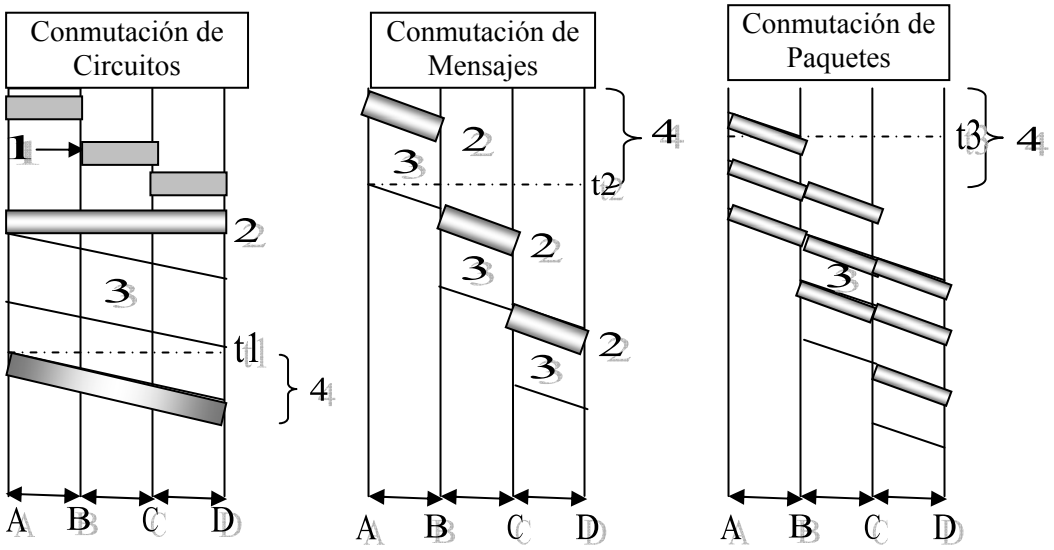


Figura I.8 *Comparación entre los tipos de Conmutación*

Para entender lo anterior en la figura I.8 se muestran las diferencias que existen entre los 3 tipos de conmutación. De manera geneal, se puede decir que el proceso de transferencia de información se divide en 4 fases:

1. Solicitud del circuito.
2. Confirmación del circuito.
3. Transmisión de información.
4. Desconexión de circuitos.

I.5.2 REDES DE DIFUSIÓN

En este tipo de redes se tiene un canal al cual están conectados todos los usuarios y todos ellos pueden recibir todos los mensajes, pero solamente extraen del

[1] ATM Modo de Transferencia Asíncrono (*Asynchronous Transfer Mode)*

canal los mensajes en los que identifican su dirección como destinatarios. Aunque el ejemplo típico lo constituyen los sistemas que usan canales de radio, no necesariamente tienen que ser las transmisiones vía radio, ya que la difusión puede realizarse por medio de canales metálicos, tales como cables de cobre. A continuación se presentan algunos ejemplos de redes de difusión con diferentes formas y arreglos de interconexión (topologías), aplicables a redes basadas en radio o en cables. Lo que si puede afirmarse es que típicamente las redes de difusión tienen sólo un nodo (el transmisor) que inyecta la información en un canal al cual están conectados los usuarios.

En este tipo de redes no existen nodos intermedios de conmutación; todos los nodos comparten un medio de transmisión común, por lo que la información transmitida por un nodo es conocida por todos los demás. Ejemplo de redes de difusión son:

- Comunicación por radio.
- Comunicación por satélite.
- Comunicación en una red de área local.

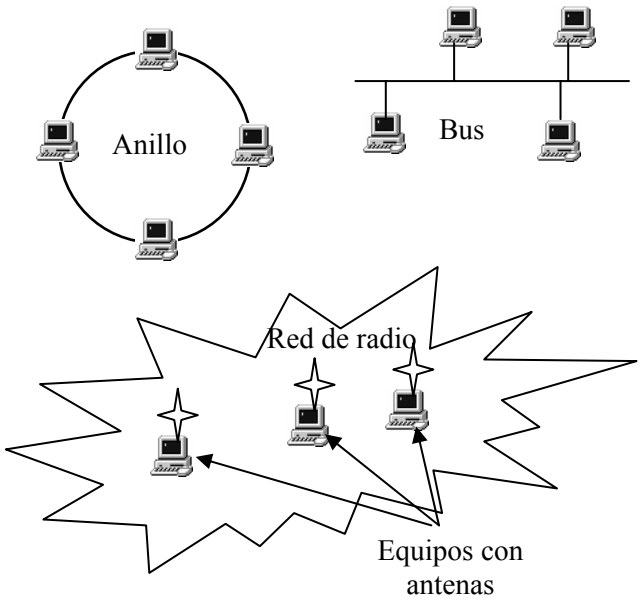


Figura I.9 *Ejemplos de topologías.*

Para todas las redes cada usuario requiere de un equipo terminal, por medio del cual tendrá acceso a la red, pero que no forma parte de la misma. De esta forma, un usuario que desee comunicarse con otro utiliza su equipo terminal para enviar su información hacia la red, ésta transporta la información hasta el punto de conexión del usuario destino con la red y la entrega al mismo a través de su propio equipo terminal.

Los usuarios no pueden transmitir información en todas las redes. Por ejemplo, en televisión o radiodifusión, los usuarios son pasivos, es decir, únicamente reciben la información que transmiten las estaciones transmisoras.

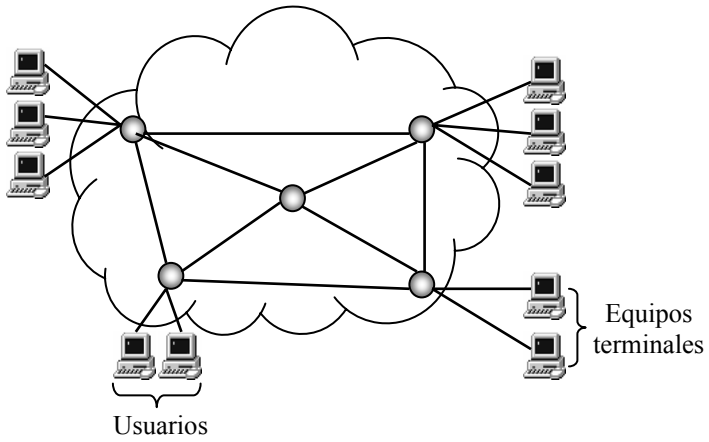


Figura I.10 *Operación de una red.*

I.6 TOPOLOGIA DE UNA RED

I.6.1 CONCEPTOS BASICOS

La topología de una red, define la distribución de cada estación en relación a la red y a las demás estaciones. Se trata de parámetros básicos que condicionan fuertemente las prestaciones de la red.

La topología de una red define entre otras cosas la distribución del cable que interconecta las diferentes computadoras, es decir, el mapa de distribución del cable que forma la red. A la hora de instalar una red, es importante seleccionar la topología más adecuada a las necesidades existentes. Hay una serie de factores a tener en cuenta a la hora de decidirse por una topología de red concreta y son:

- La distribución física de los equipos a interconectar.
- El tipo de aplicaciones que se van a ejecutar.
- La inversión que se quiere hacer.
- El costo que se quiere dedicar al mantenimiento y actualización de la red local.
- El tráfico que va a soportar la red local.

- La capacidad de expansión puesto que se debe diseñar una red teniendo en cuenta la escalabilidad.

No se debe confundir el término topología con el de arquitectura, la arquitectura de una red engloba:

- La topología.
- El método de acceso al medio.
- Protocolos de comunicaciones.

Actualmente la topología está directamente relacionada con el método de acceso al medio, puesto que éste depende casi directamente del dispositivo de interconexión a la red y éste depende de la topología elegida.

I.6.2 TOPOLOGÍA FÍSICA

La topología física de una red se encuentra determinada por la forma en la que el cableado se realiza en una red. Existen cuatro topologías físicas:

- Topología en anillo.
- Topología en bus.
- Topología en estrella.
- Topología jerárquica

Una quinta no menos importante en teoría es la:

- Topología completa que consistente en conectar todos los equipos entre sí. En la práctica no se implementa por su elevado costo, y el buen funcionamiento del resto de topologías.

El número de enlaces necesarios para implantar una topología completa se calcula mediante la fórmula I.1:

$$\frac{n \times (n-1)}{2} \qquad \textbf{(I.1)}$$

Existen mezclas de topologías físicas, dando lugar a redes que están compuestas por más de una topología física.

I.6.2.1 TOPOLOGÍA JERÁRQUICA

Se dice que una red está configurada con una topología jerárquica cuando sus elementos se encuentran interconectados en forma de una estructura de árbol, de manera que se definen elementos DCE[1]/DTE[2] llamados padres, que administran elementos de otros sistemas DTE/DCE, denominados hijos. Algunas de sus principales características son:

- El software que la opera es simple y fácil.
- El DCE padre es el que maneja y administra los errores y tareas de control.

Algunas de las desventajas que presenta una topología jerárquica son:

- Fácil que se presenten cuellos de botella.
- Saturaciones, problemas con la fiabilidad.
- Si el DCE padre falla deja de funcionar toda la red.

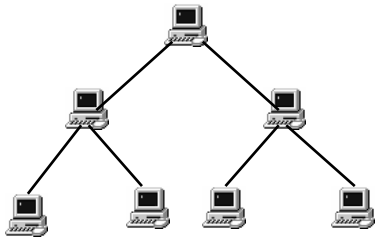


Figura I.11 *Topología Jerárquica*

I.6.2.2 TOPOLOGÍA EN BUS

Consta de un único cable que se extiende de una computadora a otra en un modo serie (Figura I.12). Anteriormente los extremos del cable se terminaban con una resistencia denominada terminador, que además de indicar que no existen más computadoras en el extremo, permite cerrar el bus.

Sus principales ventajas son:

- Fácil de instalar y mantener.
- No existen elementos centrales del que dependa toda la red, cuyo fallo dejaría inoperativas a todas las estaciones.

[1] DCE Equipo de Comunicación de datos *(Data Communications Equipment*
[2] DTE Equipo Terminal de Datos *(Data Terminal Equipment)*

Algunos de sus inconvenientes son:

- Si se rompe el cable en algún punto, la red queda inoperativa por completo.

Cuando se decide instalar una red de este tipo en un edificio con varias plantas, lo que se hace es instalar una red por planta y después unirlas todas a través de un bus troncal. Este tipo de topología se estudiará con más detalle en los capítulos siguientes.

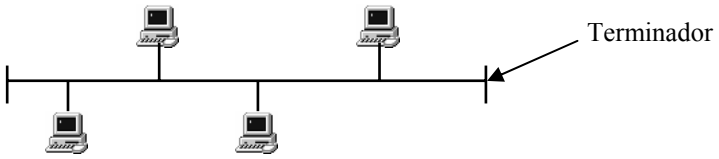


Figura I.12 *Topología Bus*

Las computadoras sobre una topología de bus, se comunican por datos direccionados para computadoras particulares y colocando aquellos datos sobre el cable en la forma de señales electrónicas. Para entender como las computadoras se comunican sobre un bus es necesario familiarizarse con 3 conceptos:

- Envío de señal
- Señal de rebote
- Terminador

ENVÍO DE SEÑAL

El dato de red en forma de señales electrónicas es enviado por todas las computadoras en la red. Sin embargo, la información es aceptada sólo por la computadora cuya dirección sea la indicada en la señal original (sólo una computadora a la vez puede enviar mensajes).

Debido a que sólo una computadora a la vez puede enviar datos sobre una red bus, el desempeño de la red es afectada por el número de computadoras conectadas a este, si se conectan muchas computadoras en la red, la mayor parte de ellas estarán esperando para poner datos en el bus y el desempeño será menor.

Sin embargo ésta no es una medida estándar para conocer el impacto de números grandes de computadoras sobre cualquier red, y que como se verá mas adelante, la capacidad que tiene una red de transmitir datos a altas velocidades depende de numerosos factores como:

- Capacidad del hardware de las computadoras sobre la red
- Número de veces que las computadoras transmiten datos
- Tipo de aplicaciones existentes y que corren sobre la red.
- Tipo de cable usado en la red
- Distancia entre las computadoras de la red

El bus es una topología pasiva. Las computadoras sobre el bus, sólo escuchan los datos enviados sobre la red. Estas no son responsables por el movimiento de datos de o para una computadora próxima. Si una computadora falla, ésta no afecta al resto de la red. En una topología activa, las computadoras regeneran señales y mueven datos a lo largo de la red.

SEÑAL DE REBOTE

Debido a que el dato o señal electrónica es enviada por toda la red, ésta viajará del extremo de un cable hacia otro. Si a la señal se le permite continuar interrumpida, esta continua rebotando a lo largo del cable y evitando que otras computadoras envíen señales, la señal se detiene después de que esta tenga una oportunidad para llegar a la dirección apropiada.

TERMINADOR

Para detener la señal de rebote se coloca un componente llamado terminador al final del cable para absorber señales libres, de esta forma se limpia el cable y las otras computadoras pueden enviar datos.

I.6.2.3 TOPOLOGÍA EN ANILLO

La topología en anillo, conecta computadoras en un simple círculo de cable. Las señales viajan alrededor del bucle en una dirección y pasan a través de cada computadora. A diferencia de la topología pasiva de bus, cada computadora actúa como un repetidor que impulsa la señal y la envía a la siguiente computadora. Debido a que la señal pasa a través de cada computadora, la falla de una computadora puede impactar a la red entera.

Sus principales características son:

- El cable forma un bucle cerrado formando un anillo.
- Las computadoras que forman parte de la red se conectan a ese anillo.

- Habitualmente las redes en anillo utilizan como método de acceso al medio el modelo *"token passing"*.

Los principales inconvenientes son:

- Si se rompe el cable que forma el anillo se paraliza toda la red.
- Es difícil de instalar.
- Requiere mantenimiento periódico.

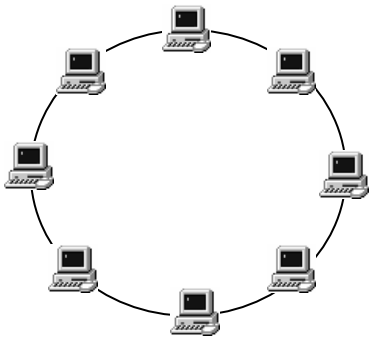


Figura I.13 *Topología Anillo*

Una metodología de transmisión de datos a través del anillo (*ring*) es llamado *token passing*[1]. El token es un pasajero que va de computadora en computadora buscando una que tenga datos para enviar. La computadora que envía, modifica el token, pone una dirección electrónica en el dato y se envía ésta alrededor del anillo. El dato pasa por cada computadora hasta que encuentra una con una dirección que equivalga a la dirección del dato.

La computadora que recibe devuelve un mensaje para la computadora que envió, indicando que el dato ha sido recibido. Después de una verificación, la computadora que envió crea un nuevo token y libera éste sobre la red.

I.6.2.4 TOPOLOGÍA EN ESTRELLA

En la topología estrella, las computadoras son conectadas por segmentos de cable hacia un componente centralizado, llamado *hub*[2]. Las señales son transmitidas desde la computadora a través del hub para todas las computadoras sobre la red. Esta topología proviene de la época en que se conectaban varias computadoras a una computadora central denominada *main frame*.

[1] Token Passing. Paso de testigo
[2] Hub. Concentrador

La red en estrella ofrece recursos y administración centralizada. Sin embargo, debido a que cada computadora es conectada a un punto central, esta topología requiere de una gran distribución de cable en una instalación de red grande. También si el punto central falla, la red entera se viene abajo.

Si una computadora, o el cable que conecta ésta al hub falla en una red de estrella, sólo la computadora de la falla no será habilitada para enviar o recibir datos. El resto de la red continuará funcionando normalmente.

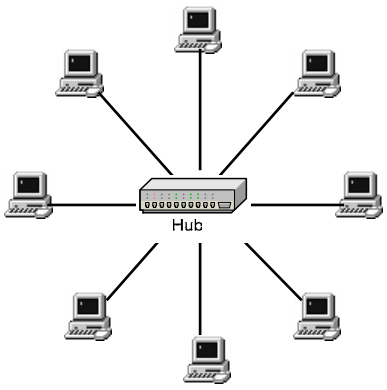


Figura I.14 *Topología Estrella*

TOPOLOGÍA EN ESTRELLA PASIVA

Se trata de una estrella en la que el punto central al que van conectados todos los nodos es un concentrador pasivo, es decir, se trata únicamente de un dispositivo con muchos puertos de entrada.

TOPOLOGÍA EN ESTRELLA ACTIVA

Se trata de una topología en estrella que utiliza como punto central un hub activo o bien una computadora que hace las veces de servidor de red. En este caso, el hub activo se encarga de repetir y regenerar la señal transferida e incluso puede estar preparado para realizar estadísticas del rendimiento de la red. Cuando se utiliza una computadora como nodo central, es éste el encargado de gestionar la red, y en este caso suele ser además del servidor de red, el servidor de archivos.

I.6.3 TOPOLOGÍA LÓGICA

Es la forma de conseguir el funcionamiento de una topología física cableando la red de una forma más eficiente. Existen topologías lógicas definidas:

- Topología anillo-estrella: implementa un anillo a través de una estrella física.
- Topología bus-estrella: implementa una topología en bus a través de una estrella física.

I.6.3.1 TOPOLOGÍA ANILLO-ESTRELLA

La topología anillo-estrella (algunas veces llamadas estrella cableada anillo) parece similar a la "bus-estrella". Ambas, son centralizadas en un hub el cual contiene el actual anillo o bus. Los hubs en una topología estrella-bus, son conectados por trozos de buses lineales, en cambio los hubs en una topología estrella-anillo son conectados en un modelo estrella por el hub principal.

Uno de los inconvenientes de la topología en anillo era que si el cable se rompía toda la red quedaba inoperativa; con la topología mixta anillo-estrella, éste y otros problemas quedan resueltos. Las principales características son:

- Cuando se instala una configuración en anillo, el anillo se establece de forma lógica únicamente, ya que de forma física se utiliza una configuración en estrella.

- Se utiliza un hub, o incluso un servidor de red como dispositivo central, de esta forma, si se rompe algún cable sólo queda inoperativo el nodo que conectaba, y los demás pueden seguir funcionando.

- El hub utilizado cuando se está utilizando esta topología se denomina MAU[1], que consiste en un dispositivo que proporciona el punto de conexión para múltiples nodos. Contiene un anillo interno que se extiende a un anillo externo.

A simple vista, la red parece una estrella, aunque internamente funciona como un anillo.

Cuando la MAU detecta que un nodo se ha desconectado (por haberse roto el cable, por ejemplo), puentea su entrada y su salida para así cerrar el anillo.

[1] MAU: Unidad de Conexión al Medio *(Media Acces Unit)*

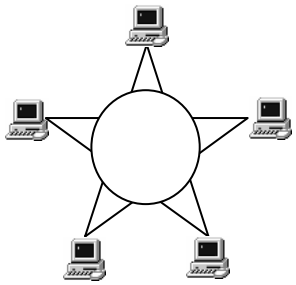


Figura I.15 *Topología Anillo - Estrella*

I.6.3.2 TOPOLOGÍA BUS-ESTRELLA

Este tipo de topología es en realidad una estrella que funciona como si fuera un bus. Como punto central tiene un concentrador pasivo (hub) que implementa internamente el bus, y al que están conectadas todas las computadoras. La única diferencia que existe entre esta topología mixta y la topología en estrella con hub pasivo es el método de acceso al medio utilizado.

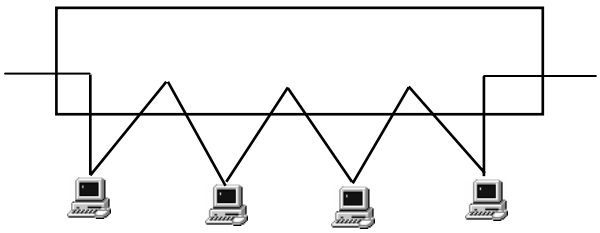


Figura I.16 *Topología Bus - Estrella*

Si una computadora se cae, esto no afecta el resto de la red. Las otras computadoras serían habilitadas para continuar comunicándose. Si un hub falla, todas las computadoras conectadas a ese hub son incapaces de comunicarse, así si este hub es vinculado con otros hub, esas conexiones también serán interrumpidas.

I.7 INTERCONEXIÓN DE REDES

Hace algunos años era impredecible la evolución que iban a tener las comunicaciones en el mundo de la informática, no se podía prever que fuera necesaria la interconexión ya no sólo de varias computadoras sino de cientos de ellas. Hoy en día no basta con tener las computadoras en una sala conectadas, es necesario conectarlas a su vez con las computadoras del resto de las salas de una empresa, y con el resto de las sucursales de una empresa situadas en distintos puntos geográficos.

La interconexión de redes permite, si se puede decir así, ampliar el tamaño de una red. Sin embargo el término interconexión se utiliza para unir redes independientes, no para ampliar el tamaño de una.

Una Intranet es un lugar en la Internet o un grupo de lugares en la Internet que le pertenecen a una organización en el cual es sólo accesible para sus miembros o empleados. El número de computadoras que componen una Intranet es limitado, depende de la topología elegida, (recuerde que en la topología se define el cable a utilizar) aunque si lo único que se quisiera fuera sobrepasar el número de computadoras conectadas, podría pensarse en simplemente segmentar la Intranet. Sin embargo existen otros factores a tomar en cuenta.

Cuando se elige la topología que va a tener una Intranet se deben considerar factores, como son la densidad de tráfico que ésta debe soportar de manera habitual, el tipo de aplicaciones que van a instalarse sobre ella, la forma de trabajo que debe gestionar, etc.; esto hace pensar que uno de los motivos por el que se crean diferentes topologías es el uso que se le va a dar a la Intranet.

De aquí se puede deducir que en una misma empresa puede hacerse necesaria, no la instalación de una única Intranet, aunque sea segmentada, sino la implantación de redes independientes, con topologías diferentes e incluso arquitecturas diferentes y que a su vez se interconecten.

Habitualmente la selección del tipo y los elementos físicos de una Intranet, se ajusta a las necesidades que se tiene; por este motivo pueden encontrarse dentro de un mismo edificio, varias intranets con diferentes topologías, y con el tiempo puede surgir la necesidad de interconectarlas.

Se puede ver que por diferentes razones se hace necesaria tanto la segmentación como la interconexión de intranets, y que ambos conceptos a pesar de llevar a un punto en común, parten de necesidades distintas.

La tabla I.4 refleja de forma escueta diferentes casos en los que se plantea la necesidad de segmentar y/o interconectar intranets, dando la opción más idónea para cada uno de los casos planteados.

NECESIDAD	SOLUCIÓN
Debido a la necesidad de manejo de aplicaciones que producen un movimiento importante de información, aumenta el tráfico en la red; esto lleva a que baje el rendimiento de la misma.	Dividir la red actual en varios segmentos: segmentar la red.
Se tiene que ampliar el número de puestos que forman la Intranet, pero se necesita mantener el rendimiento de la red	Crear un nuevo segmento de red en el que se pondrán los nuevos puestos e incluso al que se pueden mover puestos, que por disposición física pueda ser conveniente que pertenezcan al nuevo segmento creado en la misma.
Se tiene la necesidad de unir dos intranets exactamente iguales en la empresa	Se puede optar por definir una de ellas como un segmento de la otra y unirlas de esta forma; o bien, interconectar las dos intranets con un dispositivo de bajo nivel.
Se tiene la necesidad de unir dos o más redes con diferentes topologías pero trabajando con los mismos protocolos de comunicaciones.	Es necesario la interconexión de ambas redes a través de dispositivos interconectantes de nivel medio
Se tiene la necesidad de unir dos o más redes totalmente diferentes, es decir, de arquitecturas diferentes.	Es necesaria la interconexión de ambas redes a través de dispositivos interconectantes de alto nivel.

Tabla I.4 *Problemas más comunes*

I.8 JERARQUÍAS EN REDES

La manera más sencilla de clasificar las jerarquías en redes, es con base a la distancia entre computadoras, aunque esto varia dependiendo de la ubicación y lugar geográfico de la red. Si las computadoras se encuentran dentro de un mismo ámbito geográfico como una habitación, un edificio o un campus (como máximo, del orden de 1 Km.) se llama **Red de Área Local** (*Local Área Network*). Si la distancia es del orden de la decena de kilómetro entonces se está ante una **Red de Área Metropolitana** (*Metropolitan Área Network*). Si la distancia es de varios cientos de kilómetros entonces se habla de una **Red de Área Amplia** (*Wide Área Network*) y si se trata de una red que cubre todo el planeta entonces se habla de **Internet**.

Otro concepto en la jerarquía de redes son las **Redes de Área Personal** *(Personal Área Network)*. Una red de área personal es la interconexión de dispositivos de tecnología de información dentro del rango individual, típicamente dentro de un rango de 10 metros.

Escala
Multicomputadoras: 1 m
PAN[1]: 1m a 10m
LAN[2] : 10 m a 1 km
MAN[3]: 10 km
WAN[4] : 100 km a 1.000 km
Internet: 10.000 Km.

I.8.1 PAN

Una PAN, es una jerarquía en la que se utiliza tecnología que puede hacer posible la comunicación de computadoras portátiles con otras computadoras cercanas e intercambiar información digital utilizando la conductividad eléctrica del cuerpo humano como una red de datos. Por ejemplo, dos personas donde cada uno lleva puesta su tarjeta de negocios con su transmisor y receptor pueden intercambiar información con tan solo estrecharse las manos. La transferencia de datos a través del contacto intra-corporal, tal como un saludo de manos, es conocida como conexión. La salinidad natural del cuerpo humano, hace que este sea un buen conductor de electricidad.

Un campo eléctrico pasa pequeñas corrientes del orden de pico amperes a través del cuerpo humano, cuando dos personas estrechan las manos, el saludo completa el circuito y los datos personales tales como correo electrónico y números telefónicos son transferidos a la otra computadora personal o dispositivo. Así mismo la ropa de una persona también puede actuar como mecanismo para la transferencia de datos.

El concepto de PAN fue desarrollado por primera vez por Thomas Zimmerman y otros investigadores del laboratorio de medios del M.I.T y después fue soportado por los laboratorios de investigación Almaden de IBM. En una investigación en papel, Zimmerman explica como el concepto puede ser utilizado:

Como los dispositivos electrónicos comienzan a hacerse más pequeños, con bajos requerimientos de potencia y menos caros, hemos comenzado a adornar nuestros cuerpos con información personal y accesorios en comunicación, tales como: teléfonos celulares, asistentes digitales personales, video juegos de bolsillo y radio localizadores.

[1] PAN: Red de Área Personal *(Personal Area Network)*
[2] LAN: Red de Área Local *(Local Area Network)*
[3] MAN: Red de Área Metropolitana *(Metropolitan Area Netwok)*
[4] WAN: Red de Área Amplia *(Wide Area Network)*

Actualmente este no es un método para que dichos dispositivos compartan información. Realizar una red con estos dispositivos puede reducir las redundancias de entrada/salida y permitir nuevas comodidades y servicios

I.8.2 LAN

Las LAN están restringidas en cuanto a su tamaño y por ello se puede determinar de manera más exacta su velocidad de transmisión. El medio de transmisión consiste en un cable al que están conectadas todas las máquinas. Su topología, es decir la forma en que enlazan las computadoras puede ser en bus o en anillo, etc.

El IEEE (Institute of Electrical and Electronics Enginners) nos da la siguiente definición de lo que es una LAN: "Sistema de comunicación de datos que permite a un cierto número de dispositivos comunicarse directamente entre sí, dentro de un área geográfica reducida y empleando canales físicos de comunicación de velocidad moderada o alta".

I.8.2.1 CONSTITUCIÓN DE UNA RED LAN

Los componentes básicos requeridos para que funcione una LAN se pueden dividir en dos categorías: hardware y software.

- Una red de área local requiere los siguientes componentes de hardware: el servidor de archivos, las estaciones de trabajo, el cableado, equipamiento de conectividad y las tarjetas de red o NICs (*Network Interface Cards*).
- El software necesario para que una LAN funcione correctamente está formado por el sistema operativo del servidor de archivos o sistema operativo de red y el de la estación de trabajo.

I.8.2.2 CARACTERÍSTICAS

Algunas de las características que definen una red LAN son:

- Compartición de recursos, como impresoras, scaners, módems, discos remotos, etc.
- Interconexión de equipos informáticos.
- Es una red privada corporativa ya que la red es propiedad de la organización.
- Cobertura geográfica limitada, aprox. 1Km

- Velocidades de transmisión elevadas (10 Gbps).
- Tasas de error de transmisión muy bajas.
- Permite un uso transparente de los recursos, puesto que el uso de equipos remotos como impresoras es como si se tuvieran en nuestro equipo local.
- Fácil instalación y explotación.
- Facilidad para su gestión y administración.

Bien planificada e implementada, una red local aumenta la productividad de las computadoras y periféricos implicados en ella. Si no se planifica y monta apropiadamente puede ser motivo de pérdida de tiempo e información.

Las ventajas que nos puede aportar el uso se pueden resumir en los siguientes puntos:

- La compartición de recursos. Esto nos permite tener datos e información actualizados, el acceso a periféricos remotos y nos permite usar programas y aplicaciones de una forma centralizada.
- Incremento de la capacidad de comunicaciones.
- Reducción de costos. Directamente porque el número de recursos a utilizar son menores ya que estos se comparten por un conjunto de computadoras. E indirectamente por el aumento de la productividad.
- Uso de un mismo software desde distintos puestos de la red.
- Copias de seguridad centralizadas.
- Simplifica el mantenimiento del conjunto de máquinas.

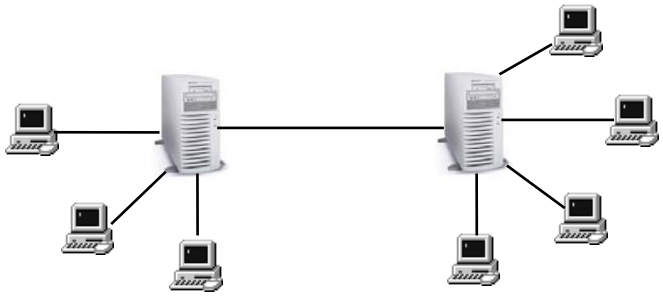


Figura I.17 *Red de Área Local (Local Área Network)*

I.8.3 MAN

Las redes de área metropolitana o MAN están basadas en una tecnología similar a las LAN y son capaces de transmitir datos, voz y señal de TV por cable local. Normalmente son redes de fibra óptica de gran velocidad que conectan segmentos

de red local de una área específica, como un campus un polígono industrial o una ciudad.

El IEEE (*Institute of Electrical and Electronics Enginners*) nos da la siguiente definición de lo que es una MAN en el estándar 802.6 (Redes de Área Metropolitana), el cual define un protocolo de alta velocidad donde las estaciones enlazadas comparten un bus dual de fibra óptica usando un método de acceso llamado Bus Dual de Cola Distribuida (DQDB por sus siglas en inglés). El bus dual provee tolerancia de fallas para mantener las conexiones en caso de que el bus se rompa.

El estándar MAN esta diseñado para proveer servicios de datos, voz y vídeo en un área metropolitana de aproximadamente 50 kilómetros a tasas de 1.5, 45, y 155 Mbits/seg. DQDB es el protocolo de acceso subyacente para el SMDS (Servicio de Datos de Multimegabits Switcheados).

Los servicios de las MAN son *Sin Conexión, Orientados a Conexión*, y/o I*sócronas* (vídeo en tiempo real). El bus se compone por una cantidad de *slots* de longitud fija en los que se acomodan los datos para transmitir sobre el bus. Cualquier estación que necesite transmitir simplemente acomoda los datos en uno o más *slots*. Sin embargo, para servir datos isócronos, los *slots* se reservan en intervalos regulares para garantizar que los datos llegan a tiempo y en orden.

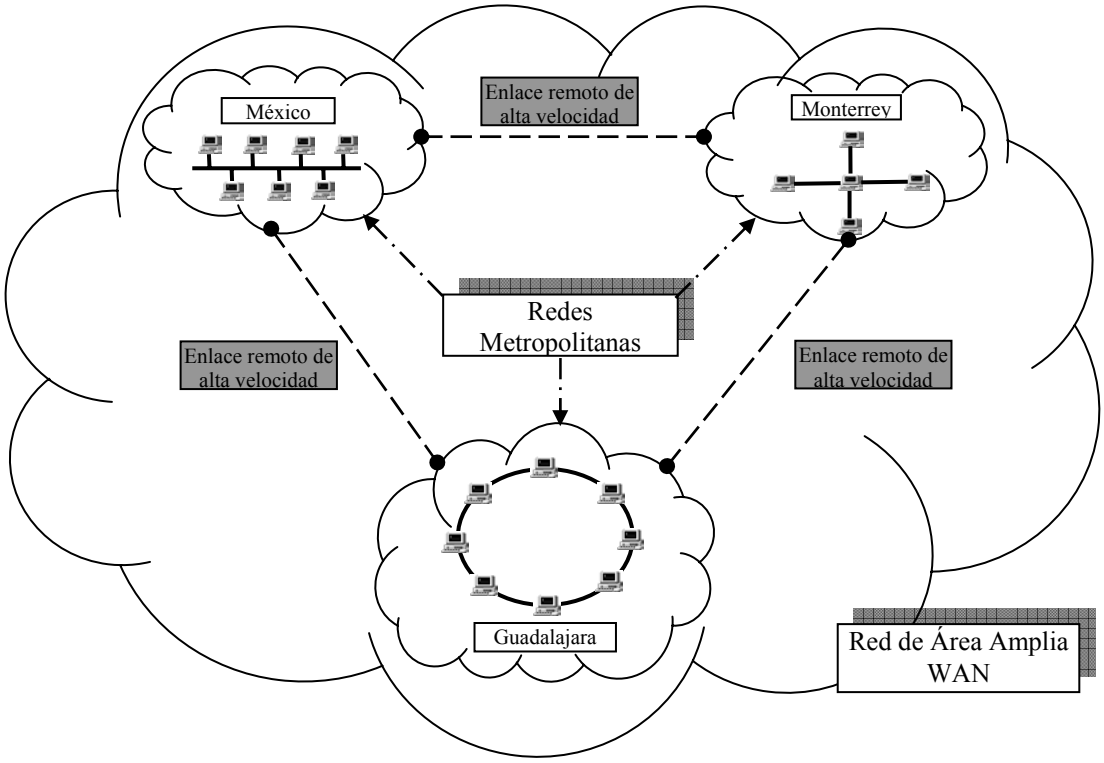


Figura I.18 *Red de Área Metropolitana (Metropolitan Área Network)*

I.8.4 WAN

Una red WAN por sus siglas en ingles *Wide Area Network,* (Redes de Área Amplia) a veces llamadas redes de gran alcance (*long haul networks*), proporcionan comunicación que cubre grandes distancias. Muchas tecnologías WAN no tienen un límite de distancia de recorrido; una WAN puede permitir que dos puntos inmediatamente lejanos se comuniquen. Por ejemplo, una WAN puede recorrer un continente o unir computadoras a través de un océano. Por lo común las WAN operan más lentamente que las LAN y tienen tiempos de retardo mucho mayores entre las conexiones.

Las velocidades convencionales para una WAN están en un rango que va de los 56 kbps a 155 Mbps. Los retardos para una WAN pueden variar de unos cuantos milisegundos a varias decenas de segundos.[1] Debido a que las tecnología LAN cubre distancias cortas, ofrece tiempos de retraso mucho menores que las WAN. Los tiempos de retardo en una LAN pueden ser cortos, como unas cuantas decenas de milisegundos, o largos, 10 milisegundos.

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

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

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

I.8.4.1 CONSTITUCIÓN

La red consiste en los Equipos de Comunicación de Datos (DCE *Data Communication Equipment)*, interconectados por canales alquilados de alta

[1] Estos retardos se deben a que algunas redes WAN se comunican por medio de envío de señales a los satélites en órbita alrededor de la Tierra.

velocidad. Cada DCE utiliza un protocolo responsable de enrutar correctamente los datos y de proporcionar soporte a las computadoras y terminales de los usuarios finales conectados a los mismos. La función de soporte del Equipo Terminal de Datos (DTE *Data Terminal Equipment)* es la de ensamblar o desensamblar los paquetes a esta función se le denomina a veces PAD (*Packet Assembly / Disasembly*).

I.8.4.2 CARACTERÍSTICAS

- Los canales suelen proporcionarlos las compañías telefónicas, con un determinado costo mensual si las líneas son alquiladas, y un costo proporcional a la utilización si son líneas normales conmutadas.
- Los enlaces son relativamente lentos de 64 kbps a 155Mbps.
- Los dispositivos DTE y los DCE están separados por distancias que varían desde algunos kilómetros hasta cientos de kilómetros.
- Las líneas son relativamente propensas a errores (si se utilizan circuitos telefónicos convencionales).

I.8.4.3 WAN VS LAN

Las redes de área local (LAN) son significativamente diferentes de las redes de cobertura amplia. El sector de las LAN es uno de los de más rápido crecimiento en la industria de las comunicaciones. Las redes de área local poseen las siguientes las características.

- Generalmente, los canales son propiedad del usuario o empresa. Los enlaces son líneas desde 1 Mbps hasta 10 Gbps.

- Las líneas son de mejor calidad que los canales en las WAN. Debido a las diferencias entre las redes de área local y las redes de área amplia, sus topologías pueden tomar formas muy diferentes.

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

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

I.8.4.4 COMPONENTES FÍSICOS

Línea de comunicación: Medios físicos para conectar una posición con otra con el propósito de transmitir y recibir datos.

Hilos de transmisión: En comunicaciones telefónicas se utiliza con frecuencia el término "pares" para describir el circuito que compone un canal. Uno de los hilos del par sirve para transmitir o recibir los datos, y el otro es la línea de retorno eléctrico.

I.8.4.5 CLASIFICACIÓN DE LAS LÍNEAS DE CONMUTACIÓN

- *Líneas conmutadas:* Líneas que requieren de marcar un código para establecer comunicación con el otro extremo de la conexión.
- *Líneas dedicadas:* Líneas de comunicación que mantienen una permanente conexión entre dos o más puntos. Estas pueden ser de dos o cuatro hilos.
- *Líneas punto a punto:* Enlazan dos DTE.
- *Líneas multipunto:* Enlazan tres o más DTE.
- *Líneas digitales:* En este tipo de línea, los bits son transmitidos en forma de señales digitales. Cada bit se representa por una variación de voltaje y esta se realiza mediante codificación digital.

I.8.4.6 TIPOS DE REDES WAN

Conmutadas por circuitos: Redes en las cuales, para establecer comunicación se debe efectuar una llamada y cuando se establece la conexión, los usuarios disponen de un enlace directo a través de los distintos segmentos de la red.

Conmutadas por mensaje: En este tipo de redes un ruteador suele ser quien se encarga de aceptar tráfico de las computadoras y terminales conectadas a él. El ruteador examina la dirección que aparece en la cabecera del mensaje hacia el DTE que debe recibirlo. Esta tecnología permite grabar la información para atenderla

después. El usuario puede borrar, almacenar, redirigir o contestar el mensaje de forma automática.

Conmutadas por paquetes: En este tipo de red los datos de los usuarios se descomponen en trozos más pequeños. Estos fragmentos o paquetes, estás insertados dentro de información del protocolo y recorren la red como entidades independientes

Redes orientadas a conexión*:* En estas redes existe el *concepto* de multiplexión de canales y puertos conocido como *circuito o canal virtual*, debido a que el usuario aparenta disponer de un recurso dedicado, cuando en realidad lo comparte con otros pues lo que ocurre es que atienden a ráfagas de tráfico de distintos usuarios.

Redes no orientadas a conexión*:* Llamadas Datagramas, pasan directamente del estado libre al modo de transferencia de datos. Estas redes no ofrecen confirmaciones, control de flujo ni recuperación de errores aplicables a toda la red, aunque estas funciones si existen para cada enlace particular. Un ejemplo de este tipo de red es Internet.

Red pública de conmutación telefónica (PSTN)*:* Esta red fue diseñada originalmente para el uso de la voz y sistemas análogos. La conmutación consiste en el establecimiento de la conexión previo acuerdo de haber marcado un número que corresponde con la identificación numérica del punto de destino.

Figura I.19 *Red de Área Amplia (Wide Area Network)*

I.8.5 INTERNET

El Internet, algunas veces llamado simplemente "La Red", es un sistema mundial de redes de computadoras, un conjunto integrado por las diferentes redes de cada país del mundo, por medio del cual un usuario en cualquier computadora puede, en caso de contar con los permisos apropiados, accesar información de otra computadora y poder tener inclusive comunicación directa con otros usuarios en otras computadoras.

Hoy en día, el Internet es un medio de comunicación público, cooperativo y autosuficiente en términos económicos, accesible a cientos de millones de gentes en el mundo entero. Físicamente, el Internet usa parte del total de recursos actualmente existentes en las redes de telecomunicaciones. Técnicamente, lo que distingue al Internet es el uso del protocolo de comunicación llamado TCP/IP (*Transmission Control Protocol/Internet Protocol*).

Para muchos usuarios del Internet, el correo electrónico (*e-mail*) ha reemplazado prácticamente al servicio postal para breves mensajes por escrito. El correo electrónico es la aplicación de mayor uso en la red. También se pueden realizar conversaciones "en vivo" con otros usuarios en otras localidades usando diversas aplicaciones como los IRC (*Internet Relay Chat*). Más recientemente, el software y hardware para telefonía en Internet permite conversaciones de voz en línea.

Internet es conocida como una red de redes, la cual es también llamada Telaraña de Área Mundial “WWW” (***World Wide Web***), donde una red se enlaza a otras redes independientes de manera que puedan compartir información entre ellas como las redes científicas, de investigación y educacionales a lo largo de todo el planeta, así como a un número creciente de redes comerciales.

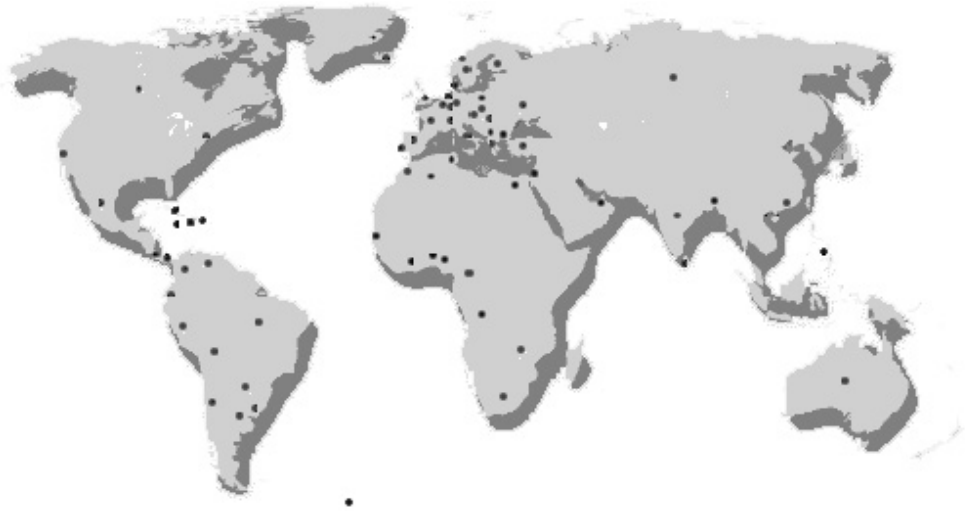


Figura I.20 *Internet*

I.9 MODELO DE INTERCONECCIÓN DE SISTEMAS ABIERTOS (OSI)

El modelo OSI describe la manera como se mueve la información de una aplicación del software en una computadora a otra a través de un medio de red. El modelo OSI es un modelo conceptual compuesto de siete capas, cada una especifica funciones particulares dentro de los procesos de intercambio de información en una red. El modelo fue desarrollado por la Organización Internacional para la Estandarización (ISO) en 1984, y es considerado el modelo arquitectónico primario para las comunicaciones entre computadoras.

El modelo OSI clasifica todas las tareas involucradas con el intercambio de la información entre las computadoras conectadas en una red de datos en siete grupos más pequeños, y manejables. Una tarea o grupo de tareas se asignan entonces a cada una de las siete capas del modelo OSI. Dado que cada capa es bastante autónoma, las tareas asignadas a cada capa pueden llevarse a cabo independientemente, esto sirve para cuando se tengan actualizaciones de una capa estas puedan ser habilitadas sin afectar otras funciones de las otras capas.

Las siete capas del modelo OSI se muestran en la figura I.21.

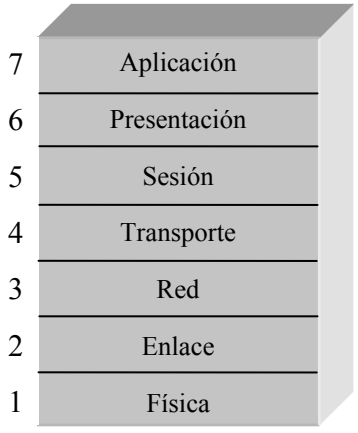


Figura I.21 *El modelo OSI contiene 7 capas independientes.*

I.9.1 CARACTERISTICAS DEL MODELO OSI

Las siete capas del modelo OSI se dividen en dos categorías: las capas superiores y las capas inferiores.

Las capas superiores del modelo OSI se ocupan de la aplicación final de los datos y generalmente se llevan a cabo en el software. La capa más alta, la capa de la aplicación, esta relacionada con el usuario final. Los usuarios y procesos de la capa de aplicación actúan recíprocamente con aplicaciones del software que contienen un componente de comunicaciones. El término de la capa superior a veces también se refiere a alguna capa sobre alguna otra capa en el modelo de OSI.

Las capas inferiores del modelo OSI están más relacionadas con los problemas del transporte de datos. La capa física y la capa de enlace se llevan a cabo tanto en el hardware como en el software. La capa más baja, la capa física, es la encargada del medio físico de la red (cableado de la red, por ejemplo) y es responsable de poner la información sobre el medio.

La Figura I.22 ilustra la división entre las capas de OSI

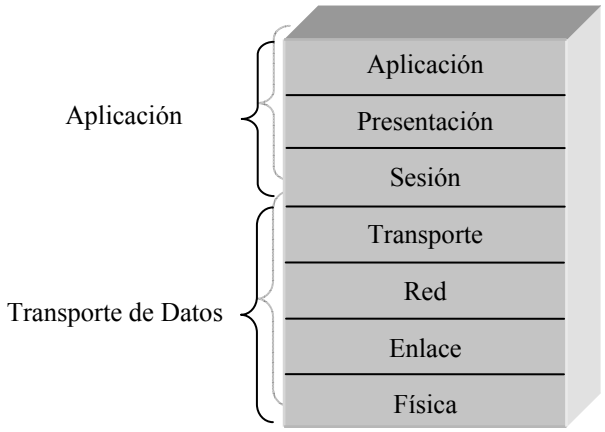


Figura I.22 *Dos juegos entrelazados de capas superiores del modelo OSI*

I.9.2 PROTOCOLOS

El modelo OSI mantiene un armazón conceptual para la comunicación entre las computadoras, pero el propio modelo no es un método de comunicación. La comunicación real es posible cuando se usan los protocolos de comunicación.

En el contexto de una red de datos, un protocolo es un conjunto formal de reglas y convenciones que gobiernan la manera de como las computadoras intercambian la información sobre un medio de la red. Un protocolo generalmente lleva a cabo las funciones de una o más de las capas del OSI.

Existe una gran variedad de protocolos de comunicación. Algunos de estos incluyen protocolos LAN, protocolos WAN, los protocolos de la red y protocolos de ruteo. Los protocolos LAN operan sobre las capas física y de enlace del modelo OSI, y definen la comunicación de los diferentes medios LAN. Los protocolos WAN operan en las tres capas más bajas del modelo OSI y definen la comunicación de los diferentes medios de área amplia.

Los protocolos de rueto son protocolos de la capa de red que son responsables de intercambiar la información entre los ruteadores, así los ruteadores puedan seleccionar el camino más apropiado para el tráfico de la red. Finalmente, los protocolos de red son los protocolos de la capa superior que existen en una colección protocolar dada. Muchos protocolos confían en otros para su funcionamiento. Por ejemplo, muchos protocolos de ruteo usan los protocolos de red para intercambiar la información entre los ruteadores. Este concepto de trabajar sobre las otras capas es la base del funcionamiento del modelo OSI.

I.9.3 MODELO OSI Y LA COMUNICACIÓN ENTRE SISTEMAS

La información que se transfiere de una aplicación del software en un sistema de la computadora a una aplicación del software en otro, debe atravesar las capas del modelo OSI.

Por ejemplo, si una aplicación del software en el sistema A necesita transmitir la información a una aplicación del software en el sistema B, el programa de la aplicación en el sistema A pasará su información a la capa de aplicación (Capa 7) del sistema A. La capa de aplicación entonces pasa la información a la capa de presentación (Capa 6) después pasa los datos a la capa de sesión (Capa 5), y así sucesivamente hasta la capa física (Capa 1). En la capa física, la información se pone en el medio físico de la red y se envía por el medio al sistema B. La capa física del sistema B toma la información del medio físico, y entonces su capa física pasa la información a la siguiente, capa de enlace (Capa 2) la cual pasa esta información a la capa de red (Capa 3), y así sucesivamente, hasta que alcance la capa de aplicación (Capa 7) del sistema B.

Finalmente, la capa de aplicación del sistema B pasa la información al programa de aplicación de destinatario para completar el proceso de comunicación.

I.9.4 INTERACCION ENTRE CAPAS

Una capa dada en el modelo de OSI generalmente se comunica con otras tres capas del modelo OSI: la capa que esta directamente sobre él, la capa que esta directamente debajo de él, y su capa par en otros sistemas de computadoras conectadas a una red.

Por ejemplo la capa de enlace en el Sistema A, se comunica con la capa de red del Sistema A, la capa física del Sistema A, y la capa de enlace en el Sistema B, como se ilustra en la figura I.23.

I.9.5 SERVICIOS DE CAPA

Toda capa del modelo OSI se comunica con sus capas adyacentes para hacer uso de los servicios proporcionados por estas. Los servicios proporcionados por las capas adyacentes ayudan a una capa del modelo OSI a comunicarse con su capa par de otros sistemas de computadoras.

En esta comunicación hay tres elementos básicos que se encuentran envueltos en los servicios de cada capa: el usuario de servicio, el proveedor de servicio, y el Punto de Acceso de Servicio (SAP *Server Access Point* por sus siglas en ingles). En este contexto, el usuario de servicio es la capa del modelo OSI que pide los servicios de alguna de sus capas adyacentes y el proveedor de servicio es la capa del modelo OSI que proporciona los servicios a los usuarios de servicio.

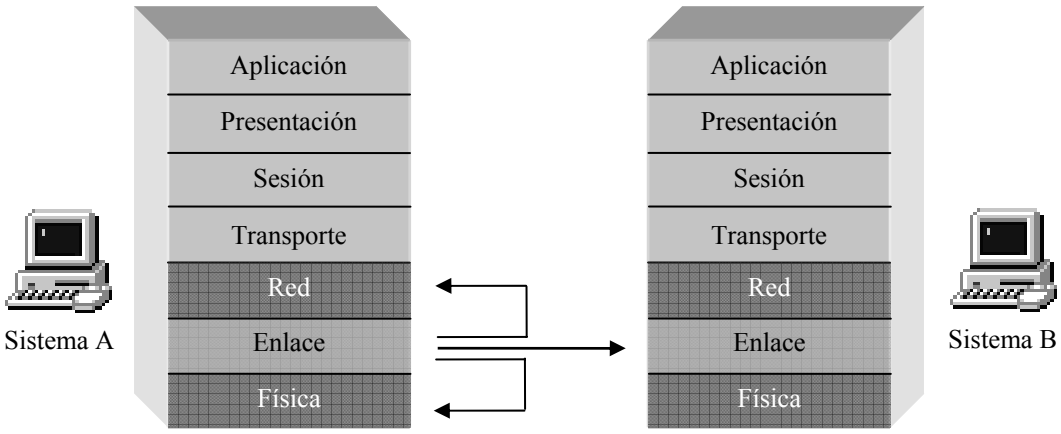


Figura I.23 *Capas del modelo OSI comunicándose con otras capas.*

Las capas del modelo OSI pueden proporcionar servicios a varios usuarios de servicios. Los SAP son solo una situación conceptual en la cuál una capa del modelo OSI puede pedir los servicios de otra capa del modelo OSI.

La figura I.24 ilustra cómo estos tres elementos actúan recíprocamente en las capas de red y de enlace.

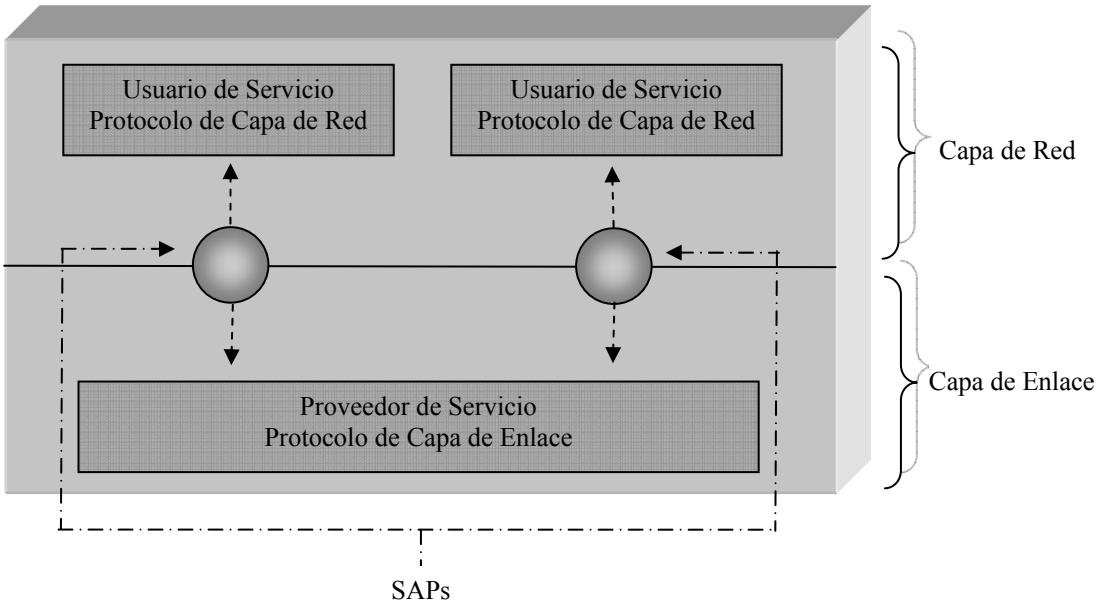


Figura I.24 *Usuarios de servicio, proveedores, interacción con la red y enlace de capas*

I.9.6 CAPAS DEL MODELO OSI E INTERCAMBIO DE INFORMACIÓN

Las siete capas del modelo OSI usan varias formas de información de control para comunicarse con su capa par de otras computadoras. Esta información de control consiste en peticiones e instrucciones específicas que se intercambian entre las capas del modelo OSI.

Típicamente la información de control toma una de las siguientes dos formas: encabezados ó colas. Los encabezados son los precedentes a los datos, los cuales han pasado a las capas inferiores de las capas superiores y las colas son añadidas a los datos que igualmente han pasado a las capas inferiores de las capas superiores.

Hay que destacar que una capa inferior del modelo OSI no requiere agregar un encabezado o una cola como información de control a los datos para las capas

superiores, es decir que los encabezados o colas van siendo agregados solo por las capas superiores y no al revés.

Los encabezados, colas, y datos solo son conceptos relativos, dependiendo de la capa que analiza la unidad de información. En la capa de red, por ejemplo, una unidad de información consiste en el encabezado de capa 3 y sus datos. Por otro lado, toda la unidad de información que se genera en la capa de red, es enviada hacia la capa de enlace y es tratada como datos de esta, por lo que a su vez se le debe asignar un encabezado o una cola para conformar la trama de la capa de red. En otras palabras, cualquier porción de datos de una unidad de información puede contener, encabezados, colas y datos de todas las capas superiores del modelo OSI. A este proceso se le conoce como encapsulamiento.

De acuerdo a las convenciones utilizadas por algunos fabricantes de equipo de redes, a la unidad de información correspondiente a la capa 1 (Capa física) se le denomina simplemente como "bits"; en cambio para el caso de la capa 2 (Capa de enlace), la unidad de información compuesta por un encabezado y/o cola se le denomina como "trama" (o *frame* en inglés), de igual manera en el caso de la información que transporta las reglas y los procesos de capa 3 (Capa de red) se le denomina "paquete" y el termino utilizado para las unidades de información de capa 4 (Capa de transporte) se le denomina "segmento".

La figura I.25 muestra cómo el encabezado y los datos de una capa superior son encapsulados dentro del encabezado de la siguiente capa inferior, así como los nombres que se le asigna a cada una de las unidades de información de cada capa.

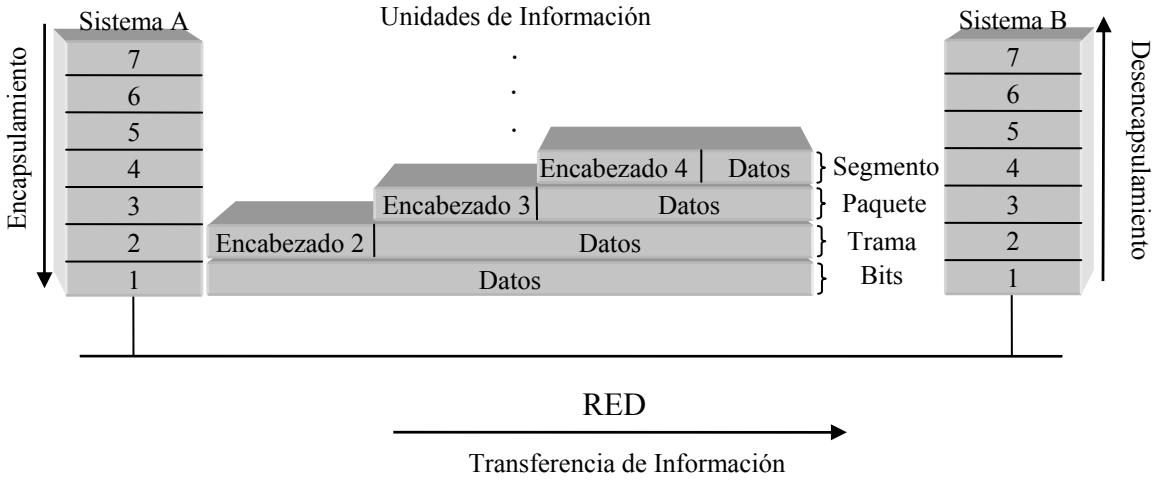


Figura I.25 *Proceso de encapsulamiento de información*

I.9.7 PROCESO DE INTERCAMBIO DE INFORMACIÓN

El proceso de intercambio de información ocurre entre dos capas pares del modelo OSI. Cada capa del sistema fuente agrega información de control a los datos, y cada capa en el sistema del destino analiza y quita la información de control de esos datos.

Si el sistema A tiene datos de una aplicación de software que desea enviar al Sistema B, estos datos se pasan a la capa de la aplicación. La capa de aplicación en el Sistema A entonces necesita comunicar cualquier información de control requerida por la capa de aplicación en el Sistema B, y esto lo hace añadiendo un encabezado a los datos. Así la unidad de información resultante (un encabezado y los datos) se pasa a la capa de la presentación que añade su propio encabezado que contiene la información de control que necesita la capa de presentación en el Sistema B. La unidad de información va creciendo en tamaño debido a que cada capa agrega su propio encabezado (y, en algunos casos, una cola) el cual contiene información de control que será usada por su capa par en el Sistema B. Una vez finalizado el proceso de encapsulamiento, la capa física del sistema A es la encargada de poner dentro del medio de la red toda la unidad de información ("bits") para que lleguen a su destino en el sistema B.

Una vez que la capa física del Sistema B recibe la unidad de información, esta la pasa a la capa de enlace. La capa de enlace en el Sistema B lee la información de control contenida en el encabezado añadido por la capa de enlace del sistema A. El encabezado es entonces removido y el resto de la unidad de información se pasa a la capa de la red. Cada capa realiza las mismas acciones: La capa lee el encabezado de su capa, y pasa la unidad de información restante a la siguiente capa más alta. Después de que la capa de la aplicación realiza estas acciones, los datos se pasan a la aplicación de software del destinatario en el Sistema B, en la misma forma en que se transmitió por la aplicación en el Sistema A.

A continuación se tratarán con detalle cada una de las funciones de las 7 capas que componen el modelo de referencia OSI.

I.9.8 CAPA FÍSICA

La Capa Física define las especificaciones eléctricas, mecánicas, procesales, y funcionales para activar, mantener y desactivar la conexión física entre los sistemas de la red.

Las especificaciones técnicas de la capa física definen características como son los niveles de voltaje, tiempos de cambio de voltaje, las tasas de datos físicos, máxima distancia para la transmisión y los conectores físicos. Las aplicaciones de la capa física pueden categorizarse también dentro de las especificaciones para las LAN o WAN.

En la figura I.26 se ilustran algunas aplicaciones comunes de la capa física para LAN y WAN.

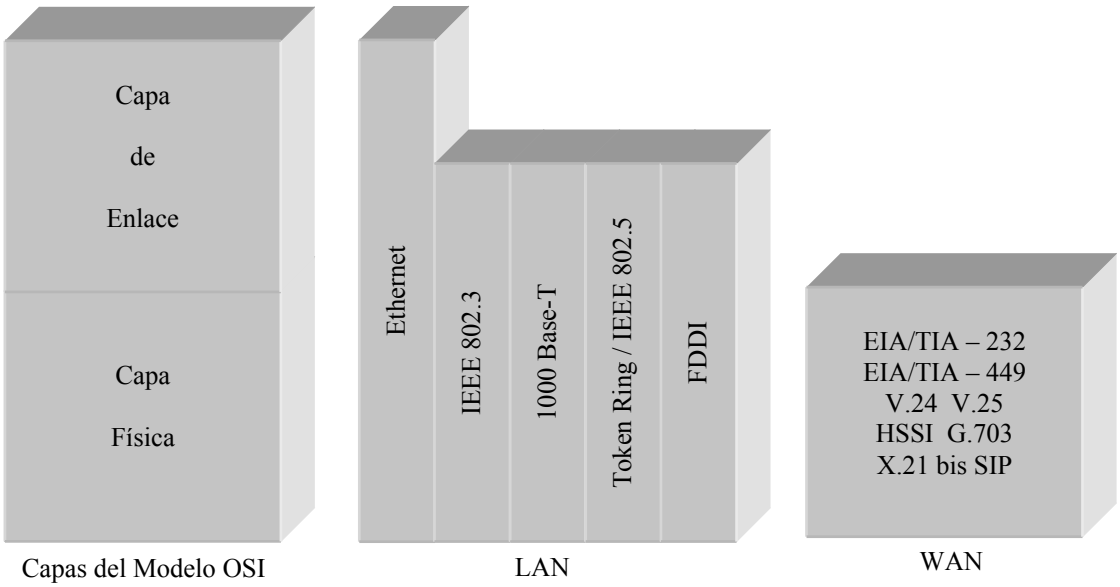


Figura I.26 *Las aplicaciones de la capa física pueden tener especificaciones LAN o WAN*

I.9.9 CAPA DE ENLACE

La Capa de Enlace proporciona el tránsito fiable de los datos a través de la conexión física de la red. Las diferentes especificaciones de la capa de enlace definen diferentes características y protocolos de la red, incluyendo el direccionamiento físico, la topología de la red, la notificación de errores, la secuencia de las tramas y control de flujo. Sus funciones son las siguientes:

- El direccionamiento físico define el cómo los dispositivos son direccionados en la capa de enlace.
- La topología de la red puntualiza las especificaciones que a menudo definen la manera en que los dispositivos son conectados físicamente, como es el ejemplo de una topología bus o una topología anillo.

- La notificación de errores, alerta a los protocolos de capas superiores que ha ocurrido un error en la transmisión.
- La secuencia de las tramas reordenar las tramas que son enviadas fuera de esta.
- El control de flujo regula la transmisión de datos para que el dispositivo receptor no se sature con un tráfico mayor del que puede manejar a la vez.

El Instituto de Ingeniería Eléctrica y Electrónica (IEEE) subdivide la capa de enlace en dos subcapas: Control de Enlace Lógico (LLC *Logical Link Control*) y Control de Acceso al Medio (MAC *Media Acces Control*). La figura I.27 ilustra las subcapas de la IEEE de la capa de enlace.

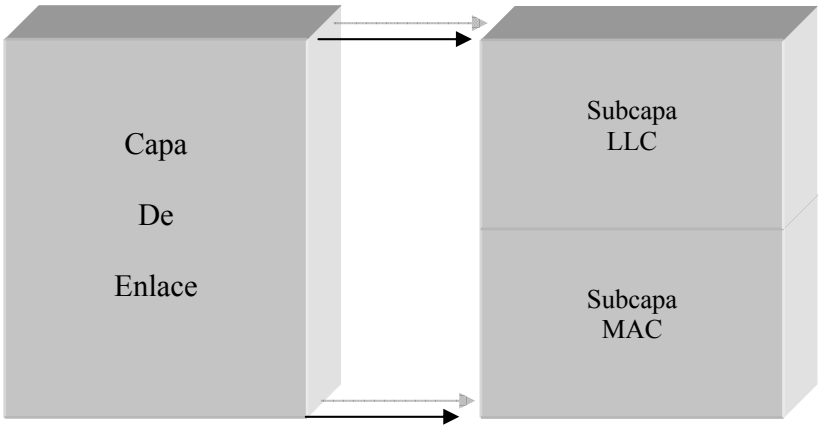


Figura I.27 *La capa de enlace contiene dos subcapas*

El Control de Enlace Lógico (LLC) es la subcapa que se encarga de manejar las comunicaciones entre los dispositivos sobre un solo enlace de red. Las especificaciones de la subcapa LLC se encuentran definidas dentro del estándar IEEE 802.2, y la cual soporta tanto los servicios orientado a conexión y no orientado a conexión usados por los protocolos de capa superior.

El estándar IEEE 802.2 define un número campos que van en la trama de la capa de enlace, los cuales permiten a los protocolos de capa-superior compartir un solo enlace físico. El Control de Acceso al Medio (MAC) es la subcapa de la capa de enlace que maneja el acceso protocolar al medio físico de la red. La especificación de la IEEE MAC define direcciones de MAC las cuales permiten la identificación de los dipositivos de red de manera única dentro de la capa de enlace.

I.9.10 CAPA DE RED

La Capa de Red define la manera como se transporta el tráfico entre dispositivos que no se encuentran interconectados de manera local. Para lograr esto, la capa de red hace uso de dos elementos de información básicos:

- Asociación de direcciones lógicas, tanto la estación fuente como la estación destino.
- Definición de rutas a través de la red que permitan alcanzar los destinos deseados.

De igual manera, se definen dos tipos fundamentales de paquetes en la capa de red:

1. Paquetes de datos; los cuales incluyen los datos del usuario y la información de control apropiada para capas superiores.

2. Paquetes para descubrimiento y actualización de rutas. Este tipo de paquetes son enviados y recibidos por dispositivos de capa 3 llamados comúnmente ruteadores. Los ruteadores (o enrutadores) son responsables de rastrear que redes existen y como llegar a ellas. Los paquetes de actualización de rutas contienen información acerca de cada red dentro de un entorno de redes definido (a veces denominado como Internetwork), la ruta que se debe seguir para alcanzar cada red y el costo o distancia (definidos mediante métricas) que existe entre la red de origen y la red de destino.

Para poder determinar que redes existen en una Internetwork, y en donde se encuentran dichos dispositivos en el contexto de esas redes, se utilizan esquemas de direccionamiento lógico. Estos esquemas varían dependiendo del protocolo de capa de red utilizado. Algunos de los más comunes y que serán estudiados con más detalle en capítulos posteriores de este trabajo son los basados en IP e IPX.

I.9.11 CAPA DE TRANSPORTE

La Capa de Transporte acepta datos de la capa de sesión y segmenta dichos datos para que sean transportados a través de la red. Generalmente, la capa de transporte es la responsable de asegurarse que los datos sean entregados libres de errores y en la secuencia apropiada, además también es responsable de realizar tareas de control de flujo.

El control de flujo maneja la transmisión de datos entre dispositivos, esto con el fin de que los dispositivos de transmisión no envíen más datos de los que el dispositivo receptor pueda procesar. La multiplexación, permite que los datos provenientes de varias aplicaciones puedan ser transmitidos dentro de un único enlace físico.

La capa de transporte también es la encargada de establecer, mantener y terminar circuitos virtuales. La verificación de errores implica, la creación de varios mecanismos para la detección de errores de transmisión, mientras que en la recuperación de errores, se toman acciones tales como peticiones para que los datos sean retransmitidos para resolver cualquier error que ocurra. Los protocolos de transporte utilizados en Internet son el TCP[1] y UDP[2]

I.9.12 CAPA DE SESIÓN

La Capa de Sesión, establece, administra y termina las sesiones de comunicación. Las sesiones de comunicación consisten en peticiones de servicios y respuestas de dichos servicios que ocurren entre aplicaciones localizadas en diferentes dispositivos de red. Estas peticiones y respuestas son coordinadas por protocolos implementados en la capa de sesión. Algunos ejemplos de la implementación de la capa de sesión incluyen el Protocolo de Información de Zona (ZIP *Zone Information Protocol*), el Protocolo Apple Talk que coordina el nombre vinculado a un proceso; y el Protocolo de Control de Sesión (SCP *Session Control Protocol*).

I.9.13 CAPA DE PRESENTACIÓN

La Capa de Presentación provee una variedad de funciones para codificar y convertir los datos que serán llevados a la capa de aplicación, estas funciones aseguran que la información enviada desde la capa de aplicación de un sistema sea entendible por la capa de aplicación de otro sistema. Algunos ejemplos del esquema de codificación y conversión de la capa de presentación, incluyen formatos de representación de datos comunes, formatos de representación de conversión de caracteres, esquemas de compresión de datos comunes, y esquemas de encriptación de datos comunes.

Los formatos de representación de datos convencionales, o el uso de imágenes, sonido y formatos de video estándares, permiten el intercambio de aplicaciones de

[1] TCP : Protocolo de Control de Transmisión *(Transmission Control Protocol)*
[2] UDP: Protocolo de Datagrama de Usuario (User Datagram Protocol)

datos entre diferentes tipos de sistemas de computadoras. Los esquemas de conversión son utilizados para intercambiar información con sistemas que utilizan diferentes representaciones de texto y datos, tales como EBCDIC[1] y ASCII[2]. Los esquemas de compresión de datos estándar permite que los datos comprimidos por el dispositivo fuente, sean apropiadamente descomprimidos por el dispositivo destino, y los estándares de esquemas de encriptación de datos, permiten la encriptación de datos por el dispositivo fuente para ser apropiadamente desencriptado por el dispositivo destino.

Las implementaciones de la capa de presentación no son típicamente asociadas con una pila de protocolos en particular. Algunos de los estándares conocidos para video son: el QuickTime y el MPEG (*Motion Picture Experts Group*). El Quick Time es una especificación de Apple para video y audio, y el MPEG es un estándar para compresión y codificación de video.

Entre los formatos más conocidos de imágenes están: el Formato de Intercambio de Gráficos (GIF *Graphics Interchange Format*), el de Unión Fotográfica de Grupo de Expertos (JPEG *Joint Photographic Experts Group*), y el Formato Etiquetado de Archivo de Imagen (TIFF *Tagged Image File Format*). Los cuales son estándares de codificación y compresión de imágenes.

I.9.14 CAPA DE APLICACIÓN

La Capa de Aplicación es la capa del modelo OSI más cercana al usuario final, lo cual significa que tanto la capa de aplicación del modelo OSI y el usuario interactúan directamente con el software de aplicación. Esta capa es la encargada de interactuar con aplicaciones de software que llevan acabo alguna comunicación. Hay que destacar que tales programas de aplicación caen fuera del alcance del modelo OSI.

Las funciones de la capa de aplicación típicamente incluyen la identificación de comunicaciones asociadas, la determinación de disponibilidad de recursos, y la sincronización de comunicación. Cuando son identificadas comunicaciones asociadas, la capa de aplicación determina la identidad y la disponibilidad de las comunicaciones asociadas por una aplicación con datos a transmitir. Cuando se determinan los recursos disponibles, la capa de aplicación debe decir si son suficientes los recursos de red para que exista la petición de comunicación. En una comunicación sincronizada, toda la comunicación entre aplicaciones requiere de

[1] EBCDIC: Código Binario Extendido para Intercambio a Código Decimal *(Extended Binary Coded Decimal Interchange Code)*

[2] ASCII: *Código* Americano Estándar para Intercambio de Información (American Standard Code for Information Interchange)

cooperación, la cual es administrada por la capa de aplicación. Algunos ejemplos de la implementación de la capa de aplicación incluyen: Telnet, FTP "Protocolo de Transferencia de Archivos" (*File Transfer Protocol*), SMTP "Protocolo de Transferencia de Correo Simple" (*Simple Mail Transfer Protocol*).

I.9.15 UNIDADES DE INFORMACIÓN

Los datos y control de información que son transmitidos a través de las redes toman una variedad de formas. Los términos utilizados para referirse a estas unidades de información no son utilizados consistentemente en la industria de redes y algunas veces son intercambiados. Las unidades de información incluye tramas, paquetes, datagramas, segmentos, mensajes, celdas y unidades de datos.

Una ***trama*** es una unidad de información asociada a la capa de enlace en la cual se incluye el origen y destino. Una trama esta compuesta de un encabezado de la capa de enlace (y posiblemente una cola) y datos de capas superiores. El encabezado y la cola, contienen información de control la cual es entendida por la capa de enlace en el sistema destino. Los datos provenientes de capas superiores son encapsulados en la capa de enlace y colocados en el encabezado y cola.

La figura I.28 ilustra los componentes básicos de la trama de la capa de enlace.

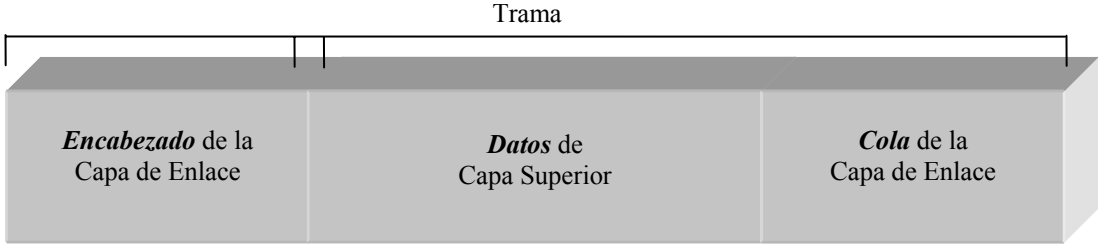


Figura I.28 *La figura ilustra los componentes básicos de una trama (frame) de la capa de enlace.*

Un ***paquete*** es una unidad de información cuya fuente y destino son asociados de la capa de red. Un paquete esta compuesto de un encabezado de la capa de red (y posiblemente una cola) y datos de capas superiores. El encabezado y la cola contienen información de control entendida por la capa de red del sistema destino. Los datos provenientes de capas superiores están encapsulados en el encabezado y la cola de la capa de red.

La figura I.29 ilustra los componentes básicos de un paquete de la capa de red.

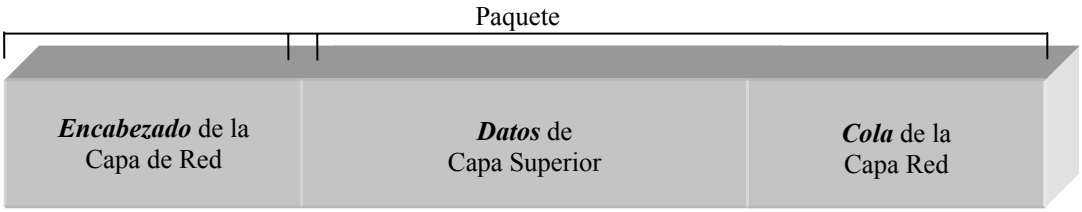


Figura I.29 *Componentes Básicos de un paquete de la Capa de Red*

El termino ***datagrama*** usualmente se refiere a una unidad de información cuyo origen y destino son asociados a la capa de red, las cuales utilizan servicios de red no orientados a conexión, el termino segmento usualmente se refiere a una unidad de información cuyo origen y destino son asociados a la capa de transporte, un ***mensaje*** es una unidad de información cuyo origen y destino asociado a las capas superiores de capa de red (frecuentemente a la capa de aplicación), y finalmente una ***celda*** es una unidad de información de tamaño fijo cuyo origen y destino son asociados a la capa de enlace.

Las celdas son utilizadas en ambientes conmutados, tales como ATM Modo de Transferencia Asíncrono (*Asynchronous Transfer Mode*) y redes SMDS Servicio de Datos Multimegabit Conmutado (*Switched Multimegabit Data Service*). Una celda esta compuesta de un encabezado y carga útil (*payload)*. El encabezado contiene información de control la cual es entendida por la capa de enlace del sistema destino y es su tamaño es de 5 bytes típicamente. La carga útil contiene datos de capas superiores que son encapsulados en la celda, la cual tiene una longitud de 48 bytes típicamente. La longitud de los campos del encabezado y carga útil siempre son los mismos para cada celda.

La figura I.30 muestra los componentes típicos de una celda

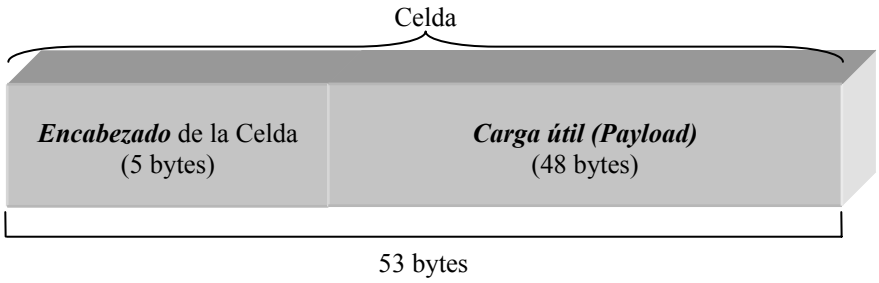


Figura I.30 *Componentes que Constituyen una Célula Típica*

Por último una ***unidad de datos*** es un término genérico que se refiere a una variedad de unidades de información. Algunas unidades de datos comunes son las

Unidades de Datos de Servicios (SDUs *Service Data Units*), unidades de protocolos de datos, y las Unidades de Datos de Protocolo Puente (BPDUs Bridge Protocol Data Units). Los SDUs son unidades de información provenientes de protocolos de capas superiores que definen una petición de servicio a un protocolo de capa inferior. El Protocolo de Unidad de Datos (PDU *Protocol Data Unit*) es la terminología que usa OSI a un paquete y las Unidades de protocolo puente (BPDU *Bridge Protocol Data Unit*) son utilizadas por el algoritmo *spanning-tree* como mensajes de hola.

II

TECNOLOGÍAS ACTUALES EN UNA RED DE DATOS

II.1 CAPA FÍSICA

La capa física del modelo de referencia OSI, define las especificaciones mecánicas, eléctricas y funcionales para activar, mantener y desactivar un enlace físico entre sistema de comunicación, tales como niveles de voltaje, sincronía, tasas de transmisión, distancias de conexión y conectores físicos.

II.1.1 SEÑALES ELÉCTRICAS

En esencia, las comunicaciones electrónicas se basan en la transmisión, recepción y procesamiento de información usando circuitos electrónicos. Toda la información debe convertirse a *energía electromagnética,* antes de que pueda propagarse por un sistema de comunicaciones electrónicas.

II.1.1.1 NATURALEZA DE LAS SEÑALES ELÉCTRICAS

Un sistema analógico es un sistema en el cual la energía electromagnética se transmite y recibe en forma analógica (una señal variando continuamente tal como una onda senoidal), asimismo un sistema digital es un sistema en el cual la energía electromagnética se transmite y recibe en forma digital (niveles discretos tal como +5 V y tierra). Los sistemas binarios utilizan señales digitales que solo tienen dos niveles discretos, frecuentemente la información de la fuente original está en una forma que no es la adecuada para la transmisión y debe convertirse en una forma mas adecuada antes de la transmisión.

Cuando la representación de un objeto es muy cercana a su forma original, se dice que esa representación es análoga o analógica, hoy en día en el ámbito de las comunicaciones de datos se utiliza el término analógico para referirse a una señal que está constantemente cambiando en proporción a lo que esta representa. Una señal analógica contiene muchos valores o niveles dentro de un cierto rango en forma continua, mientras que una señal digital, representa la información usando solo dos valores, por lo que se dice que una señal digital es discreta.

II.1.1.2 MENSAJES ANALÓGICOS Y DIGITALES

Los mensajes enviados a través de un sistema de comunicaciones electrónico, pueden clasificarse en analógicos o digitales; estos últimos se construyen con un número finito de símbolos, lo que comúnmente se conoce como mensaje M-ario.

Por otra parte los mensajes analógicos se caracterizan por contener datos cuyo valor varía en un rango continuo. En un intervalo de tiempo dato, existe un número infinito de formas de onda, en contraste con solo un número finito de mensajes digitales posibles.

Los mensajes digitales se trasmiten utilizando un conjunto finito de formas de onda eléctricas; en un caso M-ario, se utilizan M pulsos eléctricos distintos, cada uno de estos representa a uno de los M símbolos posibles. La tarea del receptor consiste en extraer un mensaje de una señal distorsionada y afectada por ruido a la salida del canal, la extracción del mensaje es más fácil en las señales digitales que en las señales analógicas, en consecuencia un sistema de comunicación digital puede transmitir mensajes con mayor exactitud que un sistema analógico en presencia de distorsión y ruido.

En contraste con los mensajes digitales, la forma de onda de los mensajes analógicos es importante, y aún una pequeña distorsión o interferencia en la forma

de onda ocasionará un error en la señal recibida. Como resultado, la distorsión y la interferencia por ruido son acumulativas a través de toda la trayectoria de transmisión. La señal se atenúa continuamente a lo largo del trayecto de transmisión, y entonces con el aumento de la distancia la señal se hace más débil, mientras que la distorsión y el ruido se hacen más grandes, finalmente, la señal queda mutilada. En estos casos la amplificación es de escasa ayuda, ya que acentúa la señal y el ruido en la misma proporción. En consecuencia la distancia a través de la cual se puede transmitir una señal analógica es limitada por la potencia del transmisor, por esa razón actualmente se están remplazando los sistemas analógicos por sistemas digitales.

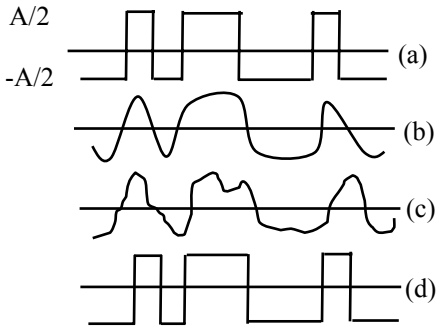


Figura II.1 *(a)señal trasmitida, (b) señal distorsionada recibida (sin ruido), (c) señal distorsionada recibida (con ruido), (d)señal regenerada (retardada)*

II.1.1.3 CONVERSIÓN ANALÓGICA A DIGITAL

Existe un punto de reunión de las señales analógicas y digitales: su conversión de analógicas a digitales (conversión A/D). El espectro de frecuencia de una señal indica las magnitudes relativas de las diferentes componentes de la frecuencia. El *teorema del muestreo* establece que si la frecuencia más alta del espectro de la señal es B (en Hz), la señal se puede reconstruir a partir de sus muestras, tomadas a una razón no menor que 2B muestras/segundo. Esto significa que para transmitir la información dentro de una señal continua, se necesita solamente transmitir sus muestras. Desafortunadamente, los valores de las muestras no son todavía digitales ya que se encuentran dentro de un rango continuo y pueden tomar cualquiera del número infinito de valores del rango. Esto se resuelve mediante lo que se conoce como *cuantiftcación,* en donde cada muestra se aproxima, o "redondea", al nivel cuantificado mas próximo. Las amplitudes de la señal $m(t)$ están dentro del rango, que se subdividen en L intervalos, cada uno de magnitud $\Delta y = 2m_p/L$. La magnitud de cada muestra se aproxima al punto medio del intervalo en el cual cae el valor de la muestra, cada muestra se aproxima ahora a uno de los L números, la información queda así digitalizada.

La señal cuantificada es una aproximación de la señal original. Se puede mejorar la exactitud de la señal cuantificada a cualquier grado que se desee aumentando el número de niveles (L).

II.1.1.4 RUIDO

En general el ruido eléctrico se define como cualquier energía eléctrica no deseada presente en la pasabanda útil de un sistema de comunicaciones, esencialmente, el ruido puede dividirse en dos categorías generales: correlacionado y no correlacionado. Correlación implica una relación entre la señal y el ruido, así mismo el ruido no correlacionado está presente en la ausencia de cualquier señal mientras que el correlacionado es producido directamente como resultado de la señal.

RUIDO NO CORRELACIONADO

Se encuentra presente sin importar si hay una señal o no, se puede dividir en dos categorías generales: externo e interno.

Ruido externo. Es generado externamente a un sistema y se introduce al mismo. Las señales externamente generadas se consideran ruido, solo si sus frecuencias caen dentro de la banda útil del filtro de entrada del sistema. Existen tres principales tipos de ruido externo: atmosférico, extraterrestre y el hecho por el hombre.

Ruido interno. Es la interferencia eléctrica generada dentro de un dispositivo. Existen generalmente tres tipos de ruido generados internamente: térmico, de disparo y tiempo de tránsito.

RUIDO CORRELACIONADO

Es una energía eléctrica no deseada que esta presente como un resultado directo de una señal, tales como las distorsiones armónicas y de intermodulación, ambas son formas de distorsión no lineal. El ruido correlacionado no puede estar presente en un sistema a menos que exista una señal de entrada. Las distorsiones armónica y de intermodulación cambian la forma de onda en el dominio del tiempo y el contenido espectral en el dominio de la frecuencia.

LA RELACIÓN SEÑAL A RUIDO

Es una relación matemática sencilla del nivel de la señal con respecto al nivel del ruido en un punto dado del sistema. La relación señal a ruido puede expresarse como una relación de voltaje y una relación de potencia, matemáticamente, S/N es:

$$\frac{S}{N} = \left[\frac{voltajedelaseñal}{voltajedelruido}\right]^2 = \left(\frac{V_S}{V_n}\right)^2 \quad \text{como una relación de voltaje (II.1)}$$

$$\frac{S}{N} = \left[\frac{potenciadelaseñal}{potenciadelruido}\right]^2 = \frac{Ps}{Pn} \quad \text{como una relación de potencia (II.2)}$$

De la relación señal a ruido, se puede determinar la calidad general de un sistema.

II.1.2 CAPACIDAD DE CANAL Y SISTEMAS DE COMUNICACIÓN IDEALES

Se pueden usar muchos criterios para evaluar una eficacia en un sistema de comunicaciones para ver si es ideal o perfecto. Algunos de estos criterios son el costo, el ancho de banda del canal utilizado, la potencia del transmisor requerida y la demora a través del sistema.

En sistemas digitales, el sistema óptimo se podría definir como aquel que reduce al mínimo la probabilidad de error de bit en la salida del sistema, sujeta a limitaciones sobre la energía transmitida y el ancho de banda del canal, por eso los errores en los bits y el ancho de banda de la señal son de primordial importancia. En 1948-1949 Claude Shanon demostró que (en el caso de señal mas ruido blanco gaussiano) la capacidad de un canal C (bits/s) se podría calcular de tal modo que si la velocidad de transferencia de la información R (bits/s) fuera menor que C, la probabilidad de errores en los bits tendería a cero. La ecuación para C es.

$$C = B\log_2\left(1 + \frac{S}{N}\right) \quad \text{(II.3)}$$

donde B es el ancho de banda del canal en Hz y S/N es la relación de la potencia de la señal a ruido (watts/watts, no dB) en la entrada del receptor digital. Shanon no explicó como se construye este sistema, pero demostró que es teóricamente posible construir un sistema como ese. De este modo, Shanon señaló una meta de rendimiento teórico que hay que tratar de lograr con sistemas de comunicación prácticos. Los sistemas que se aproximan a esta meta por lo general incorporan

codificación de corrección de errores. El ruido presente en el canal continúa provocando errores a la entrada del decodificador receptor.

En sistemas analógicos, se podría definir el sistema óptimo como aquel que logra la relación de señal a ruido mas grande en la salida del receptor sujeta a limitaciones de diseño, tales como el ancho de banda del canal y la potencia transmitida.

Nyquist en 1924 y Hartley en 1928 descubrieron otras limitaciones fundamentales para la transmisión de señales digitales, si un pulso representa un bit de datos. Nyquist demostró que se podían enviar pulsos no interferentes a través de un canal a una velocidad no mayor que 2B pulsos/s, donde B es el ancho de banda del canal en Hz. Hartley generalizó el resultado de Nyquist para el caso de transmisión de señales por pulsos de varios niveles.

II.1.3 TECNOLOGÍAS DE COBRE

II.1.3.1 MEDIOS DE TRANSMISIÓN

La conexión física entre dispositivos que integran una red de datos puede implementarse de muy diversas formas, que van desde el uso del par de cobre diseñado para las comunicaciones de redes de datos, hasta la fibra óptica. A continuación se detallan las características de los medios de transmisión así como sus usos más comunes en el área de redes para cobre.

II.1.3.2 ALAMBRE (OPEN-WIRED)

Hoy en día los cables vienen protegidos con algún material aislante. El material del conductor puede ser de cobre, aluminio u otros materiales conductores.

Los grosores de los cables son medidos de diversas maneras, el método predominante en los Estados Unidos sigue siendo el Wire Gauge Standard (AWG), "gauge" significa el diámetro, es lógico pensar que a mayor diámetro del conductor mayor será la resistencia del mismo.

Los conductores pueden ser de dos tipos ***Sólidos*** e ***Hilados***, los conductores sólidos están compuestos por un conductor único de un mismo material, mientras que los conductores hilados están compuestos de varios conductores trenzados. El diámetro de un conductor hilado varía al de un conductor sólido si son del mismo AWG y dependerá del número de hilos que tenga.

Los grosores típicos de los conductores utilizados en cables eléctricos para uso residencial son del 10-14 AWG. Los conductores utilizados en cables telefónicos pueden ser del 22,24 y 26 AWG. Los conductores utilizados en cables para aplicaciones de redes son el 24 y 26 AWG.

A continuación se muestra una tabla de conversión de milímetros y pulgadas a AWG para conductores sólidos.

Diametro mm	Diametro pulgadas	AWG
0.254	0.010	30
0.330	0.013	28
0.409	0.016	26
0.511	0.020	24
0.643	0.025	22
0.812	0.032	20
1.020	0.040	18
1.290	0.051	16
1.630	0.064	14
2.050	0.081	12
2.590	0.102	10

Tabla II.1 *Tabla de Conversión Milímetros y Pulgadas a AWG (conductores sólidos)*

Entre mas grande sea el valor AWG menor será el grosor o diámetro del conductor. El conductor 18 tiene más grosor que el cable 40, por ejemplo. Los primeros 5 cables [de izquierda a derecha] son sólidos y los últimos dos son hilados o trenzados (stranded).

II.1.3.3 PAR TRENZADO

El par trenzado consiste en alambre de cobre ordinario que es enroscado en pares para reducir la inducción electromagnética. Cada alambre tiene su propio aislante. Dado que es común el requerimiento de más de un par trenzado para comunicar dispositivos, es usual que muchos pares sean construidos dentro de un mismo cable. La implementación más común en redes de datos es la llamada UTP[1], que consiste de cuatro pares trenzados con una impedancia de 100 ohms. Otra implementación es la STP[2] de una impedancia de 150 ohms. Los pares que vienen en un solo cable son

[1] UTP *Unshield Twisted Pair* (Par trenzado sin escudo)
[2] STP *Shielded Twisted Pair* (Par trenzado con escudo)

identificados por un código de color.

APLICACIÓN EN ETHERNET

El par trenzado es usado en las siguientes implementaciones físicas de ethernet: 10baseT, 100baseT, 100baseT4 y 1000baseTx.

10baseT. Opera a 10 Mbps usando cable UTP. La distancia entre dispositivos no debe ser mayor a 100 metros, todos ellos conectados a un repetidor central, que puede ser un HUB o un switch. Los conectores usados son RJ-45 .

Especificaciones para 10base T:

Tipo de cable:	UTP con dos pares trenzados de 22, 24 o 26 AWG.
Vueltas por pie:	2 o 3
Impedancia Nominal:	100 ohms
Longitud máxima del cable:	100 m
Máxima tasa de transmisión:	10 Mps

100baseT. Implementación física de ethernet que usa cable UTP o STP categoría 5 y que opera a 100Mbps. Usa la misma configuración física que 10baseT.

100baseT4. Implementación de ethernet que usa cable UTP categoría 3 y que opera a 100Mbps. A diferencia de 100baseT, 100baseT4 usa 4 pares trenzados para la transmisión de datos. Usa la misma configuración física que 10baseT.

Existen dos tipos de cable par trenzado, el UTP[1], o cable par trenzado sin blindaje y el cable STP[2], o cable par trenzado blindado.

[1] UTP Cable de Par Trenzado sin Coraza *(Unshielded Twisted Pair Cabling)*
[2] STP Cable de Par Trenzado Acorazado *(Shielded Twisted Pair Cabling)*

CABLE UTP

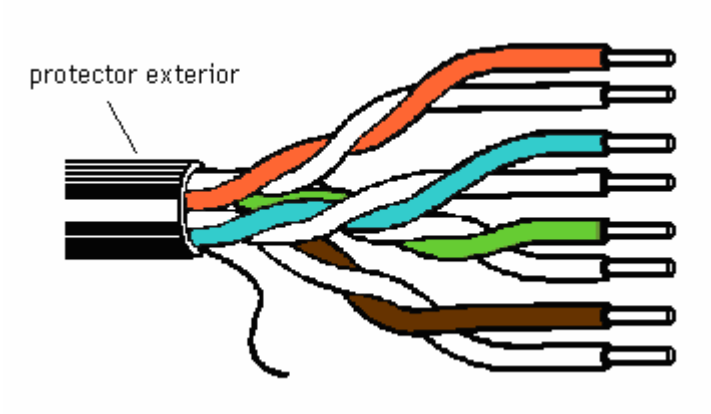


Figura II.2 *Cable UTP 4 pares*

Como el nombre lo indica, "unshielded twisted pair" (UTP), es un cable que no tiene revestimiento o blindaje entre la cubierta exterior y los cables, el UTP se utiliza comúnmente para aplicaciones de redes Ethernet; el témino UTP generalmente se refiere a los cables categoria 3, 4 y 5 especificados por el estándar TIA/EIA 568-A standard. Las categorias 5e, 6, & 7 han sido propuestos para soportar velocidades más altas. El cable UTP comúnmente incluye 4 pares de conductores. 10BaseT, 10Base-T, 100Base-TX, y 100Base-T2 y sólo utilizan 2 pares de conductores, mientras que 100Base-T4 y 1000Base-T requieren de todos los pares. A continuación se lista un sumario de los tipos de cable UTP

Tipo	Uso
Categoria 1	Voz solamente (cable telefónico)
Categoria 2	Datos hasta 4 Mbps (LocalTalk [Apple])
Categoria 3	Datos hasta 10 Mbps (Ethernet)
Categoria 4	Datos hasta 20 Mbps (16 Mbps Token Ring)
Categoria 5	Datos hasta 100 Mbps (Fast Ethernet)

Tabla II.2 *Categorías de cable UTP*

CABLE STP

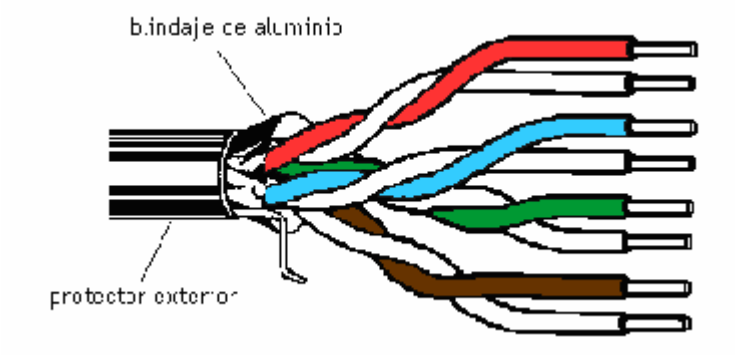


Figura II.3 *Cable STP 4 pares*

El cable STP, tiene un blindaje especial que forra a los 4 pares y comúnmente se refiere al cable par trenzado de 150 ohm definido por IBM utilizado en redes Token Ring. El blindaje está diseñado para minimizar la radiación electromagnética y la diafonía; los cables STP de 150 ohm no se usan para Ethernet, sin embargo, puede ser adaptado a 10Base-T, 100Base-TX, and 100Base-T2 Ethernet instalando un convertidor de impedancias que convierten 100 ohms a 150 ohms de los STPs.

La longitud máxima de los cables de par trenzado están limitadas a 90 metros, ya sea para 10 o 100 Mbps.

CABLEADO PARA REDES

El proceso se inicia con la selección del nivel de cable o categoría. Actualmente se usa Categoría 6 - **Unshielded Twister Pair UTP** o **UTPC6** o superior**.**

Contiene 4 pares de cables trenzados contenidos en una vaina de PVC y se identifican por colores

Función Pines/Colores Normalizados

PIN	Func.	Color
1	Tx+	
2	Tx-	
3	Rx+	
4	N/U	
5	N/U	
6	Rx-	
7	N/U	
8	N/U	

Figura II.4 *Función Pines/Colores Normalizados*

Este cable funciona con 10Base-T y 1000Base-T y es usado para conectar tarjetas de red a HUBS o Switches.

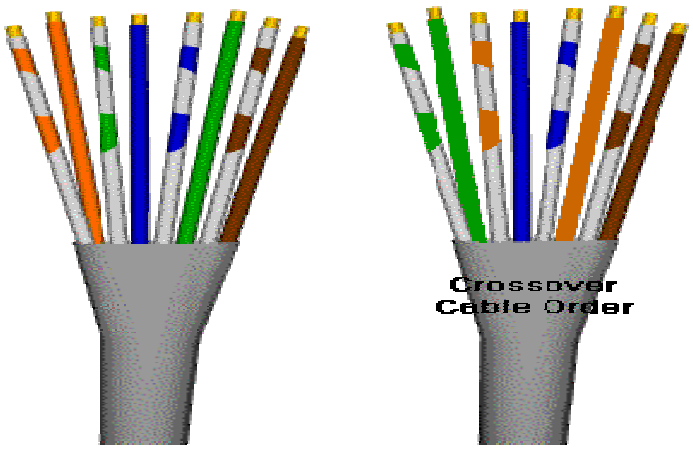


Figura II.5 *Conexión de un cable cruzado*

El grafico previo muestra la conexión de un cable "crossover" que permite conectar 2 PCs directamente.

II.1.3.4 CABLE COAXIAL

Este cable consiste de un alambre central rodeado por una malla de alambre, separados ambos por un aislante. La malla esta usualmente conectada a un sistema de tierras, y su función principal es minimizar la interferencia eléctrica y de

radiofrecuencia.

El cable coaxial se usa principalmente en la industria de televisión por cable y en redes de datos. Aunque es mas caro que el cable telefónico, el cable UTP y STP, este es mucho menos susceptible a la interferencia electromagnética y puede transportar muchos mas datos, el cable coaxial fue inventado en 1929 y usado comercialmente hasta 1941.

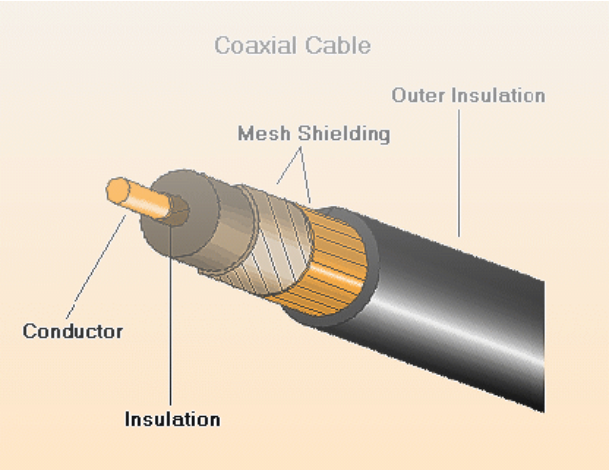


Figura II.6 *Cable coaxial*

APLICACIÓN EN ETHERNET

El cable coaxial fue usado como medio de transmisión en dos implementaciones físicas de Ethernet: 10base2 y 10base5.

10base2. También llamado "thin" (delgado) usa cable coaxial de 50 ohms (RG-58 A/U) con una longitud máxima de 185 metros entre dispositivos. Los cables en este tipo de implementación usan conectores del tipo BNC. La tarjeta de red del dispositivo a conectar a la red necesita de un conector tipo "T", terminando las conexiones con un terminador de 50 ohms. l0base2 opera a 10 Mbps y usa métodos de transmisión banda-base.

l0base5. También llamado "Tick" (grueso) usa cable coaxial de 50 ohms con una longitud máxima de 500 metros. El cable usado es prácticamente inflexible. Esta fue la primera implementación física de ethernet.

APLICACIONES EN CABLE MODEM

Aprovechando la infraestructura física de las compañías de televisión por cable, la transmisión de datos por cable coaxial se volvió una opción más de conectividad al Internet.

Los dispositivos a conectarse usan cable modems, usando las especificaciones de interfaz sobre cable DOCSIS. Los estándares DOCSIS proveen las bases para comunicar cualesquiera dos equipos terminales equipados con cable modems, los cuales están diseñados para operar sobre canales específicos de cable.

G.703

Una de las implementaciones físicas para la transmisión del primer orden de PDH (2048 kbps) es el uso de cable coaxial de 75 ohms. Usando como terminadores conectores BNC.

G.753

Una de las implementaciones físicas para la transmisión del tercer orden de PDH (34 368 Kbps) es el uso de cable coaxial de 75 ohms. Usando como terminadores conectores BNC.

II.1.3.5 CÓDIGOS DE LÍNEA

La codificación digital define como los bits de datos son representados eléctrica u opticamente sobre una línea física de comunicaciones, por esta razón los códigos generados son conocidos como códigos de línea.

La técnica de la codificación digital debe considerar por lo menos los siguientes aspectos:

- Estrecho Ancho de Banda generado a partir de la codificación para permitir la transmisión de muchos datos en un solo cauce de comunicación.

- Bajo nivel de DC generado, con altos niveles de DC la señal generada se atenúa mas por lo que las distancias de transmisión entre dispositivos se acortan. Usar cambios frecuentes en el nivel de voltaje o en la intermitencia de pulsos ópticos permiten una fácil sincronización entre el transmisor y el receptor sin que sea necesaria la adición de más información.

Debido a que la mayoría de los códigos de línea poseen componentes de baja frecuencia, la transmisión de estos es conocida como transmisión banda-base o paso-bajas.

Existen numerosos métodos para codificar datos digitales, desde el más simple NRZ hasta el complicado HDB3. La decisión de que tecnología usar para codificar toma en cuenta varios aspectos: restricciones de ancho de banda, sistemas de cableado y velocidades de transmisión.

PHASE ENCODE (MANCHESTER)

En esta codificación cada periodo de bit se divide en dos intervalos iguales. Con este esquema se asegura que todos los periodos de bit tengan una transmisión en la parte media, propiciando así un excelente sincronismo entre el receptor y el transmisor.

La codificaci6n diferencial Manchester es una variación de la codifcaci6n Manchester básica, pues en ella, un bit con valor 1 se indica por la ausencia de transición al inicio del intervalo, y un bit con valor cero se indica por la presencia de una transición al inicio del intervalo. En ambos casos, existe una transición en la parte media. El esquema diferencial exige un equipo mas sofisticado, pero ofrece una mayor inmunidad al ruido.

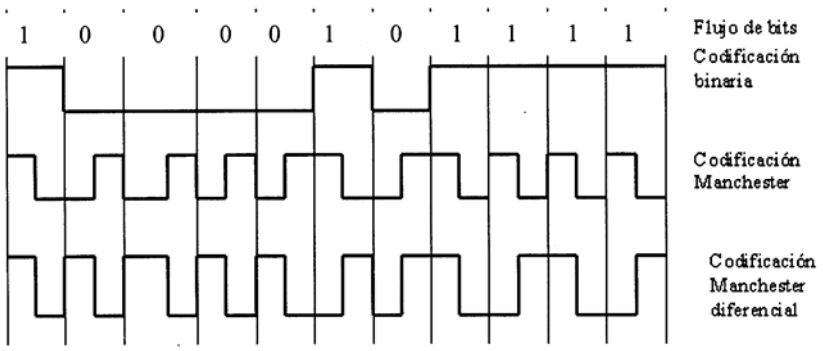


Figura II.7 *Codificación Manchester y Manchester Diferencial*

Este método tiene todas la ventajas necesarias, pero la única que no cumple es que la señal generada tiene un ancho de banda muy grande.

CODIFICACIÓN BIPOLAR

Usa tres niveles de voltaje como el RZ Polar con el objetivo de eliminar toda componente de DC.

- Bipolar Alternate Mark Inversion (AMI). En este código el uno lógico es representado por pulsos de polaridad alternada y el cero lógico con la ausencia de pulsos.

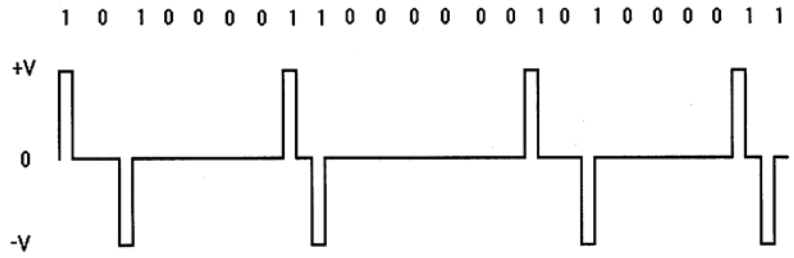


Figura II.8 *Codificación AMI*

- Bipolar 8-Zero Substitucion (B8ZS). B8ZS clasificado también como un código binario de sustitución ceros contiguos, esta será sustituida por una cadena especial que contenga transiciones y así mantener la sincronía entre el transmisor y el receptor.

- High-Density Bipolar 3 (HDB3). Este es otra implementación de los códigos binarios de sustitución de ceros, el cual es similar al B8ZS pero en lugar de sustituir cadenas de ocho ceros contiguos, este sustituye cadenas de cuatro ceros en cadenas de ceros (BNZS) opera igual que el código AMI, pero la diferencia esta en que cuando se encuentra una cadena de ocho especiales que aseguran la sincronía entre equipos.

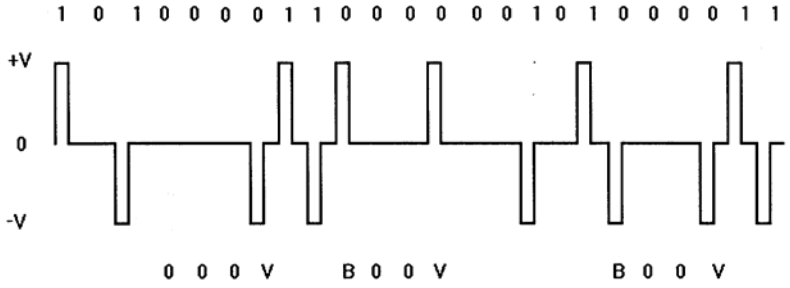


Figura II.9 *Codificación HDB3*

II.1.3.6 SISTEMAS XDSL

Los sistemas del xDSL evolucionaron a consecuencia de la necesidad de transferir información digital, hay una gran variedad de tecnologías xDSL las cuales permiten transmisión de señales analógica y digital en rangos mucho más altos

La tecnología detrás de los sistemas del xDSL continúa evolucionando. Aunque hay estandares, algunos propietarios de otros sistemas han desarrollado sistemas que derivan de los estándares de xDSL. El resultado es que algunos equipos del xDSL no son compatibles con otros equipos del xDSL de la misma clasificación.

HISTORIA DE XDSL

El primer Subscriptor Digital de líneas (DSLs) se desarrolló debido a la necesidad del costo para una comunicación de calidad sobre el alambre de cobre. El primer sistema de transmisión digital fue la línea de T1. Este sistema tenía una distancia máxima de aproximadamente 6,000 pies antes de necesitar repetidores.

La figura II.10 muestra la evolución de los sistemas de DSL. El primer sistema del xDSL fue el HDSL[1], este sistema HDSL aumentó la distancia de señales digitales de alta velocidad que podían transmitirse, con el uso de amplificadores/repetidores.

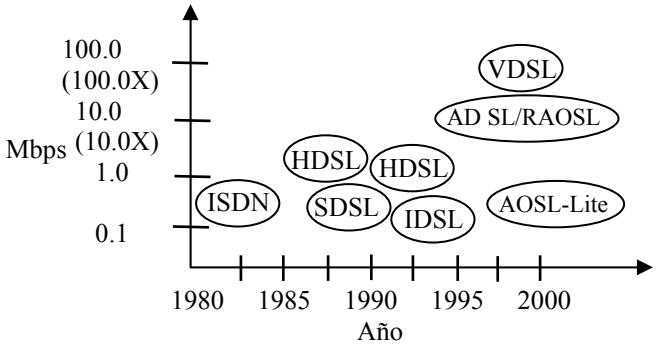


Figura II.10 *Evolución de DSL*

El sistema de HDSL requirió 2 (o 3) pares de alambres para permitir simultáneamente enviar y recibir a a 2 Mbps para una transmisión de datos. Para conservar el número de pares de cobre para la transmisión de datos, se desarrolló la tecnología SDSL[2]. Aunque los sistemas de SDSL ofrecieron más baja tasa de transmisión de datos en comparación con HDSL, se requirieron sólo 2 pares del alambre. Desde que SDSL fue desarrollado, el sistema de HDSL ha evolucionado a una segunda generación (HDSL2) eso permite el uso de 2 pares de alambre duplex con emisiones reducidas (la salida más baja). La nueva tecnología de modulación usada por sistemas de ADSL[3] aumentan la transmisión de los datos desde la oficina central hasta el cliente por encima de los 6 Mbps (algunos sistemas de ADSL a 8 Mbps). Para obtener ventajas del equipo de ISDN[4] y una obtener una mayor eficacia, un vástago d tecnología de ISDN se adaptó para el desarrollo del local loop llamado IDSL[5]. Los sistemas de ADSL evolucionaron para formar la línea del subscriptor digital adaptable (RADSL) la cual permite que los rangos de datos sean automáticamente o manualmente cambiados por el proveedor de servicio.

[1] HDSL (*High Digital Suscriptor Line)*
[2] SDSL *(Sincronous Digital Suscriptor Line)*
[3] ADSL *(Asymetric Digital Suscriptor Line)*
[4] ISDN
[5] IDSL *(Digital Suscriber Line)*

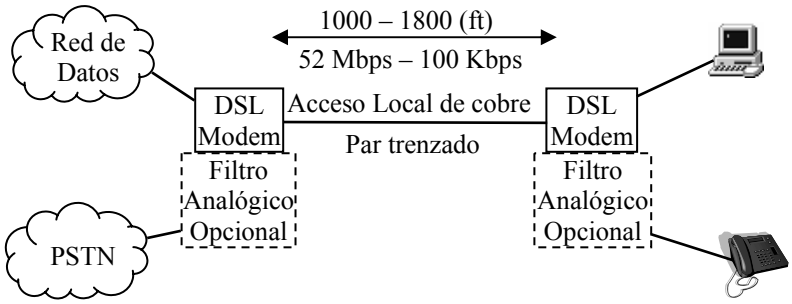


Figura II.11 *Sistema básico de xDSL*

Para simplificar el consumo de instalación para el equipo de DSL, y el vástago de transmisión baja de datos de ADSL se desarrolló ADSL-Lite. Usando una tecnología similar al sistema de ADSL, la línea del subscriptor de muy alta velocidad digital (VDSL) fue creado para proporcionar transferencias arriba de 52 Mbps sobre distancias muy cortas.

La figura II.18 muestra un sistema de xDSL básico. Este diagrama muestra que la llave para las tecnologías de xDSL es más eficiente usando un ancho de banda de 1 MHz en un solo par de líneas de cobre. Un sistema de xDSL consiste en módems compatibles sobre cada local loop. Para algunos sistemas, el sistema de xDSL permite múltiples tipos de transmisión en un solo par de cobre. Esto incluye comunicaciones analógicas o ISDN (por ejemplo las POTS) y comunicaciones digitales (ADSL o VDSL). Este diagrama muestra el tráfico para los sistemas de DSL. Generalmente, la distancia más larga de una línea de cobre, es en proporción el mas bajo rango de datos. Las distancias de menos de 1,000 pies pueden lograr tasas de datos por encima de 50 Mbps.

TECNOLOGÍAS DE XDSL

Hay una gran variedad de tecnologías DSL, dichas tecnologías continúan evolucionando, entre las cuales se encuentran: IDSL, HDSL, SDSL, HDSL2, ADSL, RADSL, CDSL y VDSL. IDSL es una versión simplificada de de ISDN; HDSL fue la primera tecnología que requirió 2 pares de cobre; SDSL fue una segunda versión de HDSL; ADSL fue la primera tecnología de DSL que tuvo velocidades de traslado diferentes; RADSL es una versión de ADSL que permite el cambio automático en las proporciones durante la transmisión de datos; CDSL es una versión de ADSL que simplifica el hardware de la red a través de una transmisión de datos reducida; VDSL es una tecnología DSL de muy alta velocidad que es usada para distancias cortas.

IDSL (DIGITAL SUBSCRIBER LINE)

IDSL es una tecnología digital que precede los sistemas del xDSL, similar a la tecnología del xDSL, ISDN trabaja también sobre estándares de cobre; cada línea de ISDN proporciona dos canales digitales a 64 Kbits por segundo y un cauce digital (usado principalmente para los propósitos de control) a 16 Kbps.

IDSL es un híbrido de ISDN y de DSL, usa la misma estructura de datos de ISDN en el par cobre y entrega un ancho de banda de 144 Kbits por segundo a través de dos canales de 64 Kbps y un canal de 16 Kbps. La diferencia para los sistemas de IDSL es que este sistema sólo usa 64 Kbps de canales de DSO y los canales de control de ISDN (canal D) son ignorados; el sistema de IDSL multiplica el número de canales eficazmente en un solo par de cobre por 2x. La habilidad de evitar usar la señalización de ISDN es muy importante como las actualizaciones del software, permitir el funcionamiento de ISDN puede costar más de $500,000 por switch.

HDSL (HIGH BIT DIGITAL SUSCRIBER LINE)

Se desarrolló la tecnología de HDSL para superar algunas limitaciones significantes de los primeros sistemas de transmisión digitales (T1 y El), estas limitaciones incluyeron una distancia máxima de 6,000 pies entre los repetidores y un requisito para el acondicionamiendo de línea.

Los sistemas electrónicos para tecnología de transmisión digital usada en 1960 y principios de 1970 eran caros, sin embargo, en 1980 el bajo costo de dichos sistemas generó que estuvieran disponibles y esto permitió desarrollar tecnologías de transmisión de datos más eficaces.

Para los sistemas T1 y El se modificaron las características físicas de las líneas de cobre para permitir la transmisión digital, esto requirió equipo y personal especializado, éste era un proceso caro. Se descubrió que las tecnologías para altas velocidades que se desarrollaron en los años sesenta para T1 (1.544 Mbps) y El (2 Mbps) podrían reemplazarse con tecnologías de transmisión más eficaces que no requirán calidad en la línea, lo cual permitió instalaciones más rápidas y sistemas más eficaces para la transmisión de datos.

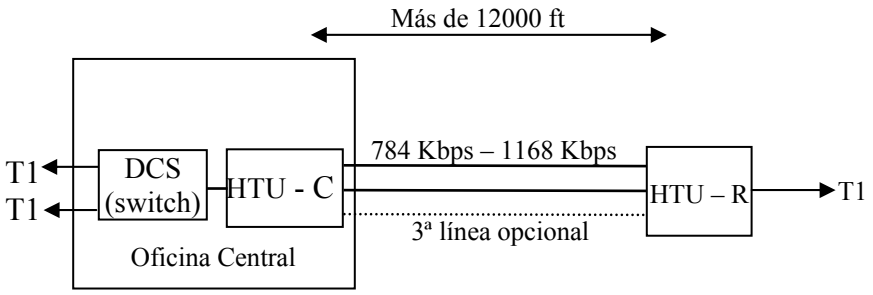


Figura II.12 *HDSL*

La figura II.12 muestra un sistema de HDSL básico, el cual muestra que la primera aplicación para HDSL usó dos pares (y a veces 3 pares) de cobre, cada sistema tiene una terminal(HTU) HDSL, un HTU-C (central) y HTU-R (remoto). Este ejemplo muestra que cada par de cobre de HDSL lleva 784 Kbps en full dúplex (simultáneamente envía y recibe). Para llevar el equivalente de una línea de T1, se usan dos líneas, también es posible llevar una línea del E1 usando 3 pares de cobre, aunque el transporte ideado para HDSL es diferente para un T1 o línea del El, el HTU-C y HTU-R convierten los protocolos a las líneas de TI normales.

La ventaja del sistema de HDSL es el aumento en distancia de una línea que pudiera ir entre repetidores, los sistemas de HDSL pueden tener hasta 12,000 pies (o más con un mayor calibre del alambre) en comparción de un T1 o línea del El que sólo pueden tener hasta 6,000 pies entre repetidores, además de que las líneas de HDSL son más tolerantes.

SDSL (SYMMETRIC DIGITAL SUBSCRIBER LINE)

SDSL ofrece una transmisión de datos a una velocidad semejante a la de HDSL, con dos diferencias clave: SDSL usa sólo un par de cobre (opuesto a los 2 pares requeridos para HDSL) y la distancia de la línea debe ser menor de 10,000 pies entre la oficina central del provedor del servicio de Internet.

HDSL2 HIGH BIT RATE DIGITAL SUBSCRIBER LINE - 2ND GENERATION

HDSL segunda generación (HDSL2) se desarrolló en 1998 como la siguiente generación de tecnologías de HDSL, las principales características de este sistema incluyen la interferencia minimizada a otras líneas de cableado, rango extendido, aumento en la proporción de transmisión de datos y la habilidad para la transmisión de datos en un solo par de cobre. Para lograr estos objetivos, la línea que codifica usada para el sistema de HDSL2 difiere de sus predecesores (HDSL y SDSL).

ADSL (ASYMMETRIC DIGITAL SUBSCRIBER LINE)

ADSL es un sistema de comunicación que transfiere información analógica y digital sobre un par de cobre, la información analógica puede ser un estándar POTS o ISDN, el rango máximo de la transmisión digital baja (los rangos del usuario final) puede variar de 1.5 Mbps a 9 Mbps y el rango máximo de la transmisión digital alta (del cliente a la red) varía de 16 Kbps a aproximadamente 800 Kbps. La tasa de transmisión de datos varía, dependiendo de la distancia y la distorsión de la línea, la tecnología ADSL es capaz de transmitir películas digitales, televisión, catálogos de cuadro, la calidad del CD audio, eslabones para las redes de alta velocidad, e Internet de gran velocidad en los negocios pequeños y casas.

Al contrario de las tecnologías de xDSL actuales, ADSL es asimétrico en su naturaleza, fue elaborado a consecuencia de que muchos clientes requerían servicios con una transmisión de datos de gran velocidad de la red. Los canales de transmisión de ADSL pueden ser divididos en canales de alta velocidad y al mismo tiempo continúa proporcionando los POTS normales, dichos POTS o el canal de ISDN están separados del módem digital por filtros.

Esto permite POTS in-interrumpidos o ISDN aun cuando el sistema de transmisión de datos de gran velocidad se pone inoperable.

El máximo rango de transmisión de datos para módems de ADSL varía dependiendo de la distancia, los niveles de interferencia, calidad de la línea de cobre, generalmente, ADSL proporcionará el siguiente rango de transmisión de datos y se muestra en Tabla II.5.

Rango de Datos	Medida del conductor	Distancia
1.5 o 2 Mbps	24 AWG/0.5 mm	18000 ft/5.5 Km
1.5 o 2 Mbps	26 AWG/0.4 mm	15000 ft/4.6 Km
6.1 Mbps	24 AWG/0.5 mm	12000 ft/3.7 Km
6.1 Mbps	26 AWG/0.4 mm	9000 ft/2.7 Km

Tabla II.3 *Rango de transmisión de datos de ADSL*

Algunos protocolos están disponibles para los módems de ADSL incluso Ethernet, ATM e IP, esto permite al cliente un plug and play en la capacidad, si el servicio de DSL está disponible en su área.

La versión ADSL de Gdmt puede transferir los datos por debajo de los 8 Mbps y por arriba de los 1.5 Mbps si el módem se localiza a una distancia de más de 10,000-12,000 pies de la oficina central (CO), la transmisión de datos Gdmt puede proporcionar una transmisión de 1.5 Mbps a 18,000 pies de la oficina central, si se

usa un "splitterr", este debe instalarse en la línea para separar la señal analógica de la digital de gran velocidad.

De acuerdo con expertos de la industria, arriba del 95% del acceso con el par de cobre tiene una distancia que está dentro del alcance de servicio de ADSL. Pueden localizarse clientes que se localizan más allá de estas distancias con los sistemas digitales basados en fibra, desgraciadamente, algunas compañías locales usan los IDSL para la transmisión digital en el acceso local de la red y este sistema no es directamente compatible con el servicio ADSL.

Inicialmente, un Foro de ADSL fue establecido para ayudar a promover servicios de ADSL y equipo, dado que dicho Foro ha estado involucrado con la evolución de tecnología de DSL (por ejemplo VDSL y ADSL-Lite), actualmente se ha renombrado el Foro de DSL.

El primer código de línea oficial para los sistemas de ADSL fue DMT, subsecuentemente de su introducción, variantes que usan el código CAP han surgido. Es probable que las variaciones de códigos de línea continuarán apareciendo para la mejora de sistemas de ADSL.

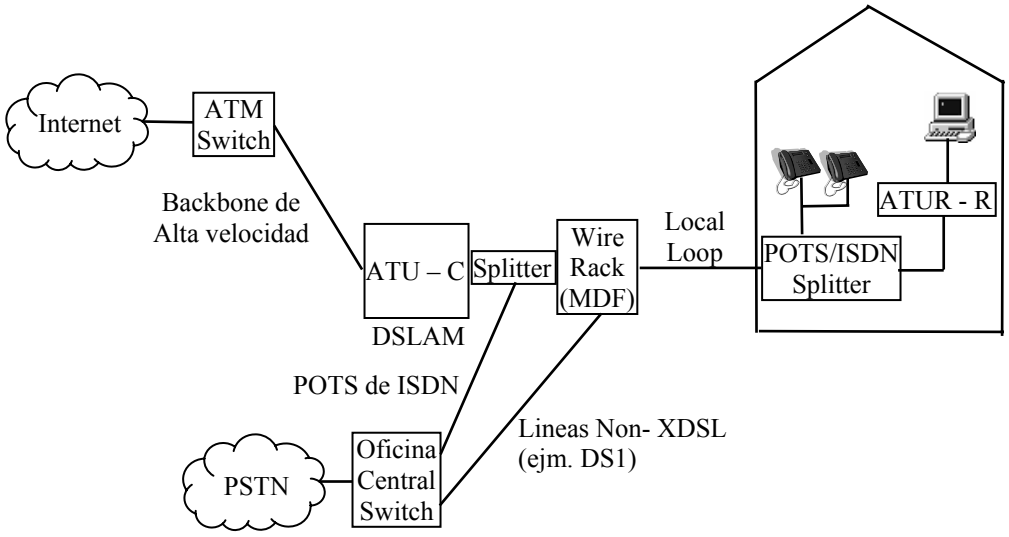


Figura II.13 *ADSL*

La figura II.13 muestra un sistema ADSL típico, este diagrama muestra que una sola línea de acceso de cobre puede conectarse a redes diferentes. Éstos incluyen las redes de swicheo publico (PSTN) y las redes de comunicaciones de datos (normalmente Internet o servidor de medios de comunicación). La habilidad de los sistemas de ADSL para combinar y separar la señal de baja frecuencia (POTS o IDSN) se realiza a través del uso de un splitter, el cual está compuesto de dos filtros de frecuencia; uno para el paso bajas y uno para el paso altas. Los módems de DSL trasmiten a la oficina central (ATU-C) y la ADSL transfiere a la unidad remota o

negocio (ATU-R), el DSLAM se conecta a la línea de acceso vía el marco de distribución principal (MDF), este es el punto donde terminan de líneas de acceso de cobre que conectan los usuarios finales a la oficina central.

RADSL (RATE ADAPTIVE DIGITAL SUBSCRIBER LINE)

El RADSL opera al mismo ancho de banda que ADSL con la capacidad dinámica de ancho de banda cambiante, los anchos de banda pueden cambiar debido a la calidad de la línea durante la transmisión de datos o como resultado de limitaciones impuestas por el proveedor de servicio (diferentes rangos para servicios diferentes).

CDSL (CONSUMER DIGITAL SUBSCRIBER LINE)

El CDSL o ADSL Universal fue desarrollado para superar un desafío de la instalación de sistemas de ADSL, CDSL también es conocido como ADSL-lite o G.Lite, este elimina el requisito de tener que instalar un splitter en la casa o negocio. Sin embargo, el intercambio es de baja transmisión de datos (aproximadamente 1.5 Mbps para bajos rangos y 384 kbps para altos rangos).

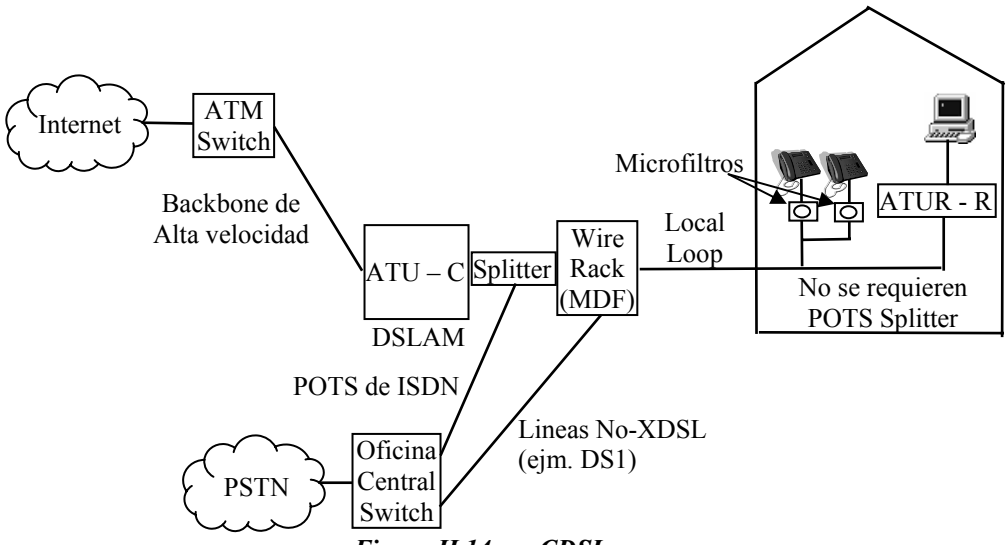


Figura II.14 CDSL

La figura II.14 muestra un sistema de CDSL típico. Este diagrama muestra que la red de DSL básica es similar a la red de ADSL, la diferencia primaria está en el equipo del usuario final y su conexión a la red; el sistema de CDSL no requiere un splitter para la casa o negocio, en cambio, el usuario final puede instalar microfiltros entre la línea y los teléfonos normales, estos microfiltros bloquean los datos transmitidos a altas velocidades.

VDSL (VERY HIGH BIT RATE DIGITAL SUBSCRIBER LINE)

Al principio del 2000, el rango-bit de VDSL era la tecnología de DSL más rápida disponible hasta el momento, VDSL ofrece rangos bajos de 13 a 52 Mbps y 1.5 a 26Mbps para rangos altos, desgraciadamente, tales proporciones de transmisión de datos están limitadas (aproximadamente 1,000 y 4,500 pies de logitud).

VDSL que se derivaron de la transmisión de bajos rangos de datos fueron ATM, SONET y SDH, estas incluyen 51.84 Mbps, 25.92 Mbps y 12.96 Mbps. La tabla II.5 muestra la distancia aproximada y las proporciones de los datos asociados con VDSL.

VDSL se ve como una tecnología para fibra óptica, también permite el uso de teléfonos analógicos junto con las conexiones de datos de velocidades altas; sin embargo, VDSL sólo transfiere datos de velocidad altas para distancias cortas.

La tecnología de VDSL se parece la tecnología de ADSL, sin embargo, ADSL fue diseñado para adaptarse a condiciones de línea más hostiles, la tecnología de VDSL realmente es mucho más sencilla de implementar.

Las versiones iniciales de VDSL dividen la frecuencia multiplexando, para separar los rangos de los canales altos y bajos, sin embargo, las nuevas versiones de VDSL pueden compartir las mismas bandas de frecuencia.

Rangos de flujo bajo	Máxima distancia	Rangos de flujo alto
12.96 – 13.8 Mbps	4500 ft/1.5 Km	1.6 – 2.3 Mbps
25.92 – 27.6 Mbps	3000 ft/ 1.0 Km	19.2 Mbps
52.84 – 55.2 Mbps	1000 ft/0.3 Km	Igual a Flujo bajo

Tabla II.4 *Rango de transmisión de datos VDSL*

DSL usa la radiofrecuencia sobre ADSL. Las antenas telefónicas pueden capturar y pueden transmitir señales por radio a través de signos, usar una radio aficionado cerca de las líneas de VDSL puede disminuir la capacidad de transmisión de datos de sistemas VDSL dramáticamente, igualmente la transmisión de VDSL también puede interferir con las señales de radio.

La figura II.15 muestra un sistema de VDSL, en el cual la fibra termina en una unidad de red óptica (ONU), esta convierte la señal óptica en una señal eléctrica que puede usarse por medio del módem de VDSL en el DSLAM, la señal del modem DSL proporciona un splitter que combina la señal analógica y digital para el acceso a la línea de cobre.

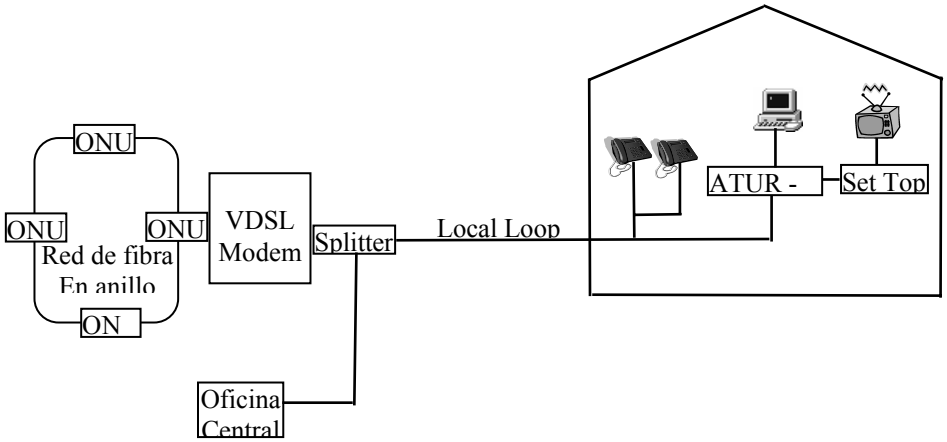


Figura II.15 *VDSL*

El splitter realmente se coloca en los últimos cientos de Km de la línea de acceso de cobre. La figura muestra que las POTS analógicas de la compañía local todavía pueden viajar atrás miles de Km a la oficina central. La señal de VDSL llega a un splitter que separa la señal analógica de alta velocidad del VDSL digital.

COMPARACIÓN DE TECNOLOGÍAS

Generalmente, la disponibilidad de una nueva tecnología de modulación y el bajo costo de los circuitos electrónicos que realizan dicho proceso ha ocasionado un cambio dramático en el par de cobre para alcanzar grandes velocidades en las señales de datos.

Tecnología DSL	Datos DownStram (Kbps)	Datos Upstream (Kbps)	Pots/ISDN Co-existencia	Distancia máxima (ft)
ISDL	128	128	No	18000
HDSL	784 – 2048	784 – 2048	No	12000
SDSL	384	384	No	12000
HDSL-2	1544 – 2048	1544 – 2048	No	12000
ADSL/RADSL	1000 – 8000	1000 – 8000	Si	18000
ADSL Lite	800 – 2000	16 – 200	Si	18000
VDSL	1000 – 52000	1000 – 52000	Si	4500 (1000 para rangos más altos)

Tabla II.5 *Comparación de tecnologías xDSL*

Cada una de las tecnologías de xDSL fue desarrollada para satisfacer una necesidad comercial específica y desafíos tecnologicos. Las claves comerciales para el desarrollo de tecnología de xDSL incluyen la habilidad de tener una compatibilidad dirigida hacia atrás (análogo simultáneamente analógico y digital),

una velocidad de transmisión de datos alta, la habilidad de operar las líneas de los local loops , lograr la mayor distancia sin repetidores y una instalación simple.

La tabla II.5 muestra una comparación de las tecnologías de xDSL, la cual muestra que existen intercambios entre cada una de las tecnologías, generalmente, la más larga en distancia, es la más baja en proporción de datos; sin embargo, con el proceso señalado, pueden lograrse proporciones de datos más altas y distancias más largas.

II.1.3.7 INTERFACES

Son aquellos elementos que nos hacen posible la conexión entre determinado tipo de cable que transporta una señal y un equipo o accesorio que la envía o recibe, nos facilitan la tarea de conectar y desconectar, permitiéndonos cambiar de equipo o cableado rápidamente.

HSSI

Los adaptadores de puertos de HSSI proporcionan hasta dos EIA/TIA 612/613, interfaces en serie de la alta velocidad, proporcionan conectividad a las unidades de servicio externas, a los servicios del acceso en NxT1, NxE1, T3 (45 Mbps), E3 (34 Mbps) y las tarifas ópticas síncronas Sts-1 de la red (SONET) (51,82 Mbps).

Descripción	Cisco 7100	Cisco 7200	Cisco 7200VXR	Cisco 7500/VIP2	Número De Pieza
Adaptador Portuario De 1-port HSSI	Sí	Sí	Sí	Sí	Pa-h
Adaptador Portuario De 2-port HSSI	Sí	Sí	Sí	Sí	Pa-2h

Tabla II.6 *Características HSSI*

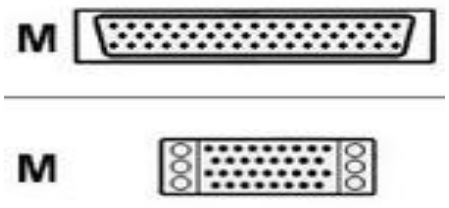


Figura II.16 *Adaptador Portuario de HSSI*

RS-232

Los estándares son para velocidades de 256 Kbps a longitudes menores y de 15M (50 pies) o menor, hoy los puertos de alta velocidad en nuestra PC han aumentado enormemente. La regla del pulgar para la longitud de un cable de datos depende de la velocidad de estos, definiendose la calidad del cable. Las comunicaciones de datos entre los equipos se dividen en dos amplias categorías: single-ended y diferenciado; RS-232 (single-ended) fue introducido en 1962, y a pesar de los rumores que se dieron para su desecho, se ha seguido utilizado extensamente en la industria.

Los canales full-duplex se establecen para las comunicaciones de dos vías; las señales RS232 son representadas por los niveles voltaicos con respecto a un campo común del sistema. El estado “apagado” (MARCA) tiene el nivel negativo de la señal, y el estado "activo" (ESPACIO) tiene el nivel positivo de la señal. RS232 tiene numerosas líneas de hand shaking (usadas sobre todo con los módems), y también especifican un protocolo de comunicaciones.

Un puerto Rs-232 puede proveer de energía limitada a otro dispositivo; el número de las líneas de salida, del tipo de IC del conductor del interfaz, y del estado de las líneas de salida son consideraciones importantes.

Los datos se transmiten y se reciben en los pines 2 y 3 respectivamente; DSR es una indicación del módem (es decir, el módem o el DSU/CSU) de que está encendido al igual que el DTR indica al módem que el DTE está encendido. El DCD indica si se esta recibiendo una buena señal de un módem lejano.

Los pines 4 RTS y 5 CTS se utilizan para controlar, en la mayoría de las situaciones son asincrónicas, RTS y CTS están constantemente encendidos a través de la sesión de la comunicación, sin embargo donde el DTE seconecta con una línea de múltiples puntos, se utiliza RTSpara girar la portadora en el módem por intervalos. En una línea de puntos múltiples, es imprescindible que solamente una estación este transmitiendo a la vez, cuando un equipo desea transmitir, levanta RTS, el módem gira la portadora, espera algunos milisegundos para que la portadora se estabilice, y después levanta CTS. Cuando la estación ha acabado su transmisión, da de baja RTS, CTS y la portadora del módem juntas. Las señales del reloj (pines 15, 17, y 24) se utilizan solamente para las comunicaciones sincronías, el módem o el DSU extraen el reloj de la secuencia de datos y proporcionan una señal constante de reloj al DTE.

Db-25	Dce	Db-9			
1			Aa	x	Tierra Protectora
2	TXD	3	BA	I	Datos Transmitidos
3	RXD	2	BB	O	Datos Recibidos
4	RTS	7	Ca	I	Petición De enviar
5	CTS	8	CBES	O	Claro Para enviar
6	DSR	6	Cc	O	Modem Listo
7	Tierra	5	Ab	x	Tierra De la Señal
8	"copia MÁS OSCURA"	1	CF	O	Detector De la Señal De Línea Recibida
9			--	x	Reservado para la prueba del MODEM
10			--	x	Reservado para la prueba del MODEM
11				x	No asignado
12	SCF			O	Línea Signl Detctr De Secndry Rcvd
13	SCB			O	Claro secundario a enviar
14	SBA			I	Datos Transmitidos Secundarios
15	DB			O	Transmisn Signl Elemnt Timng
16	SBB			O	Datos Recibidos Secundarios
17	DD			O	Sincronización De Elemento De Señal De Receptor
18				x	No asignado
19	SCA			I	Petición secundaria de enviar
20	DTR	4	"copia MÁS OSCURA"	I	Terminal De los Datos Listo
21	CG			O	Detector De la Calidad De la Señal
22		9	CE	O	Indicador Del Anillo
23	CH/CI			I / O	Selector De la Tarifa De la Señal De los Datos
24	DA			I	Transmita La Sincronización De Elemento De Señal
25				x	No asignado

Tabla II.7 *Entradas y salidas del Rs-232*

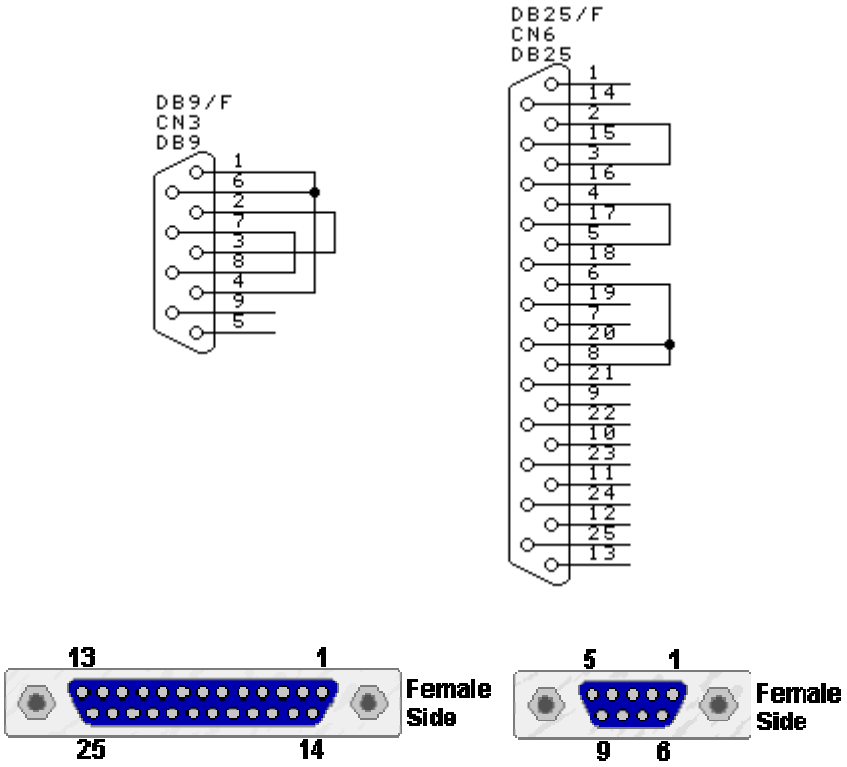


Figura II.17 *Conectores Rs-232*

RS-232D utiliza los conectores del tipo RJ45

No. Del Perno.	Descripción De la Señal	Abbr.
1	Dce Listo, Indicador Del Anillo	DSR/RI
2	Detector De la Señal De Línea Recibida	DCD
3	Dte Listo	DTR
4	Tierra De la Señal	SG
5	Datos Recibidos	RxD
6	Datos Transmitidos	TxD
7	Claro Para enviar	CTS
8	Petición De enviar	RTS

Tabla II.8 *Descripción de RS-232*

INTERFAZ G.703

G.703 es un estándar que describió originalmente redes digitales del excedente de la voz, es una recomendación del CCITT que se asocia al estándar PCM; la voz aconverita a una forma digital requiere un ancho de banda de 64 Kkbps (+/- 100 PPM), dando por resultado la unidad básica para G.703, multiplicando esto da lugar

a T1 (1544 Kbps) y a E1 (2048 Kbps). Las redes modernas trabajan con voz y datos y así que son G.703. Otras características que describen los G-esta'ndares son:

Algunas definiciones	
G.704	Capítulo
G.706	Procedimiento Crc-4
G.732	Dirección de la avería

Tabla II.9 *Definiciones*

G.703 se puede transportar sobre el par de cobre equilibrado (120 ohms TP) y desequilibrado. La versión equilibrada viaja a una velocidad de 64 Kbps, y se transmite de tres formas diferentes: co-direccional (4-alambres), central-direccional (6/8 alambres) y contra-direccional (8-alambres).

CO-DIRECCIONAL .

Esto es una versión 4-alambres, el la que cada dirección (transmisión, recepción) consiste en 2 alambres trenzados juntos, proporcionando una señal equilibrada.

Los datos y la sincronización son envíados en el mismo excedente de la dirección y por los mismos alambres. Esto hace el co-direccional.

Algunas Características Eléctricas	
Marca	1,0 VDC
Espacio	0 VDC +/- 0,10 VDC
Anchura del pulso	usec 3,9

Tabla II.10 *Características eléctricas*

La codificación se hace en tres pasos:

1. Un 1 binario es substituido antes de 1100 y un 0 binario antes de 1010.
2. Conversión en una señal de tres niveles (AMI) alternando la polaridad de bloques consecutivos.
3. La conversión al 8vo bloque violado de AMI. Every de la polaridad se alterna. Las marcas de bloque violadas el pedacito pasado en un octeto.

CENTRAL-DIRECCIONAL

Esto es una versión raramente usada, las señales del reloj se alimentan en diversos alambres de un reloj centralizado, la razón de la versión de 8 o 6 alambres

se debe a la posibilidad de que se envien señales del reloj balanceadas en ambas direcciones y al mismo tiempo, o en direcciones separadas; el primero tiene 6-alambres (2 registros, 4 datos), el segundo tiene 8-alambres (4 registros, 4 datos).

Algunas Características Eléctricas	
Marca	1,0 VDC
Espacio	0 VDC +/- 0,10 VDC
Anchura del pulso	usec 15,6

Tabla II.11 *Características eléctricas*

La técnica de la modulación usada es AMI.

CONTRA-DIRECCIONAL

Esto es siempre una versión de 8-alambres, la cual utiliza un par para transmitir y otro par para la recepción y dos pares para las señales de reloj. Todas las señales de reloj se envían al DTE, lo que significa que todas son originadas por el DCE.

Algunas Características Eléctricas	
Marca	1,0 VDC
Espacio	0 VDC +/- 0,10 VDC
Anchura del pulso	usec 15,6

Tabla II.12 *Características eléctricas*

La técnica de la modulación usada es AMI.

El resto de las velocidades utilizan un diverso esquema de codificación y diverso ancho en el pulso, también los voltajes de pueden variar.

Una descripción rápida para el más común:

Algunas características eléctricas para el T1	
El cablegrafiar	co-direccional
Marca	3,0 VDC
Espacio	0 VDC +/- 0,30 VDC
Anchura del pulso	647 nanosegundos
Codificación	AMI (bipolar) o B8ZS
Velocidad	kbps 1544 +/- 50 PPM

Tabla II.13 *Características eléctricas del T1*

El cablegrafiar	**Par coaxial o un simétrico (4 alambres) para cada dirección**
Marca	Equilibrado: 3,0 VDC Desequilibrado: 2,37 VDC
Espacio	Equilibrado: 0 VDC +/- 0,237 VDC Desequilibrado: 0 VDC +/- 0,3 VDC
Anchura del pulso	488 nanosegundos
Codificación	AMI o bipolar de alta densidad de la orden 3 (HDB3)
Velocidad	kbps 2048 +/- 50 PPM

Tabla II.14 *Algunas características para E1*

Para una descripción más detallada vea los documentos correspondientes sobre la serie-E y la serie-T.

Señal	Descripción RJ45	Dte RJ45	Descripción de BNC	DTE BNC
RxA	Reciba La Negativa De la Entrada	1	Reciba La Entrada	Extremidad
RxB	Reciba El Positivo De la Entrada	2	Reciba La Tierra	Anillo
TxA	Transmita La Negativa De la Salida	4	Transmita La Salida	Extremidad
TxB	Transmita El Positivo De la Salida	5	Transmita La Tierra	Anillo
S1	Transmita La Tierra	3		
S2	Reciba La Tierra	6		

Tabla II.15 *Fijación de especificaciones*

INTERFAZ V.35

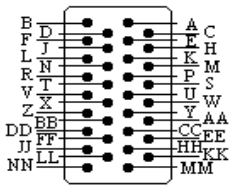
V.35 es una interfaz parcialmente balanceada con una sola terminal, en la que los datos y los bits del reloj estan balanceados, los bits son single-ended, y son utilizados comúnmente para tasas de transmisión a 56 Kbps y 64 Kbps.

	BITS DE LOS DATOS		CONTROL DE LOS PLOMOS	
VDC	**B > A**	**A > B**	**-3 a -25**	**+3 a +25**
binario	1	0	1	0
señal	MARCA	ESPACIO	MARCA	ESPACIO
función	de	En	de	En

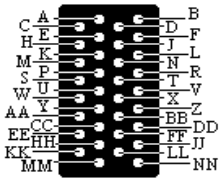
Tabla II.16 *V.35*

El voltaje de salida de un transmisor balanceado que indica una MARCA es +0.35Vdc para la línea de B, -0.2Vdc para la línea de A, la indicación de una condición del ESPACIO es +0.35Vdc para la línea de A, -0.2Vdc para la línea de B y la diferencia de voltaje de la salida es 0.55Vdc. El receptor debe de tener por lo menos una diferencia de 0.01Vdc entre la línea de A y la línea de B, dado que la longitud de cable máxima depende de la velocidad y de la capacitancia requeridas por el cable. La medida especifica es de los 2000ft/600m hasta los 4000ft/1200m @

100kbps, de los 300ft/90m en los usos de sincronia a 10Mbps solamente, y ningún equipo del asincrono V.35 alrededor.



Varón M/34



Hembra M/34

Perno	Señal	Abbr.	Dte	Dce
A	Tierra Del Chasis		-	-
B	Tierra De la Señal		-	-
C	Petición De enviar	RTS	Fuera de	En
D	Claro Para enviar	CTS	En	Fuera de
E	MODEM Listo	DSR	En	Fuera de
F	El Soporte Detectó	DCD	En	Fuera de
H	Terminal De los Datos Listo	DTR	Fuera de	En
J	Loopback Local	LL	En	Fuera de
K	Prueba Local		Fuera de	En
L	No asignado			
M	No asignado			
N	No asignado			
P	Envíe Los Datos A	TxD-	Fuera de	En
R	Reciba Los Datos A	RxD-	En	Fuera de
S	Envíe Los Datos B	TxD+	Fuera de	En
T	Reciba Los Datos B	RxD+	En	Fuera de
U	Terminal Que mide el tiempo De A		Fuera de	En
V	Reciba A Que mide el tiempo		En	Fuera de
W	Sincronización Terminal B		Fuera de	En
X	Reciba La Sincronización B		En	Fuera de
Y	Envíe A Que mide el tiempo		En	Fuera de
Z	No asignado			
Aa	Envíe La Sincronización B		En	Fuera de
BB	No asignado			
Cc	No asignado			
DD	No asignado			
EE	No asignado			
FF	No asignado			
HH	No asignado			
JJ	No asignado			
KK	No asignado			
LL	No asignado			
Milímetro	No asignado			
NN	No asignado			

Tabla II.17 *Descripción del V.35*

Existen dos versiones de V.35, el primero se llama V.35 Winchester, el otro se llama V.35 Straight, uno se refleja al otro. Hay dos versiones de cerraduras del tornillo de V.35. La versión mide 16/10 milímetros, las medidas de la versión francesa 10/10 milímetros. La versión que se utiliza aqui se conoce como doméstica y la francesa como internacional.

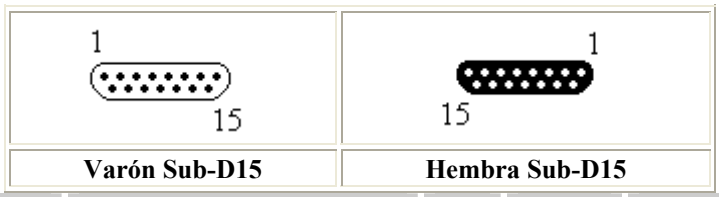
INTERFAZ X.21

Voltajes:	**+/- 0.3Vdc**
Velocidades:	Máximo 100Kbps (X.26)
	Máximo 10Mbps (X.27)

Tabla II.18 *Voltajes X.21*

La interfaz X.21 fue recomendada por el CCITT en 1976, esta definida para una interfaz digital entre el equipo y el equipo del portador (DCE) de los clientes (DTE), y el primario utilizado para el equipo de telecomunicaciones.

Todas las señales son balanceadas, tienen siempre un par (+/-) para cada señal, utilizado en RS422, eléctricamente las señales X.21 son iguales que RS-422.



Varón Sub-D15	**Hembra Sub-D15**

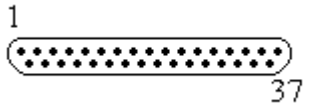
Perno	Señal	abbr.	Dte	Dce
1	Protector		-	-
2	Transmita (a)		Fuera de	En
3	Control (a)		Fuera de	En
4	Reciba (a)		En	Fuera de
5	Indicación (a)		En	Fuera de
6	Sincronización De la Señal (a)		En	Fuera de
7	No asignado			
8	Tierra		-	-
9	Transmita (b)		Fuera de	En
10	Control (b)		Fuera de	En
11	Reciba (b)		En	Fuera de
12	Indicación (b)		En	Fuera de
13	Sincronización De la Señal (b)		En	Fuera de
14	No asignado			
15	No asignado			

Tabla II.19 *Descripción X.21*

Como se puede ver de las especificaciones de fijación, la sincronización de el elemento de señal (reloj) es proporcionada por el DCE, lo cual significa que su abastecedor es responsable de su correcto funcionamiento y que el X.21 es una interfaz síncroao. El handshaking del hardware es hecho por las líneas de control, este es utilizado por el DTE y la indicación es el DCE uno.

INTERFAZ RS-449

El estándar de EIA Rs-449 especifica las características funcionales y mecánicas de la interconexión entre equipo terminal de datos (DTE) y la conformación a los estándares de interfaz eléctricos de EIA Rs-422 y Rs-423.



	Varón		Hembra	
Perno	Señal	Abbr.	Dte	Dce
1	Protector			
2	Indicador De la Tarifa De la Señal	S	Fuera de	En
3	No asignado			
4	Envíe Los Datos (a)	Sd-	Fuera de	En
5	Envíe La Sincronización (a)	St-	En	Fuera de
6	Reciba Los Datos (a)	Rd-	En	Fuera de
7	Petición De enviar (a)	Rs-	Fuera de	En
8	Reciba La Sincronización (a)	Rt-	En	Fuera de
9	Claro Para enviar (a)	Cs-	En	Fuera de
10	Loopback Local	LL	Fuera de	En
11	Modo De los Datos (a)	Dm-	En	Fuera de
12	(a) Listo Terminal	Tr-	Fuera de	En
13	Receptor (a) Listo	Rr-	En	Fuera de
14	Loopback Alejado	RL	Fuera de	En
15	Llamada Entrante	IC	En	Fuera de
16	Señal Freq./Sig. Tarifa Selecta.	SF/SR+	In/Out	Out/In
17	Sincronización Terminal (a)	Tt-	Fuera de	En
18	Pruebe El Modo (a)	Tm-	En	Fuera de
19	Tierra De la Señal	SG		
20	Reciba El Campo común	RC		
21	No asignado			
22	Envíe Los Datos (b)	SD+	Fuera de	En
23	Envíe La Sincronización (b)	ST+	En	Fuera de
24	Reciba Los Datos (b)	RD+	En	Fuera de
25	Petición De enviar (b)	RS+	Fuera de	En
26	Reciba La Sincronización (b)	RT+	En	Fuera de
27	Claro Para enviar (b)	CS+	En	Fuera de
28	Terminal En Servicio	ES	Fuera de	En

29	Modo De los Datos (b)	DM+	En	Fuera de
30	(b) Listo Terminal	TR+	Fuera de	En
31	Receptor (b) Listo	RR+	En	Fuera de
32	Seleccione El Recurso seguro	Ss	En	Fuera de
33	Calidad De la Señal	SQ	En	Fuera de
34	Nueva Señal	Ns	Fuera de	En
35	Sincronización Terminal (b)	TT+	Fuera de	En
36	Indicador Espera	SB	En	Fuera de
37	Envíe El Campo común	Sc		

Tabla II.20 *Descripción RS-449.*

II.1.4 TECNOLOGÍAS DE FIBRA ÓPTICA

Las primeras telecomunicaciones ópticas en la atmósfera libre tropezaron con los mismos inconvenientes que las transmisiones por microondas. Así como se utilizaron guías de onda con atmósfera controlada para limitar la atenuación de las microondas, se visualizó la idea de controlar el medio de propagación de la luz. Fue así como se originaron las guías de onda de luz, es decir, las fibras ópticas. Las ondas luminosas se propagan dentro de un cilindro de vidrio extremadamente puro y no absorbente.

La fibra óptica debe ser lo más transparente posible, a fin de que pueda utilizarse, para esto se usa vidrio extremadamente puro, llamado sílice. Así, entre menos sea la atenuación en la fibra, más larga podrá ser esta. Considerando el rápido progreso que ha tenido la tecnología en la reducción de la atenuación, y aunada al desarrollo de fuentes fiables que emiten en longitudes de onda para las cuales la fibra presenta un mínimo de atenuación, se dio origen a las telecomunicaciones por fibra óptica que se conocen actualmente.

A partir de 1975, la tecnología de las fibras ópticas ha avanzado a un ritmo vertiginoso desde todos los puntos de vista, evolucionando a medida que los laboratorios perseveraban en su desempeño de conseguir sistemas capaces de transmitir más cantidad información, a velocidades más elevadas, a mayores distancias y con costos mas reducidos. La fibra óptica se empezó a utilizar en los enlaces telefónicos de comunicaciones, ampliando después su radio de acción a las redes de abonado, donde se espera su futuro más prometedor. Precisamente su gran ancho de banda, del orden de los 140 THz en la banda de 900 a 1600 nm, permitirá su empleo masivo en las redes de área local (LAN), redes metropolitanas (MAN) y redes de área amplia (WAN).

II.1.4.1 SISTEMAS DE COMUNICACIÓN POR FIBRA ÓPTICA

Los recientes progresos de la tecnología en rayos láser semiconductores y en fibras ópticas de baja atenuación hace posible la realización sistemas de telecomunicación mediante fibras ópticas como canal de transmisión. Es importante conocer su estructura general, así como las ventajas potenciales de su utilización en diversos campos.

Un sistema de comunicación por fibra óptica está constituido por tres elementos (figura II.18):

- Un módulo de emisión, que tiene por función transformar la información en forma de señal eléctrica a información en forma de luz. A este módulo se le llamará emisor óptico.
- Un canal de transmisión de la luz, que es la fibra óptica.
- Un módulo de recepción, que tiene por función transformar la información óptica recibida en información con la forma de señal eléctrica; se le llamará receptor óptico.

Figura II.18 *Sistema de comunicación por fibra óptica*

Las transmisiones a distancias demasiado grandes pueden necesitar la utilización de uno o varios repetidores, cuya función es amplificar la señal óptica. Un repetidor está constituido por un receptor óptico seguido por un emisor óptico (figura II.19).

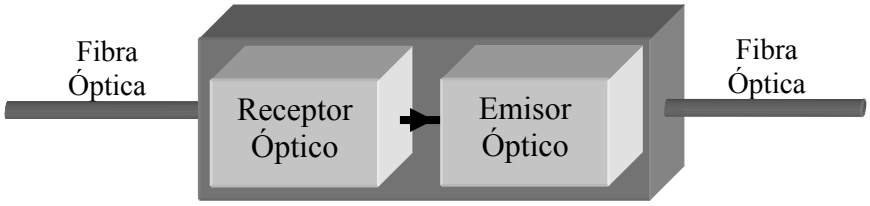


Figura II.19 *Repetidor Óptico*

El emisor óptico contiene la fuente de luz, que puede ser un diodo electro-luminiscente o un diodo láser. El emisor óptico contiene al receptor óptico, el cual puede ser un foto-diodo o un fototransistor. El emisor y el receptor ópticos están dotados de conectores que permiten acoplar la fuente y receptor de la luz a la fibra.

El canal de transmisión puede contener conectores que le permitan acoplar dos fibras entre sí (figura II.20)

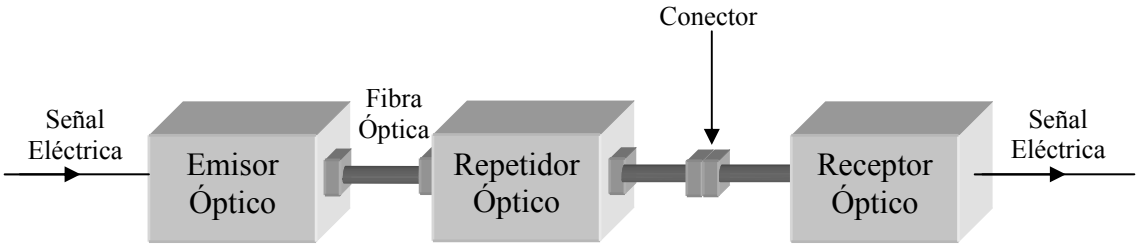


Figura II.20 *Sistema general de comunicación por fibra óptica con conectores*

II.1.4.2 TIPOS Y TRANSMISIONES DE SEÑALES

La fibra óptica es un medio de transmisión de información analógica o digital en la cual los principios básicos de funcionamiento se justifican de forma clara, aunque poco rigurosa, aplicando las **leyes de la óptica geométrica**.

II.1.4.3 MODOS DE PROPAGACIÓN

Los modos son ondas que se propagan en una fibra óptica y que siempre tienen componentes de campos eléctricos o magnéticos a lo largo del eje de la fibra. Los modos pueden subsistir en distancias que varían desde algunos milímetros hasta varios metros, en función de las fibras.

Las fibras se pueden clasificar por sus modos en:

Monomodo: Modo de propagación, o camino del haz luminoso, único.
Multimodo: Modo de propagación, o múltiples trayectorias de haces luminosos.

Para facilitar el uso de los términos, de ahora en adelante nos referiremos a los tipos de fibras ópticas como se encuentra regularmente en la literatura contemporánea, así para referirnos a las fibras monomodo lo haremos con SMF[1], y para las fibras multimodo nos referiremos con MMF[2]

II.1.4.4 CLASIFICACIÓN DE LAS FIBRAS ÓPTICAS

Una fibra óptica está constituida por dos cilindros concéntricos de materiales dieléctricos (figura II.21). Para que haya una propagación de la luz por reflexiones

[1] *SMF: Fibra Monomodo (Single-Mode Fiber)*
[2] *MMF: Fibra Multimodo (Multimode Fiber)*

internas totales, el índice de refracción n_1 del material que constituye el cilindro interior conocido como núcleo (core) debe ser ligeramente superior al índice de refracción del material que rodea al núcleo y que consta de otro cilindro exterior concéntrico de material de índice n_2 conocido como cubierta o vaina (cladding). El perfil del índice puede variar bruscamente en la interfaz núcleo-cubierta (fibra de índice escalonado) o aumentar gradualmente de la cubierta hacia el centro (fibra de índice gradual).

Finalmente se tiene un revestimiento que típicamente es un polímero conocido como cable. Un cable de fibra óptica o cable óptico puede contener una sola o muchas fibras. El cable óptico debe asegurar un medio ambiente adecuado para las fibras y facilitar su manejo; por lo menos, de manera tan fácil como la de los cables metálicos clásicos.

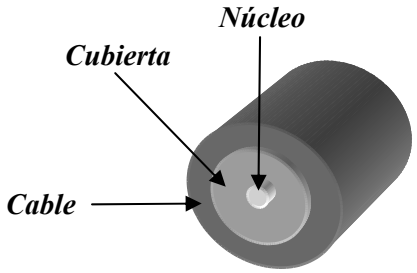


Figura II.21 *Fibra Óptica*

La fibra debe poseer un diámetro muy pequeño (generalmente 125 μm) y una longitud muy grande.

La fibra ideal no existe y sin embargo la tecnología de fabricación; tiende a optimizar todas estas características. Según la utilización que se haga de la fibra, algunas de estas características tienen mayor o menor importancia.

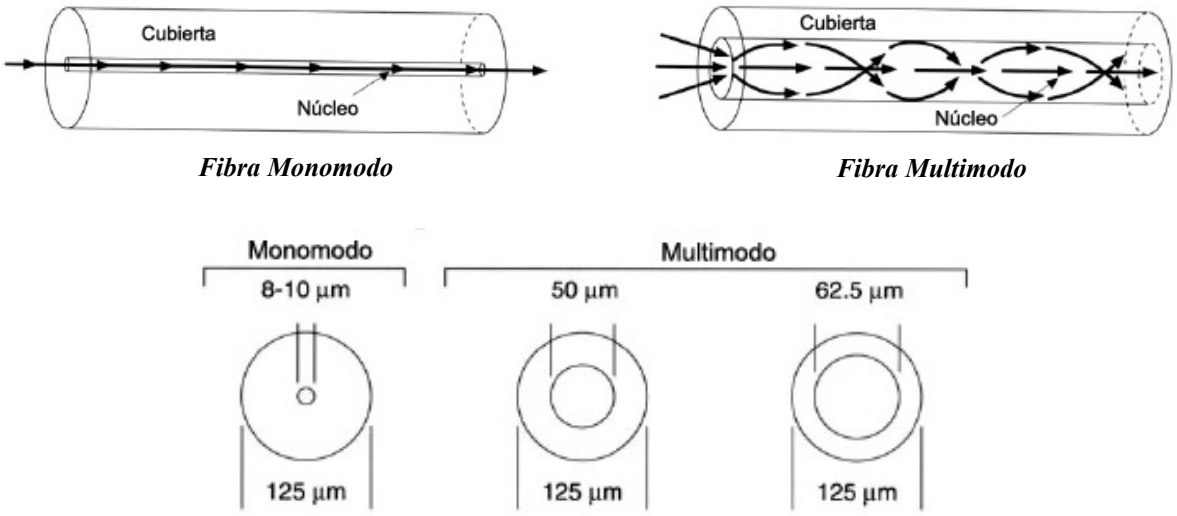
Las fibras ópticas tambien se pueden clasificar en:

POR MATERIALES DIELÉCTRICOS	***FIBRA ÓPTICA DE SILICIO*** ***FIBRA ÓPTICA DE VIDRIO MULTICOMPUESTO*** ***FIBRA ÓPTICA PLÁSTICA***
Por Modo De Propagación	*Fibra óptica Monomodo (SM)* *Fibra óptica Multimodo (MM)*
Por Distribución Del Índice De Refracción	*Fibra óptica de índice escalonado* *Fibra óptica de índice gradual*

Tabla II.21 *Clasificación de las fibras ópticas*

II.1.4.5 FIBRA MULTIMODO (MMF) Y MONOMODO (SMF)

La mayoría de las redes ópticas modernas utilizan SMF (figura II.22), la cual tiene un núcleo mucho más pequeño que las MMF (figura II.22). El pequeño tamaño del núcleo permite que una sola longitud de onda de luz pase, lo que asegura que no habrá problemas de traslape o distorsión en los datos, así mismo permite que esta alcance distancias 50 veces mayor que una MMF. Para dar una idea del tamaño en una SMF, el núcleo usualmente esta alrededor de los 8 a 10 μm de diámetro y la cubierta es 10 veces más gruesa con un diámetro de 125 μm. Una vez que se agrega el recubrimiento de polímero, el diámetro total de la fibra queda alrededor de los 0.25 mm. En cuanto a la MMF, el núcleo usualmente esta alrededor de los 50 a 62.5 μm y la cubierta al igual que la SMF, con un diámetro de 125 μm.



Fibra Monomodo ***Fibra Multimodo***

Figura II.22 *Tipos de Fibra Óptica*

II.1.4.6 TRES PRINCIPALES TIPOS DE FIBRAS

Existen tres diferentes tipos de fibras, las cuales se clasifican por su construcción como a continuación se verá:

FIBRA DE ÍNDICE ESCALONADO

Las MMF de índice escalonado están fabricadas a base de vidrio, con una atenuación de 30 dB/km, o plástico, con una atenuación de 100 dB/km. En estas fibras, el núcleo está constituido por un material uniforme cuyo índice de refracción es claramente superior al de la cubierta que lo rodea. El paso desde el núcleo hasta la cubierta conlleva por tanto una variación brutal del índice, de ahí su nombre de índice escalonado. Esta es la fibra conocida como clásica cuya fabricación es más fácil.

La fibra de índice escalonado puede no tener cubierta; es la más simple, pero también la de menor eficiencia (figura II.23).

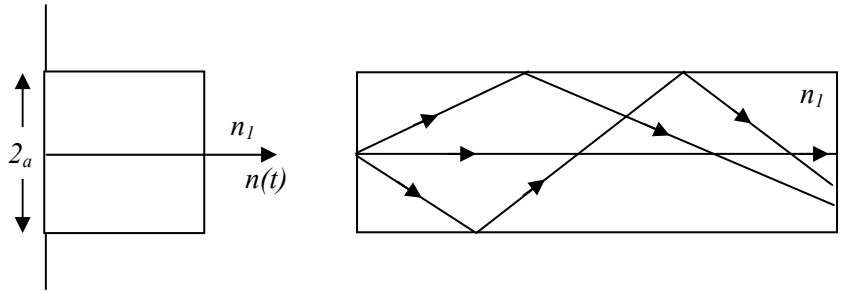


Figura II.23 *Fibra de índice escalonado sin cubierta.*

Esta fibra puede tener un diámetro 2a, hasta de 1 mm o más. La fibra de índice escalonado de buena calidad posee cubierta (Figura II.24).

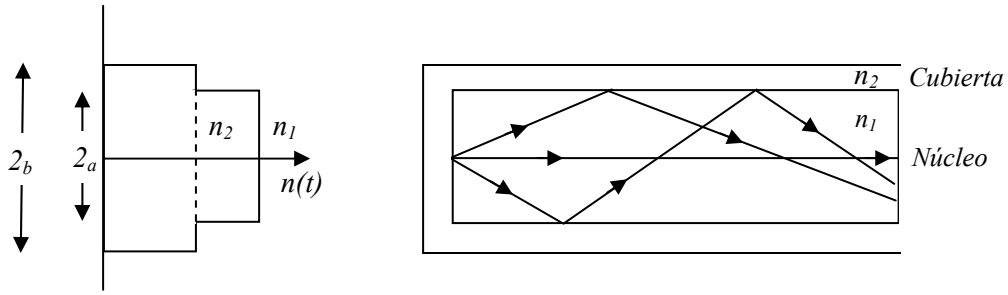


Figura II.24 *Fibra de índice escalonado con cubierta*

Estas fibras, son utilizadas por lo general para uniones de corta distancia, tienen diámetros del núcleo 2_a que varían de 10 a 200 μm y diámetros de cubierta 2_b que varían de 150 a 250 μm.

FIBRA DE ÍNDICE GRADUAL

El principio de las MMF de índice gradual se basa en que el índice de refracción en el interior del núcleo no es único y decrece cuando se desplaza del núcleo hacia la cubierta. Los rayos luminosos se encuentran enfocados hacia el eje de la fibra, como se puede ver en la figura II.25.

Estas fibras permiten reducir la dispersión entre los diferentes modos de propagación a través del núcleo de la fibra.

La fibra de índice gradual se utiliza en los enlaces de más alta capacidad de información.

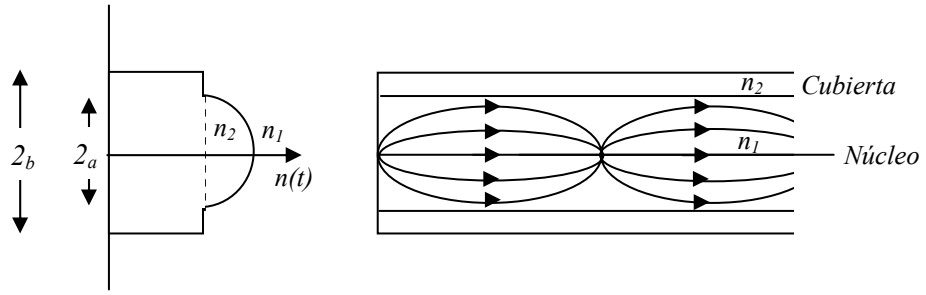


Figura II.25 *Fibra de índice gradual.*

El perfil del índice es pseudo parabólico. El diámetro del núcleo 2_a es generalmente de 50 μm y el de la cubierta de 125 μm.

FIBRA MONOMODO (SMF)

Potencialmente, esta es la fibra que ofrece la mayor capacidad de transporte de información. Las mayores velocidades de transmisión se consiguen con esta fibra, pero también es la más compleja de implantar. La figura II.26 muestra que sólo pueden ser transmitidos los rayos que tienen una trayectoria que sigue el eje de la fibra, por lo que se ha ganado el nombre de monomodo. Son fibras que tienen el diámetro del núcleo en el mismo orden de magnitud que la longitud de onda de las señales ópticas que transmiten. Si el núcleo está constituido de un material cuyo índice de refracción es muy diferente al de la cubierta, entonces se habla de fibras monomodo de índice escalonado. Las elevadas velocidades de transmisión que se pueden alcanzar constituyen la principal ventaja de las SMF, ya que sus pequeñas dimensiones implican un manejo delicado e implican dificultades de conexión que aún no se dominan del todo bien. Este tipo de fibra que promete en las telecomunicaciones a gran distancia una elevada eficiencia, todavía permanece dentro del campo de las investigaciones.

El diámetro del núcleo 2_a es de alrededor de 6 a 8 μm, mientras que el diámetro de la cubierta es de 125 μm. Para este tipo de fibra se consideran posibles bandas pasantes superiores a los 50 GHz por kilómetro.

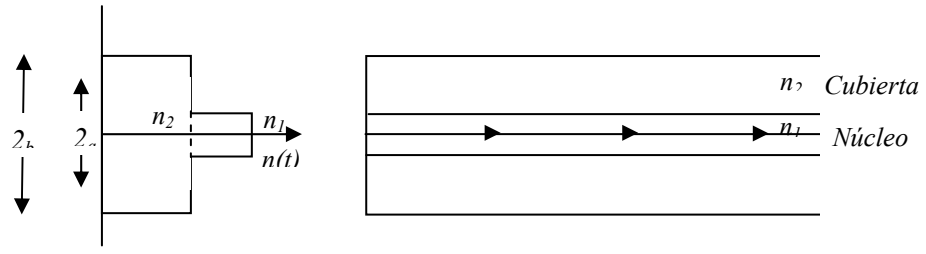


Figura II.26 *Fibra Monomodo.*

II.1.4.7 ATENUACIÓN EN LA FIBRA ÓPTICA

Son varios los mecanismos de degradación contribuyen a las pérdidas de energía en una fibra óptica, siendo unas de carácter intrínseco a la fibra, tal como la composición de vidrio, y otros de origen externo, causado por impurezas, defectos de cableado, de geometría de la fibra, etc. Para los fines que persigue el diseño de redes, nos enfocaremos en las pérdidas que pueda sufrir la fibra de origen externo, esto debido a que las causas de carácter intrínseco no serán determinantes para el diseño ya que la fibra que se adquiera para la implementación de una red deberá cumplir con los estándares de calidad. La atenuación se mide en decibeles por unidades de longitud (dB/km), y se puede clasificar en:

INTRÍNSECAS (DEL MATERIAL):

- Pérdidas por Absorción
- Pérdidas por Scattering Rayleigh
- Pérdidas por Scattering debido a una estructura no uniforme del núcleo.

EXTRÍNSECAS (INSTALACIÓN):

- **Pérdidas causadas por curvaturas**: Siempre que la fibra se somete a una curvatura por bobinado, tendido, etc., se origina una atenuación adicional por el hecho de que la interfaz núcleo-revestimiento deja de ser geométricamente uniforme, lo cual causa que no se cumpla el principio de reflexión total.

- **Pérdidas causadas por micro-curvaturas**: Los defectos que provocan las llamadas pérdidas por micro curvaturas son las irregularidades entre el núcleo y el revestimiento, las fluctuaciones de diámetro (error de elipticidad) y, fundamentalmente, las tortuosidades del eje de la fibra (error de concentricidad), esto puede ser causado por presión externa. Las pérdidas por micro-curvaturas, influyen en enlaces de largo alcance.

- **Pérdidas por empalmes**: Por preparación de empalme o conexión, Por corte defectuoso, suciedad de las superficies a empalmar, características distintas de la F.O., empalmes mecánicos (0.2 a 0.4 dB), empalmes por fusión (< 0.2 dB) valor típico (< 0.1 db), pérdidas de inserción del conexionado (0.3 a 0.8 dB), etc.

- **Pérdidas por acoplamientos:** Se puede presentar al conectar la fibra con aparatos receptores y transmisores.

- **Pérdidas por Radiaciones nucleares**: Otro factor de pérdidas son las radiaciones nucleares, sobre todo si no se trata de fibras dopadas con silicio sino con vidrios silicatados.

II.1.4.8 ATENUACIÓN TOTAL

Si se suman todas las pérdidas antes anunciadas, se obtiene una curva como la de la figura II.38, en la que se observa:

- Una zona por debajo de los 800 nm, que no es conveniente utilizar por ser de alta atenuación.
- Una zona por encima de los 1600 nm que presenta problemas de atenuación por el efecto de los rayos infrarrojos. Además, la tecnología de emisores y fotodetectores para esta longitud de onda es muy reciente.
- Tres zonas de mínima atenuación, denominadas ventanas, que determinan las longitudes de onda habituales para trabajar. Los primeros sistemas de fibra trabajaron en la primera ventana (850 nm). En este momento la zona de trabajo más habitual es la segunda ventana, en torno a los 1300 nm.

La tendencia actual es la utilización de laséres en la tercera ventana, en torno a los 1550 nm. La ventaja de esa utilización radica en una mayor vida del láser a medida que aumenta su longitud de onda.

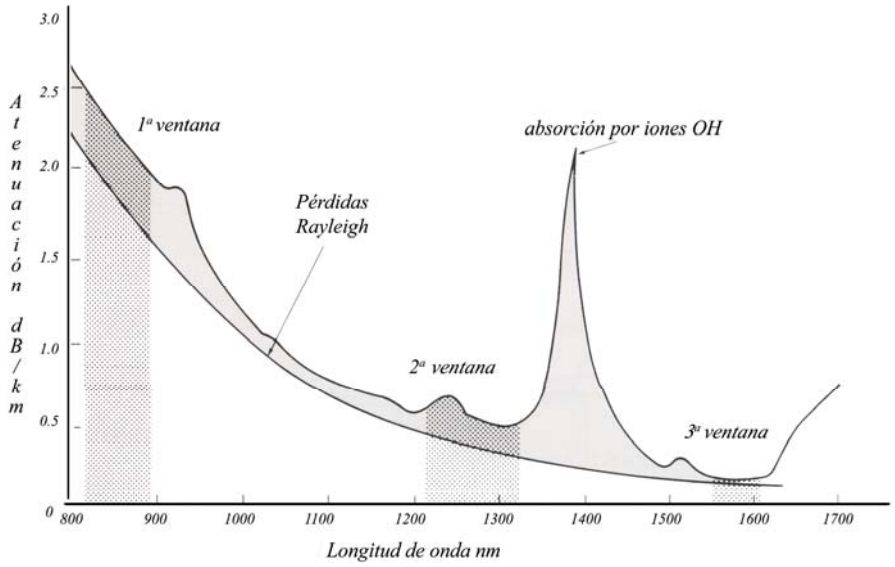


Figura II.27 *Pérdidas en una Fibra*

En la siguiente tabla se recogen las categorías de fibras multimodo según la recomendación G.651 del CCITT.

Longitud de onda	*Categoría*	*Atenuación [dB/km]*
850	1	≤ 4,0
	2	≤ 3,5
1300	3	≤ 3,0
	I	≤ 3,0
	II	≤ 2,0
	III	≤1,5
	IV	≤ 1,0
	V	≤0,8

Tabla II.22 *Categorías de fibras multimodo*

DISPERSIÓN

Si en la fibra se llega a producir un alargamiento en la duración de los pulsos luminosos, pueden mezclarse dos pulsos sucesivos diferentes en la entrada de la fibra y con esto hacer que la información se pierda. El alargamiento provocado por la fibra reduce de manera considerable, en este caso, la frecuencia máxima a la cual es posible emitir pulsos y, por tanto, limita la capacidad de una fibra para transportar información. Este parámetro es conocido como dispersión y define la capacidad máxima que, por unidad de longitud, se puede transmitir por una fibra.

En general hay tres tipos de dispersión y son:

- ***Dispersión Modal (o Intermodal)****:* Conocida como dispersión multimodo o MD[1], y solo afecta a las MMF, es causada por los diferentes modos (haces de luz) siguen rutas distintas en la fibra, esto provoca que los rayos recorran distancias diferentes en tiempos diferentes.

- ***Dispersión Cromática:*** La dispersión cromática también conocida como CD[2], se subdivide en dispersión espectral, intramodal o del material y en dispersión por efecto de guía de onda. Por lo que la dispersión cromática es la suma de ambas.

- ***Dispersión por Modo de Polarización:*** Este tipo de dispersión que también se le conoce como PMD[3], es introducido por las fibras que tienen una imperfección en la concentricidad. Como consecuencia,

[1] MD: Dispersión Modal (Modal Dispersion)
[2] CD: Dispersión Cromatica (Chromatic Dispersion)
[3] PMD: Dispersión por Modo de Polarización (Polarization Mode Dispersion)

diferentes polarizaciones de la señal óptica tienen diferentes retardos de propagación.

La dispersión modal y la dispersión espectral, son inherentes a las MMF, por el contrario, las dispersiones del material y de guía de ondas se refieren a cada modo.

ANCHO DE BANDA

El ancho de banda es la capacidad del medio para transportar la información, y esta, es inversamente proporcional a las pérdidas:

Mayor Ancho de Banda = Pérdidas mas bajas

La concepción y la realización de un sistema de comunicación óptica deben adaptarse al problema en particular a resolver. Es por tanto primordial conocer las características esenciales del enlace óptico a realizar, a fin de efectuar una selección juiciosa de los diversos elementos constitutivos. Lo anterior se verá con mayor detenimiento más adelante.

II.1.4.8 TRANSMISORES Y RECEPTORES ÓPTICOS PARA SISTEMAS DE TRANSMISIÓN DIGITAL

FUENTES ÓPTICAS

Entre las diferentes fuentes ópticas que existen, los diodos láser (LD) y los diodos emisores de luz (LED) son los únicos que satisfacen todos lo requerimientos exigidos por los sistemas de telecomunicaciones. Actualmente, la instalación de sistemas de comunicaciones por fibras ópticas se ha difundido ampliamente debido principalmente a dos factores: enorme capacidad de transmitir información, y costo relativamente bajo. Estos logros han sido posibles gracias a los grandes avances tecnológicos: desarrollo de fibras de vidrio con bajas pérdidas y grandes anchos de banda; desarrollo de dispositivos ópticos de alta calidad y confiabilidad (fuentes ópticas – LED, LD, detectores ópticos-PIN y APD).

Las fuentes han de emitir luz a una longitud de onda concordante con una de las ventanas de bajas pérdidas en la fibra, también deben cumplir otros requisitos no menos importantes:

- Bajo consumo.
- Alta fiabilidad con los cambios de temperatura.

- Pequeño tamaño.
- Alta potencia de salida y pobreza espectral suficiente en los casos de largas secciones de regeneración.
- La fuente debe admitir en su interior la modulación a la velocidad de transmisión del sistema, aunque últimamente puede obviarse esta condición acudiendo a moduladores exteriores a la propia fuente.

DETECTORES ÓPTICOS

El detector convierte la señal óptica que procede de la fibra en señal eléctrica como primera parte del proceso de recepción; a continuación, la señal se regenera, bien para llevarla a un equipo terminal o para ser incorporada a la siguiente etapa de un repetido óptico. Los detectores deben de tener:

- Alta sensibilidad (potencia mínima necesaria en la entrada del detector para obtener una tasa de errores menor de una prefijada).
- Bajo consumo y dimensiones físicas compatibles con la fibra óptica.
- Una baja tasa de errores típicamente menos de 10^{-10} para permitir la recuperación de la señal original.
- Bajo ruido.
- Características estables respecto al medio ambiente.
- Ancho de banda grande (respuesta rápida).

Existen básicamente dos tipos de fotodetectores de semiconductor, que se emplean en los receptores ópticos para sistemas de telecomunicaciones. El primero es comúnmente referido como fotodetector PIN y el segundo es referido como fotodetector de avalancha (APD).

En aquellas aplicaciones, donde se requiere una alta sensibilidad, se recomienda tener como receptores fotodetectores de avalancha; sin embargo los fotodetectores PIN, son los más comunes en los sistemas de transmisión por fibras ópticas.

En un sistema de transmisión digital por fibras ópticas, el transmisor óptico convierte una secuencia de pulsos eléctricos en una secuencia de pulsos ópticos, los cuales se transmiten a través de la fibra óptica. La señal sufre atenuación y distorsión antes de que la convierta en señal eléctrica el receptor óptico. La señal de salida del receptor óptico es una versión distorsionada del mensaje transmitido, por lo que debe procesarse por un regenerador con el fin de tener una réplica del mensaje y pueda retransmitirse si se requiere.

II.1.4.9 MODULACIÓN ÓPTICA

En una red óptica digital, los datos son representados por 1s y 0s. En redes eléctricas una corriente o voltaje eléctrico alto es representado por un "1", mientras que una corriente o voltaje eléctrico bajo, corresponde a un "0". Para crear estos pulsos desde una fuente constante de electricidad, un conmutador eléctrico muy rápido puede ser usado, otro camino que puede ser utilizado con el mismo fin de crear pulsos eléctricos puede ser encendiendo y apagando el apagador de la pared, repetidamente muy muy rápido.

Por otro lado, en el dominio óptico, nosotros tenemos un láser como una fuente de señal. En una operación regular, este láser esta entregando luz todo el tiempo. ¿Que se necesita?, lo que se requiere es algún tipo de capacidad de conmutación en orden para alterar este flujo constante dentro de un flujo de niveles de potencia altos y bajos, para representar la información en forma digital, este es el rol de la *modulación*, y por eso decimos que la luz necesita ser *modulada*.

II.1.4.10 RAPIDEZ DE TRANSMISIÓN

La tasa binaria de una transmisión es igual al número de elementos binarios o bits transmitidos por segundo, siendo su unidad el bit por segundo (bit/s); La rapidez de modulación de una transmisión es el número de intervalos unitarios transmitidos cada segundo, y su unidad es el baud. El código RZ, necesita dos intervalos unitarios por bit, mientras que el código NRZ utiliza un intervalo unitario por bit, si la tasa binaria es de 64 kbit/s (PCM con B = 4 kHz y cuantización de 7 bits, mas un bit de control), el canal de transmisión deberá tener una rapidez de modulación de 64 kilobaud en codificación NRZ, y de 128 kilobaud en codificación RZ.

II.1.4.11 DEMODULACIÓN

En la recepción, los pulsos codificados son demodulados mediante un convertidor digital analógico y se realiza la operación inversa de la que se efectúo al principio. A los sistemas que efectúan las operaciones de conversión analógica-digital (muestreo, cuantización) y digital-analógica, se les llama *codec* (codificador-decodificador).

II.1.4.12 TRANSMISIÓN DE VARIAS SEÑALES (MULTICANALIZACIÓN)

El rápido avance de la tecnología de las fibras ópticas, así como la introducción de las técnicas digitales, han hecho que se reconsidere el concepto de las redes de

comunicaciones, en la actualidad en varios países, los cables con conductores de fibras ópticas se han sometido a prueba en todos los niveles de los sistemas de comunicación, obteniendo resultados positivos, por lo que hay una constante investigación de nuevas técnicas para la transmisión por fibras ópticas.

Es importante transmitir al mismo tiempo varias señales, a esto se le llama *multiplex* o *multicanalización*. Una forma de hacer esto, sería utilizando un sistema de transmisión para cada señal; sin embargo, esta solución no es conveniente económicamente, por lo que es preferible transmitir los diversos mensajes por el mismo canal de transmisión (en este caso, la misma fibra óptica).

Debido a que esta tesis, se referirá solamente a sistemas modernos de telecomunicaciones, se omitirán las técnicas de multicanalización analógicas para fibras ópticas, ya que estas poco a poco se han ido descontinuando.

II.1.4.13 MULTICANALIZACIÓN POR DIVISIÓN

Una de las técnicas que permite transmitir por un mismo canal muchas señales digitales, es la Multicanalización por División de Tiempo (TDM *Time Division Multiplexing)*.

La multicanalización se realiza con un multiplexor que transmite, en serie, sobre la línea de transmisión los 8 bits del canal 1, después los 8 bits del canal 2 y así sucesivamente. Después de que se transmitió el canal décimo sexto, se envía el bit de sincronización y el multiplexor transmite los 8 bits de una nueva muestra del canal 17, una vez que se concluye con el envío de la trama de los 32 canales, se reinicia la secuencia. Al extremo receptor, un demultiplexor realiza la operación inversa, es decir, que envía los 8 bits de cada canal hacia una línea diferente donde se decodificarán. Lo anterior se verá con más detalle cuando se vean las jerarquías digitales.

Lo anterior se puede apreciar si se toma como ejemplo un sistema PCM[1] de 8 bits, la señal por transmitir es una señal telefónica (B= 4 kHz), la frecuencia de muestreo es de 2 B, o bien 8 kHz, lo que corresponde a un muestreo cada 125 μs (1/8kHz). Si cada bit dura 1 μs, entonces la transmisión de una muestra toma 8 μs, por lo que antes de la transmisión de otra muestra de esta señal, hay un tiempo de 117 μs (ya que el muestreo se da cada 125 μs menos los 8 μs que se toma una muestra), durante el cual el canal de transmisión no se utiliza. Este tiempo libre permite transmitir muestras de otras 14 señales telefónicas diferentes. En telefonía, existe un formato normalizado llamado E, en el cual se transmiten 256 bits durante

[1] PCM: Modulación por Codificación de Pulsos (Pulse Code Modulation)

los 125 µs, esto corresponde a 32 señales PCM codificadas con 8 bits, donde 2 de ellas se utilizan para señalización y sincronía (véase la figura II.28).

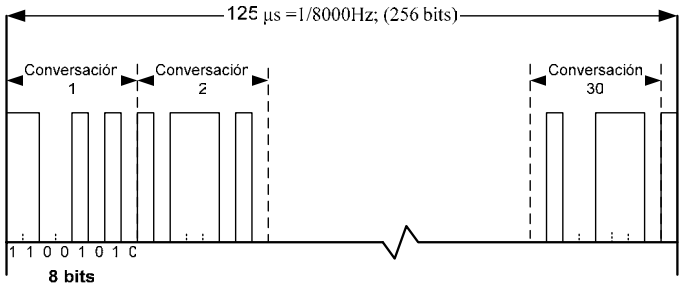


Figura II.28 *Multicanalización por división de tiempo (TDM). Formato E1 que permite multicanalizar 30 conversaciones telefónicas codificadas en PCM con 8 bits. [8bits x (30 conversaciones + 2 canales de señalización y sincronía)] x 8000Hz =2.048 Mbit/s*

El sistema de multicanalización antes descrito no es exclusivo para los sistemas de telecomunicaciones por fibra óptica.

II.1.4.14 MULTICANALIZACIÓN POR DIVISIÓN DE LONGITUD DE ONDA (WDM)

Debido a la lucha constante por desarrollar nuevas técnicas para el aprovechamiento más eficiente y económico de los medios de comunicación, los sistemas ópticos han desarrollado el Multiplexaje por División en Longitud de Onda WDM (*Wavelength Division Multiplexing)*; con el cual es posible que la capacidad de transmisión sobre una fibra óptica sea incrementado para transmitir múltiples longitudes de onda sobre una sola fibra y para lograr capacidades de transmisión del orden de terabits por segundo.

Las primeras redes WDM emplearon dos longitudes de onda: una en la ventana de los 1310 nm y otra en la ventana de los 1550 nm. Hoy en día los sistemas de WDM utilizan 16, 32, 128 o más longitudes de onda en la ventana de los 1550 nm y son comúnmente llamadas redes de Multiplexaje por División de Longitud de Onda Densa *(DWDM Dense Wavelength Division Multiplexing),* por que empaqueta de manera densa o compacta la longitud de onda.

Con esta técnica de multicanalización, todos los canales se transmiten simultáneamente y utilizan cada uno de ellos todo el ancho de banda del medio de transmisión. Se les asigna una longitud de onda en particular, por medio de un modulador electro-óptico, el cual convierte la señal eléctrica en energía luminosa,

con una longitud de onda específica, que se distribuye en forma simultánea en toda la fibra óptica.

Para alimentar la energía luminosa de la fibra, se utilizan dispositivos que se les llaman distribuidores selectivos de longitudes de onda, éstos tienen bastante aplicación en sistemas de distancias cortas y enlaces sin repetidores, un sistema completo con multiplexaje por longitud de onda se muestra en la figura II.29.

Los multiplexores de este tipo pueden ser unidireccionales o bidireccionales, en los multiplexores unidireccionales (figura II.29-a), las señales se transmiten en una misma dirección con varios portadores ópticos con diferentes longitudes de onda, los multiplexores bidireccionales (figura II.29-b) transmiten la información en dos sentidos sobre la misma fibra, utilizando diferente longitud de onda en cada sentido. Cada uno de los dispositivos del sistema WDM combina señales con una determinada longitud de onda para transmitirlas sobre la fibra, desde luego, también en el receptor se requieren dispositivos que separen estas señales.

Este tipo de sistemas básicamente se forman con:

- Fuentes ópticas. Estos elementos convierten la señal eléctrica en energía luminosa y la emiten con diferentes longitudes de onda.
- Multiplexores ópticos. Los multiplexores combinan la energía luminosa emitida por las fuentes ópticas para alimentarla a la fibra.
- Medio de transmisión. Esta es la fibra óptica que lleva la información separada por longitudes de onda, la cual debe tener baja atenuación para las longitudes de onda de interés.
- Demultiplexores ópticos. Dispositivos que separan la energía luminosa que le llega a través de la fibra por medio de la longitud de onda.
- Fotodetector. Este es el elemento que se encarga de hacer la conversión de energía óptica a señal eléctrica.

Las características que deben cubrir estos dispositivos son:

- Bajas pérdidas por inserción;
- Baja diafonía;
- Facilidad de fabricación;
- Fácil adaptación de conectores, para tener una transmisión directa;
- Tamaño pequeño;
- Alta confiabilidad.

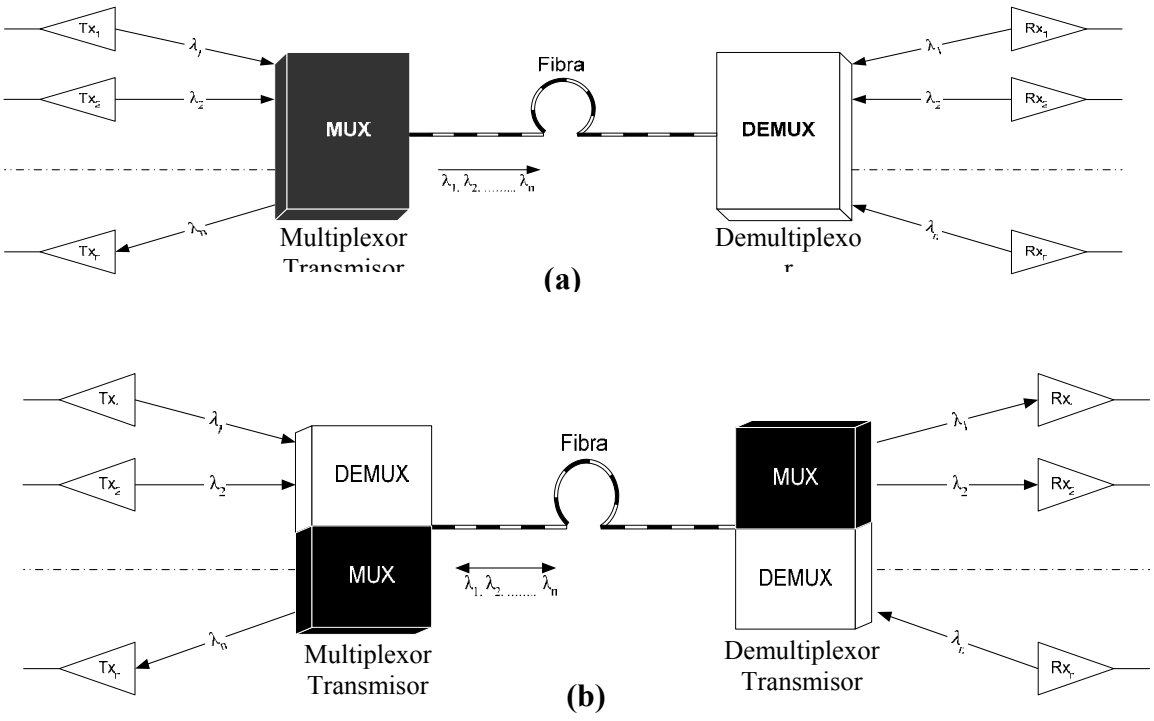


Figura II.29 *sistema de transmisión haciendo uso de multiplexación por división de longitud de onda, en configuración: (a) unidireccional y (b) bidireccional.*

El empleó de los multiplexores/demultiplexores depende del tipo de sistema. Los unidireccionales son sencillos, ya que sólo requieren óptica para el acoplamiento hacia las fibras de los haces luminosos que emiten las diferentes fuentes, y dispositivos de dispersión para separar las longitudes de onda.

Cuando se usan sistemas bidireccionales en los extremos del enlace se deben de tener multiplexores y demultiplexores, ya que en un sentido se deben de transmitir un número de longitudes de onda, así como también se debe ser capaz de recibir señales ópticas de diferentes longitudes de onda.

La Unión internacional de Telecomunicaciones (ITU) ha estado trabajando en estandarizar un conjunto de longitudes de onda para utilizarse en las redes WDM.

Esto es necesario para asegurar la interoperabilidad entres sistemas de distintos fabricantes, la recomendación de la ITU-T G.692, "Interfaces Ópticas para Sistemas Multi-Canal con Amplificadores Ópticos", define los parámetros ópticos para los sistemas DWDM utilizados entre oficinas y para aplicaciones de largo alcance *(long-haul)*, G.692 especifica sistemas de línea óptica con un máximo numero de canales de 4, 8, 16, 32, o mas longitudes de onda, transportando señales STM-4,

STM-16, o STM-64 sobre una fibra, utilizando cualquier transmisión uni o bidireccional.

Los sistemas WDM se utilizan en redes locales, en telecomunicaciones de larga distancia (entre troncales), en telecomunicaciones de banda ancha, tales como videoconferencias, videoteléfono, TV, audio y otros.

II.1.5 TECNOLOGÍAS DE MEDIOS INALÁMBRICOS

II.1.5.1 CARACTERIZACIÓN DEL CANAL DE RADIO (MODELO DE PROPAGACIÓN)

La caracterización ó el modelado de los canales de radio son una parte fundamental en el diseño de los sistemas de de las comunicaciones inalámbricas, esto se debe a que un canal de radio introduce ciertos factores que limitan la propagación de las ondas dentro de este, estas limitantes deben ser consideradas dado que la trayectoria entre un transmisor y un receptor de una transmisión inalámbrica puede variar de una simple línea de vista a una complicada trayectoria obstruida por diferentes obstáculos.

A diferencia de los canales alámbricos que son predecibles y estacionarios, los canales inalámbricos son extremadamente aleatorios y por lo tanto no es tan sencillo su análisis, es por eso que el modelado de los canales del radio, ha sido históricamente una de las partes más complicadas en el diseño de los sistemas de comunicaciones inalámbricas y móviles, y es típico, que para resolver el problema se haga una moda estadística, basada en algunas otras medidas hechas específicamente para un sistema de comunicación deseado.

La principal limitación que se considera en la caracterización de un canal de comunicación inalámbrico es la atenuación que experimenta la señal al viajar del transmisor al receptor. Como dijimos anteriormente la trayectoria que sigue una señal de radio de un transmisor a un receptor puede ser simplemente en lo que se conoce como línea de vista (LOS *line-of-sight*), en la cual la señal llega al receptor en línea directa sin pasar por obstrucción alguna.

Pero hay que considerar que en una transmisión inalámbrica también hay canales de comunicación en los cuales la trayectoria que sigue una señal hacia el receptor es indirecta, esto quiere decir que en el camino que recorre la señal, se atraviesan construcciones, estructuras y otro tipo de obstáculos que afectan a esta, y es cuando se dice que no hay línea de vista entre el transmisor y el receptor (N-LOS *No line-of sight*) y es el caso donde tenemos que considerar las diferentes causas de

perdida y atenuación a las que se ve expuesta la señal, dentro de las cuales principalmente se consideran la Reflexión, la Difracción, Dispersión y la Refracción, y que en conjunto producen aun más efectos de perdida.

La reflexión ocurre cuando en el camino, una señal electromagnética se encuentra con objetos que son mucho más largos que la longitud de onda de la señal.

La Difracción ocurre cuando la señal se encuentra con superficies irregulares como son los bordes afilados o esquinas.

La Dispersión ocurre cuando el medio a través del cual se propaga la onda contiene un gran número de pequeños objetos mas pequeños que la longitud de onda, esto produce que la onda electromagnética sea dispersa en muchas direcciones.

En general los modelos de propagación o caracterización de un canal de radio tienen por objetivo el predecir la potencia promedio que será recibida en el receptor a una distancia dada del transmisor, así como el obtener la variación de la potencia que se tiene en la proximidad de un lugar. De una manera mas sencilla si nosotros observamos la figura II.30, vemos una simple disminución de la potencia a medida que aumentamos la distancia.

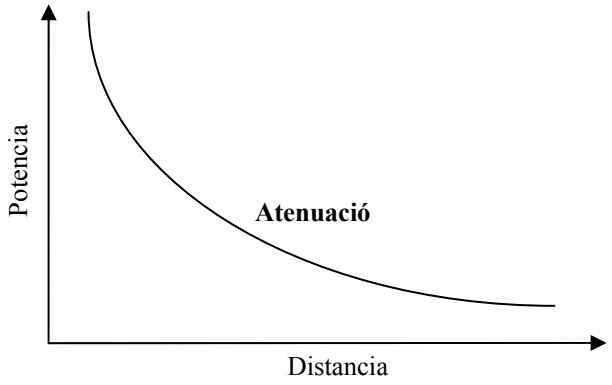


Figura II.30 *Pérdida de la potencia (Atenuación)*

Pero si ahora vemos la misma gráfica pero a una menor distancia de un par de kilómetros observamos que la potencia tiene varias fluctuaciones alrededor del valor promedio de la potencia de la señal, pero con la característica de que estas fluctuaciones tienen un largo periodo. Los modelos de propagación que describen a este tipo de fenómenos se les conocen como modelos de perdida de amplia-escala (*large – scale fading, large-scale loss ó long-term fading)*.

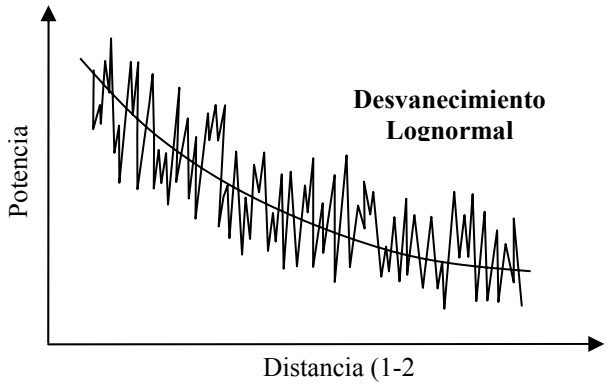


Figura II.31 *Pérdidas en Amplia-Escala*

Ahora bien si consideramos una menor distancia, veremos que las fluctuaciones de la señal de la potencia recibida cambia aun con mayor rapidez que en el caso anterior. Este fenómeno es descrito ahora por los llamados modelos de perdida de pequeña-escala (*Small-scale ó short-term fading)* y como dijimos se da en distancias cortas de unas cuantas longitudes de onda ó en intervalos de recepción pequeños, y en general están descritos en términos de la distribución de Rayleigh.

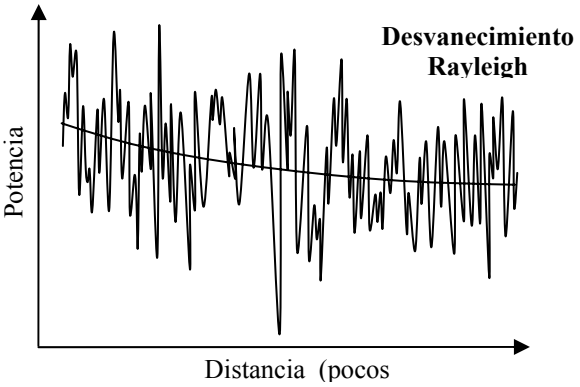


Figura II.32 *Pérdidas en Pequeña-Escala*

Ya sean modelos de amplia-escala ó pequeña-escala, cada modelo hecho para un sistema de comunicación inalámbrico toma en cuenta diferentes factores de pérdida, y principalmente aquellos que contribuyan más con esta, en la frecuencia que se desea trabajar. Mas adelante mencionaremos algunos de los modelos ó caracterización de canales de radio que se han hecho y que muchas veces son aceptados por otros sistemas de comunicación inalámbricos, debido a que estos ya toman en cuenta las pérdidas suficientes para considerar un buen modelo de canal a cierta frecuencia, además que ya no es necesario volver invertir tiempo en hacer una nueva caracterización del canal en la cual seguramente se obtendrán resultados bastante semejantes a los ya propuestos, y que como se dijo anteriormente estos no son tan sencillos de hacer.

II.1.5.2 MODULACIÓN

La modulación es el proceso mediante el cual la señal que contiene la información (señal en banda base) es modificada para ser transmitida. Esto involucra el paso de la traslación de frecuencia, en la cual su respuesta en frecuencia de la señal mensaje aparece como un filtro paso banda alrededor de la frecuencia portadora, donde la señal de la frecuencia portadora *c(t)* éste expresada como:

$$c(t) = A_0 \cos[2\pi f_0 t + \phi], \tag{II.4}$$

La modulación puede llevarse acabo, al variar la amplitud de la portadora A_0, cambiando la frecuencia de la portadora, ϕ, o cambiando la fase de la portadora, f_0, Estos esquemas de modulación son conocidos respectivamente como modulación en amplitud (AM), modulación en frecuencia (FM) y modulación en fase (PM).

La demodulación es el proceso inverso, el cual se enfoca en la extracción del mensaje en banda base de la portadora de tal manera que este pueda ser entendido por el receptor.

Ahora los esquemas de modulación pueden ser divididos primeramente en dos grandes grupos, los esquemas de modulación analógica y los esquemas de modulación digital, los primeros poco a poco han dejado de usarse tanto en los sistemas de comunicaciones móviles como en sistemas de comunicaciones de datos inalámbricos. Muchos de los sistemas de comunicaciones inalámbricos usan técnicas de modulación digital, donde la información es representada como una secuencia de pulsos, la modulación digital ofrece mayores ventajas que la modulación analógica como son: una mejor inmunidad al ruido, facilidad de multiplexación, compatibilidad con los procesos de señales digitales, etc.

MODULACIÓN DIGITAL

Aunque los sistemas de comunicación analógica son más simples y fáciles de implementar, los sistemas de modulación digital proveen una mejor alternativa para la transmisión de la información; esto no solo es debido por su incremento a la inmunidad al ruido, sino también a las ventajas que ofrecen los nuevos avances en las técnicas de procesamiento digital de señales, así como la disponibilidad de procesadores basados en microcircuitos VLSI.

Para las señales moduladas digitales, la señal modulante, $m(t)$, es una señal digital dada por los códigos de líneas binarios o de niveles múltiples. A continuación describiremos brevemente

SEÑALIZACIÓN PASABANDA DE MODULACIÓN BINARIA

Transmisión por cierre y apertura (OOK), también llamada transmisión por desplazamiento de amplitud (ASK), la cual consiste en activar desactivar una portadora senoidal una señal binaria unipolar. Es idéntica a la modulación binaria unipolar en una señal DSB-SC, la transmisión de radio del código Morse es un ejemplo de esta técnica. Por consiguiente, la técnica OOK fue una de las primeras técnicas de modulación que se utilizó y precede a los sistemas de comunicación analógicos.

Transmisión por desplazamiento de fase binaria BPSK, la cual consiste en desplazar la fase de una portadora senoidal portadora 0˚ a 180˚ con una señal binaria unipolar. Es equivalente a la señalización PM con una forma de onda digital y también es equivalente a modular una señal DSB-SC con una forma de onda digital polar.

Transmisión por desplazamiento de frecuencia (FSK), la cual consiste en desplazar la frecuencia de una portadora senoidal desde una frecuencia de marca (correspondiente, por ejemplo, al envío de un 1 binario) de acuerdo con la señal de banda base digital. Es idéntica modular una portadora de FM con una señal digital binaria.

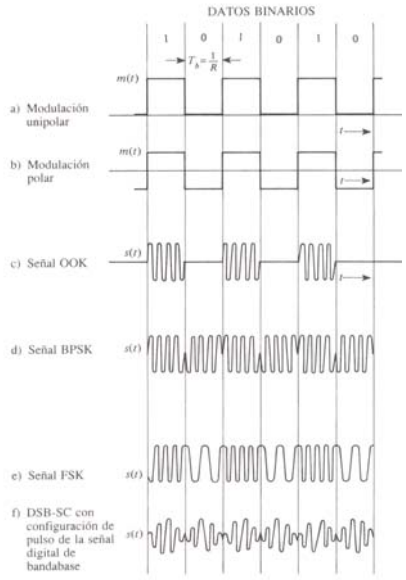


Figura II.33 *Señales pasabanda moduladas digitalmente.*

MODULACIÓN POR DESPLAZAMIENTO DE FASE EN CUADRATURA QPSK

Si el transmisor es un transmisor PM con una señal de modulación digital M=4 niveles, a la salida del transmisor se genera transmisión por desplazamiento de fase M-ario (MPSK). Una gráfica de los valores permitidos del envolvente compleja, $g(t) = A_c e^{j\theta(t)}$, contendría cuatro puntos, un valor de g (un número complejo general) por cada uno de los cuatro valores multinivel, correspondientes a las cuatro fases que se permiten tenga θ. Por ejemplo, con fases que los valores multinivel permitidos en el DAC son -3, -1, +1 y +3 V; entonces en la figura II.34a estos valores multinivel podría corresponder a las fases PSK de 0, 90, 180 y 270°, respectivamente. Y en la figura II.34b estos niveles corresponderían a las fases portadoras de 45, 135, 225, 315°, respectivamente, estas dos constelaciones de señales en esencia son las mismas excepto por un desplazamiento en la referencia de fase portadora. Este ejemplo de PSK M-ario en el que M=4 se llama señalización transmitida por desplazamiento de fase cuadratura (QPSK).

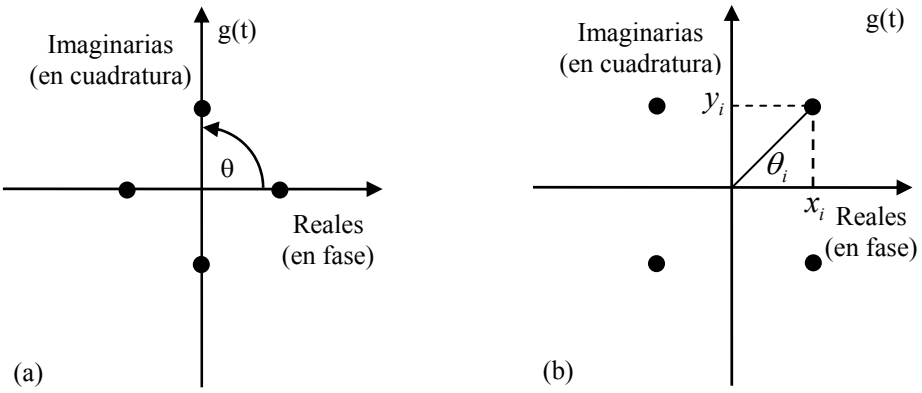


Figura II.34 *Constelaciones de señales QPSK*

MODULACIÓN DE AMPLITUD EN CUADRATURA (QAM)

La señalización por medio de la portadora en cuadratura, se llama modulación de amplitud en cuadratura (QAM), en general, las constelaciones de señales QAM no están limitadas en contar puntos de señalización sólo en un círculo (de radio A_c, como en el caso de MPSK). La señal QAM general es:

$$s(t) = x(t)\cos\omega_c t - y(t)sen\omega_c t \qquad \text{(II.5)}$$

donde

$$g(t) = x(t) + jy(t) = R(t)e^{j\theta(t)} \qquad \text{(II.6)}$$

Por ejemplo, en la figura II.35 se muestra una constelación QAM muy conocida hasta el 16 símbolos (M=16 niveles), donde la relación entre (R_i, θ_i) y (x_i, y_i) se puede evaluar con facilidad por cada uno de los 16 valores de señal permitidos, en este caso se permiten que x_i y y_i tengan cuatro niveles por dimensión, en esta señal QAM los 16 símbolos se pueden generar con dos convertidores (*l/2*=2) bit digital a analógico y modulador balanceados en cuadratura.

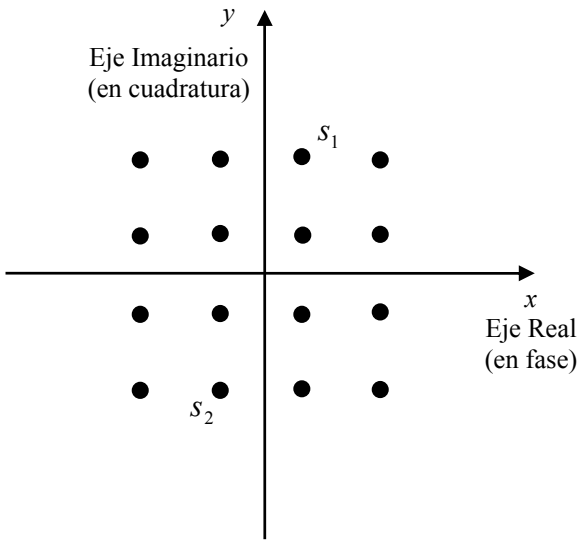


Figura II.35 *Constelación QAM de 16 bits*

MODULACIÓN POR DESPLAZAMIENTO DE FASE DIFERENCIAL DPSK

Con PSK normal hay una fase de referencia acerca de la cual la fase de la onda transmitida cambia cuando es modulada. Con este tipo de sistema, tanto el transmisor como el receptor tienen que mantener una referencia de fase absoluta contra la cual la señal recibida es comparada. Con Desplazamiento de Fase Diferencial (DPSK) la información es transmitida en forma de cambios de fase discretos, donde la referencia de fase es la fase de la señal de fase previamente transmitida. La ventaja de esta técnica es que una referencia de fase absoluta no tiene que ser mantenida.

El requisito de tener que mantener una fase de referencia absoluta que se presenta para PSK Y QPSK complica el conjunto de circuitos necesitado, especialmente para demodulación. Con Cambio de Fase Diferencial con clave no hay tal requisito ya que la fase de referencia no es absoluta, pero es la fase del bit previamente transmitido, esto significa que el conjunto de circuitos del demodulador requeridos son más simples que para PSK, o QPSK.

MODULACIÓN QPSK DIFERENCIAL (DQPSK)

De la misma forma que el cambio en DPSK es relacionado con el estado de la última fase transmitida, también lo es para DQPSK, excepto que hay cuatro fases de cambio posibles permitidas. La demodulación de señales DPSK puede ser lograda con un conjunto de circuitos más simple que para la demodulación de PSK o QPSK porque no se necesita referencia de fase absoluta. La referencia de fase es tomada de la fase del último bit recibido. Esto significa que circuitos de bucle de fase bloqueada, o de bucle de Costas no son requeridos.

La señal DPSK es pasado tanto a un detector de fase como a una línea de retardo de un período de bit, el detector de fase produce un voltaje de salida positivo cuando las fases de sus dos señales de entrada son la misma y una salida negativa cuando están en contrafase, así si la fase de la señal de entrada de DPSK es:

ããã00ã00

la entrada retrasada al detector será:

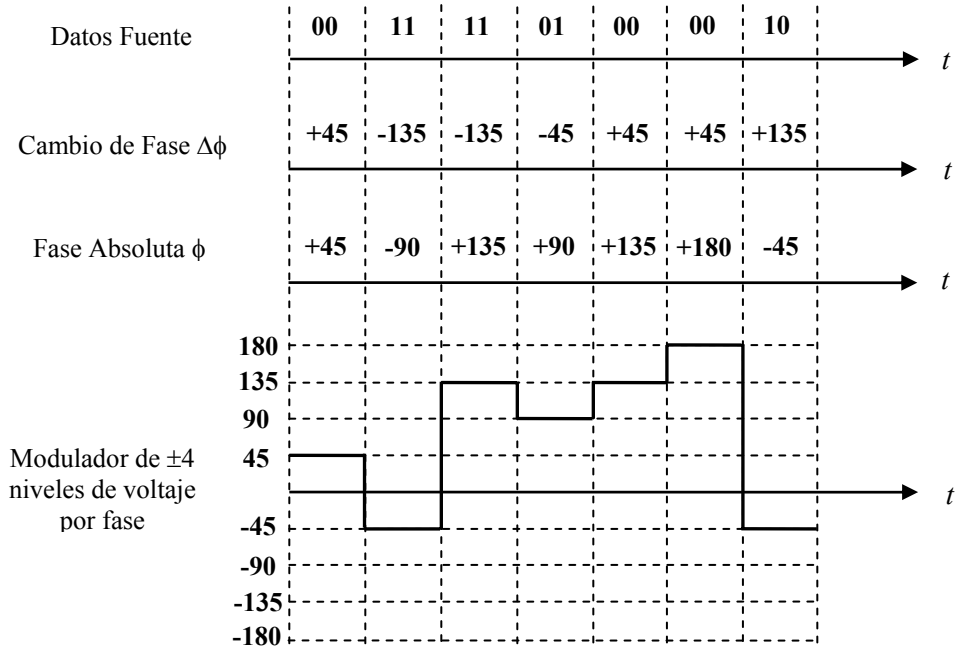
-ããã00ã0

(el estado del primer bit retrasado dependerá de que ha continuado antes, supondremos una condición inicial de 0) La acción del detector será:

- La entrada de DPSK ã ã ã 0 0 ã 0 0
- La entrada retrasada 0 ã ã ã 0 0 ã 0
- La salida del detector + - - + - + + -
- Equivalente a 1 0 0 1 0 1 1 0

que es la salida de información requerida.

La simplificación de los requisitos del circuito asociado con DPSK, y de aquí los ahorros en costos resultan, en la no necesidad de circuitos de bucle de fase bloqueada, etc. esto es balanceado por el hecho de que el desempeño señal a ruido es peor que para PSK. Esto es porque ambas entradas al detector de fase son ruidosas (si hay ruido en alguna habrá ruido retrasado en la otra) y así el estado de la salida del detector será susceptible a este ruido, esto empeora la relación señal a ruido de 2 a 3 dB. Una constelación posible para DQPSK es mostrada en el diagrama de abajo:



Figurra II.36 *Constelación de DQPSK para unos datos posibles*

CCK COMPLEMENTARY CODE KEYING

CCK es una modulación M-aria Ortogonal, la cual usa conjunto complejo de funciones de Walsh/Hadamard conocidas como códigos complementarios, esta modulación es un mapeo de bits como se define a continuación.

Tenemos que la entrada son los datos siguientes $(d_0, d_1, d_3, d_4, d_5, d_6, d_7)$, donde d_0 es el primer bit que llega, la modulación CCK primero mapea los bits del dato dentro de las fases por pares; el primer par (d_0, d_1) es mapeado diferencialmente, de acuerdo al dato previo, el cambio de fase es definido en la tabla II.23, el resto de los pares (d_i, d_{i+1}) son mapeados a las fases definidas en la tabla II.24.

Primer Par (d0, d1) (d0 es el primero)	Símbolos Pares Cambio de Fase (+jω)	Símbolos Impares Cambio de Fase (+jω)
00	0	Π
01	π/2	3π/2
11	Π	0
10	3π/2	π/2

Tabla II.23 *Tabla de codificación DQPSK*

Pares de bits (d_i, d_{i+1}) (d_i es el primero)	Fase
00	0
01	π/2
10	Π
11	3π/2

Tabla II.24 *Tabla de Codificación QPSK*

El proceso de mapeo puede ser considerado como un código de error de corrección extendido (8,3), sin embargo el cálculo es un campo Galois $GF(4)$, el código de palabras de CCK es determinado entonces por las 4 fases derivados de los bits de datos para obtener así un código de 256 palabras existente.

II.1.5.3 CODIFICACIÓN

Si los datos a la salida de un sistema de comunicación digital contienen errores que son demasiado frecuentes para el uso deseado, con frecuencia se reducen con el uso de una de dos técnicas principales.

- Solicitud de recepción automática (ARQ, por sus siglas en inglés: automatic repeat request)

- Corrección de errores de transmisión (anticipada) (FEC, por sus siglas en inglés: forward error correction)

En un sistema ARQ, cuando un circuito receptor detecta errores en un bloque de datos, solicita que se retransmita el bloque de datos; en un sistema FEC, los datos transmitidos se codifican de modo que el receptor pueda detectar y corregir los errores. Estos procedimientos también se clasifican como codificación de canal porque se utilizan para corregir errores provocados por el ruido presente en el canal, este procedimiento difiere de la codificación en la fuente, donde el objetivo de la codificación es extraer la información esencial de la fuente y codificarla a forma digital de modo que se pueda guardar o transmitir mediante técnicas digitales.

La codificación implica agregar bits adicionales (redundantes) a la corriente de datos de modo que el decodificador reduzca o corrija los errores a la salida del receptor. Sin embargo, los bits adicionales tienen la desventaja de incrementar la velocidad de transferencia de datos (bits/s) y, por ende, de incrementar el ancho de banda de la señal codificada.

Los códigos se clasifican en dos amplias categorías:

Códigos de bloque. Es una transformación de k símbolos binarios de entrada en n símbolos binarios de salida, por consiguiente, el codificador de bloques es un dispositivo sin memoria. Puesto que n>k, se selecciona la codificación que produzca redundancia, tal como bits de paridad, los cuales son utilizados por el codificador para corregir y detectar errores. Los códigos están denotados por (n,k), donde la velocidad de codificación r se define como r=k/n. los valores prácticos de r varían desde ¼ hasta 7/8, y k varía desde 3 hasta varios de cientos.

Códigos convolucionales. Un codificador que tiene memoria produce un código convolucional, el codificador convolucional acepta k símbolos binarios en su entrada y produce n símbolos binarios en su salida, donde los n símbolos de salida se ven afectados por v + k símbolos de entrada y se incorpora memoria porque v>0. La velocidad de codificación esta definida por r=k/n, los valores típicos de k y n varían desde 1 hasta 8, y los de v desde 2 hasta 60. La variación de r es entre ¼ y 7/8, un valor reducido de la velocidad de codificación r indica un alto grado de redundancia, lo que proporciona un control de errores más efectivo a expensas de incrementar el ancho de banda de la señal codificada.

CÓDIGOS DE BLOQUE

Antes de analizar los códigos de bloque, se precisan varias definiciones: El peso de hamming de una palabra de código es el número binario de 1 bit, por ejemplo, la palabra de código 110101 tiene un peso de hamming de 4; la distancia de hamming entre dos palabras de código, denotadas por d, es el número de posiciones en las cuales difieren, por ejemplo, la distancia entre las palabras de código 110101 y

111001 es de d=2, una palabra de código recibida se puede verificar para ver si contiene errores. Algunos de los errores se podrían detectar y corregir si d≥s+t+1, donde s es le número de errores que se puede detectar, y t es el número de errores que se puede corregir (s≥t), por consiguiente, si d≥2t+1 se puede detectar y corregir un patrón de t o unos cuantos errores.

CÓDIGO HAMMING

Hamming ideó un procedimiento para diseñar códigos de bloques con capacidad de corrección de error simple, un código hamming es un código de bloque que tiene una distancia hamming de 3, como d≥2t+1, t=1, y se puede detectar y corregir un error simple, sin embargo, se permiten sólo ciertos códigos (n,k), los códigos hamming permisibles son:

$$(n,k) = (2^m - 1, 2^m - 1 - m) \qquad \text{(II.7)}$$

Donde m es un entero y m ≥ 3. por tanto, algunos de los códigos permisibles son (7,4), (15,11), (31,26), (63,67) y (127,120); la proporción de codificación r tiende a 1 conforme m se va haciendo más grande.

Además de los códigos de hamming, existen muchos otros tipos de códigos de bloques, una clase muy aceptada se compone de los códigos cíclicos; los códigos cíclicos son códigos de bloques, de tal modo que se puede obtener otra palabra de código con cualquier palabra de código, desplazando los bits del lado derecho y colocándolos del lado izquierdo. Este tipo de códigos tienen la ventaja de ser muy fáciles de cifrar desde la fuente del mensaje por medio de registros de desplazamiento lineal baratos con retroalimentación, esta estructura permite también su fácil decodificación. Algunos ejemplos de códigos cíclicos y afines son los de Bose-Chaudhuri-Hocquenhem (bch), reed-salomon, hamming, y los códigos máxima longitud de reed-müller y golay.

CÓDIGOS BCH

Es una generalización de los códigos Hamming que permiten la corrección de múltiples errores, estos son una potente clase de códigos cíclicos que proporcionan una gran selección de bloques de longitud, índice de código, tamaño de alfabeto y capacidad de corrección de error.

El código BCH (Bose-Chaudhuri-Hocquenghem) es uno de los más importantes códigos de bloques lineales. En este código, los datos se dividen en bloques de k bits

de información: cada bloque representa cualquiera de los dos a la k de distintos mensajes. El codificador añade (n-k) bits y construye un bloque de n bits de longitud, que se conocen como bits de código, estos (n-k) bits añadidos son conocidos como bits redundantes, bits de paridad o bits de chequeo y no se usan para transmitir información. Este código es conocido como del tipo (n-k), la razón (n-K)/K dentro de un bloque se le conoce como la redundancia del código, y la razón de los bits de datos al número total de bits, k/, se le conoce como la razón de código.

La codificación de bloque es usada en la mayoría de los sistemas celulares del mundo; para AMPS (Adcance Mobile Pone Service) en Estados unidos, la longitud de palabra para el canal de forwading signaling es de 40 bits de longitud, cada palabra codificada de 40 bits, contiene 28 bits de datos y 12 bits de chequeo, y forma un (40, 28, 5) código BCH, aquí la distancia entre palabras código es de cinco. En el canal de reverse control la palabra se forma codificando 35 bits de datos en una palabra de código BCH de (48, 36) que también tienen una distancia de cinco (48, 36, 5), en ambos canales el bit de más a la izquierda se designa como el más significativo.

El código BCH es una generalización de los códigos Hamming que permiten la corrección de múltiples errores, estos son una potente clase de códigos cíclicos que proporcionan una gran selección de bloques de longitud, índice de código, tamaño de alfabeto y capacidad de corrección de error.

II.1.5.4 TÉCNICAS DE ACCESO AL MEDIO

Hay aplicaciones donde es necesario considerar la capacidad de acceso múltiple, la capacidad antiinterferenia, el rechazo de interferencia y la operación cubierta o la capacidad de baja probabilidad de intercepción (LPI, por sus siglas en inglés: *low probability of intercept*). Las últimas consideraciones son especialmente importantes en aplicaciones militares. Estos objetivos de rendimiento se pueden optimizar con técnicas de espectro amplio.

Existen muchos tipos de sistemas de Espectro Disperso (SS por sus siglas en ingles: spread spectrum), para que un sistema se pueda considerar como SS, el sistema debe satisfacer dos criterios.

1. El ancho de banda de la señal transmitida, s(t), tiene que ser mucho mayor que el del mensaje, m(t)
2. El ancho de banda relativamente amplio s(t) debe ser producido por una forma de onda modulante independiente, c(t), llamada señal difusora, y el

receptor debe conocer esta señal para que la señal del mensaje, m(t), pueda ser detectada.

Algunos se los tipos más comunes de señales de SS son:

- Secuencia Directa (DS, por sus siglas en inglés: direct sequence). En ésta se utiliza un DSB-SC de modulación difusora
- Salto de Frecuencia (FH, por sus siglas en inglés: frequency hopping). En ésta gc(t) es del tipo FM donde existen M=2k saltos de frecuencia determinados por las palabras de k-bits obtenidas a partir de la forma de onda de código difusor, c(t).
- Técnicas víricas que incluyen tanto DS como FH

DSSS

Supóngase que la forma de onda de información, m(t), proviene de una fuente digital y que m(t) es una forma de onda polar con valores de -+1.

El principio de funcionamiento es como sigue: Los datos fuente a transmitir se someten a una operación OR exclusiva con una secuencia binaria seudo aleatoria o secuencia PN(pseudo Noise) originando una secuencia de salida con una tasa mucho mayor que la tasa de datos fuente. La señal resultante es modulada y transmitida y ocupa una banda de frecuencia mucho mayor (esparcida o dispersa) que la banda original de los datos fuente.

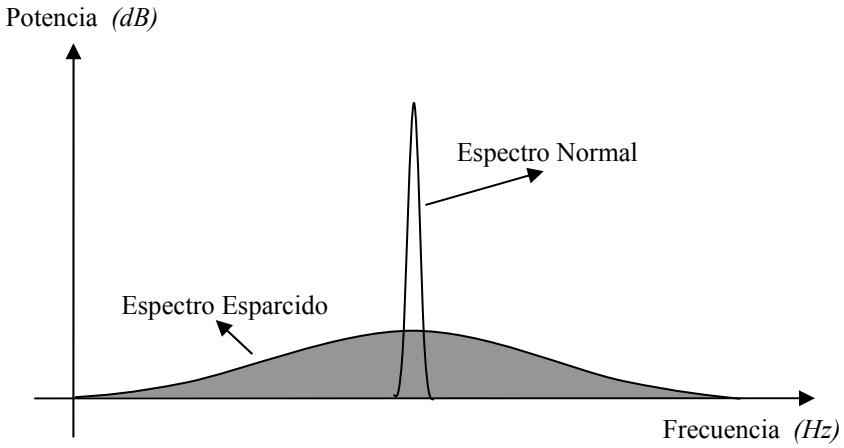


Figura II.37 *Espectro de Banda Esparcida*

Para los demás dispositivos que estén operando en la misma banda de frecuencia, esta señal aparece como (pseudo) ruido, todas las estaciones pertenecientes a la misma LAN tienen la misma secuencia PN por lo que sus transmisiones pueden interferirse mutuamente, entonces es preciso usar entonces un método de acceso al medio apropiado que asegure que sólo se realizará una sola

transmisión en un momento dado, esto será considerado más adelante. Ahora se hará un breve análisis sobre la secuencia seudo aleatoria mejor conocida como PN

SECUENCIA BINARIA PSEUDO ALEATORIA

Cada periodo de la secuencia PN está formado por N dígitos o "chips" de duración Ts. Las secuencias PN no se producen espontáneamente sino que son generadas por métodos artificiales lo que permite la reproducción de secuencias PN idénticas que son imposible de lograr con secuencias aleatorias de cualquier otro tipo.

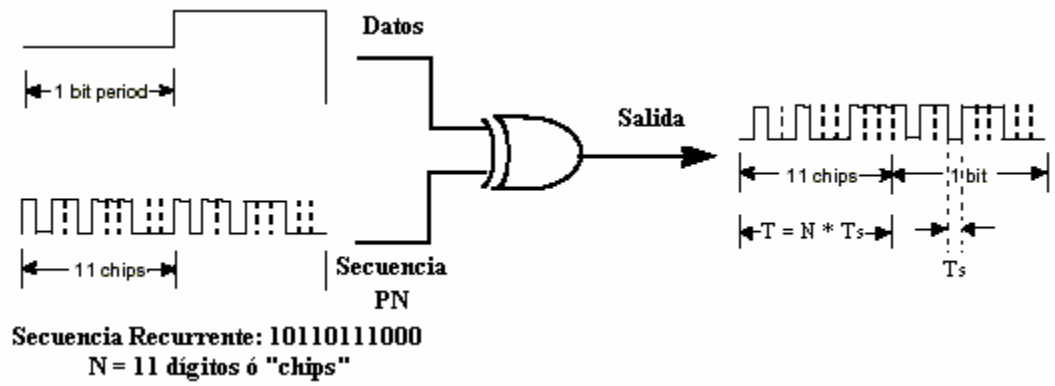


Figura II.38 *Secuencia binaria Pseudoaleatoria*

La secuencia PN se genera mediante registros de desplazamiento y compuertas OR exclusiva conectadas en un lazo de retroalimentación.

FHSS

En los sistemas FHSS la señal digital a transmitir, generalmente FSK o DPSK, vuelve a modular una portadora cuya frecuencia cambia constantemente de acuerdo con una secuencia PN

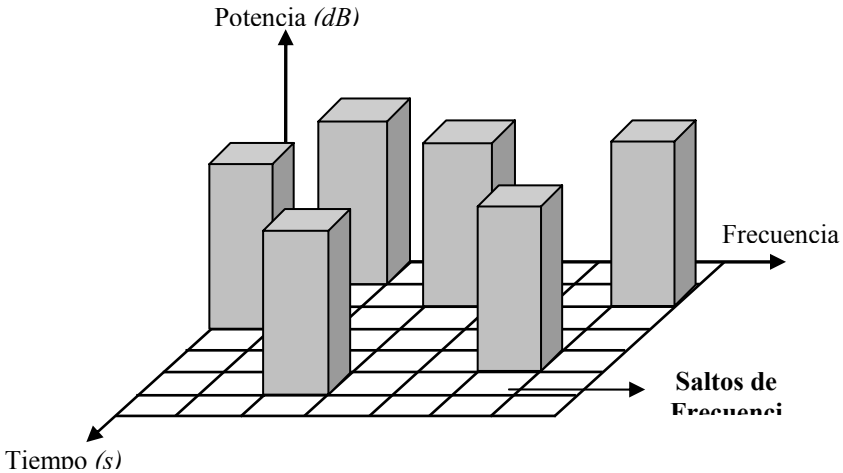


Figura II.39 *Banda Esparcida por Saltos de Frecuencia*

La cantidad de frecuencias es igual a $M = 2^k$, donde *k* es el número de "chips" tomados de una secuencia PN, por ejemplo, si k=8, habrá 256 frecuencias de portadora diferentes que serán moduladas por la señal FSK o DPSK. Esto significa que durante un intervalo de tiempo T se utiliza una de M frecuencias y en el intervalo siguiente se cambia o salta en forma aleatoria a cualquiera otra de las M-1 frecuencias. Se reduce así el efecto de interferencia pues en el caso de existir una, ella tendría efecto solamente en uno de los M intervalos de tiempo.

Las frecuencias de portadora se generan en un sintetizador de frecuencia que es controlado por *k* "chips" tomados de una secuencia PN. En la práctica en valor de *k* es igual al número de etapas n del generador de las secuencias PN. Estas frecuencias cambian cada T seg.

II.1.5.5 INFRARROJOS

Dentro de las redes de datos inalámbricas, existen las redes de datos que utilizan los rayos infrarrojos como medio de transmisión. Estas redes pueden ser divididas de acuerdo al ángulo de apertura con que se emite la información en el transmisor, estos sistemas de infrarrojos pueden clasificarse en sistemas de corta apertura, también llamados de rayo dirigido o de línea de vista (*Line of Sight*, LOS de la misma manera que los sistemas de radiofrecuencia) y en sistemas de gran apertura, reflejados o difusos (*diffused*).

La tecnología de infrarrojos cuenta con muchas características sumamente atractivas para utilizarse en redes de datos inalambricas, y otras que no lo son tanto. Las longitudes de onda de operación se sitúan alrededor de los 850-950 nm, es decir, a unas frecuencias de emisión que se sitúan entre los 3,15·10e14 Hz y los 3,52·10e14

Hz. Las cuales son frecuencias cercanas a la de la luz y, por lo tanto, con un comportamiento similar, es decir, no pueden atravesar objetos sólidos como paredes, por lo cual es un sistema seguro contra receptores no deseados, aunque esta característica también supone un serio inconveniente a su capacidad de difusión. Asimismo, y debido a su alta frecuencia, presenta una fuerte resistencia a las interferencias electromagnéticas artificiales radiadas por otros dispositivos.

En cuanto a las restricciones de uso, la transmisión de infrarrojos con láser o con diodos no requiere autorización especial en ningún país, excepto por los organismos de salud que limitan la potencia de la señal transmitida. Y, por último, y como atractivo reclamo todo tipo de fabricantes, utiliza componentes sumamente económicos y de bajo consumo energético, importantes características muy a tener en cuenta en aquellos dispositivos que deban formar parte de equipos móviles portátiles.

Entre las limitaciones principales que se encuentran en esta tecnología se puede señalar que es sumamente sensible a objetos móviles que interfieren y perturban la comunicación entre emisor y receptor. Además, las restricciones en la potencia de transmisión limitan la cobertura de estas redes a unas cuantas decenas de metros, y lo que de aún más grave, la luz solar directa, las lámparas incandescentes y otras fuentes de luz brillante pueden interferir seriamente la señal.

CARACTERIZACIÓN DEL CANAL

Al igual que en los sistemas de comunicación de radiofrecuencia la caracterización del canal para los rayos infrarrojos son sumamente complicados de realizar y en los cuales también cada modelado considera diferentes factores, entre los cuales tenemos: las dimensiones del cuarto donde esta en funcionamiento el sistema, el tipo de materiales que cubren las paredes, y la posición tanto del transmisor como del receptor, etc. Dentro de los modelados la mayoría son de los llamados Indoor ya que por su naturaleza de los rayos infrarrojos y como se menciono anteriormente su mayor aplicación de estos son en habitaciones o cuartos cerrados.

Dentro de estos un canal infrarrojo difuso es un canal multitrayectoria, que al igual que el canal de RF (interior) produce dispersión temporal en las señales transmitidas, pudiendo causar interferencia entre símbolos (ISI), la cual a su vez limita la capacidad del sistema.

A diferencia del canal de RF, el canal infrarrojo difuso, es un canal que no produce desvanecimiento Raleygh, la explicación de esto es debido a que; los foto detectores en los sistemas infrarrojos difusos tienen dimensiones típicas que

alcanzan el centímetro cuadrado, y en consecuencia, en ellos caben aproximadamente diez mil longitudes de onda de la luz utilizada en estos sistemas, lo cual produce la suficiente diversidad espacial, como para que la potencia de la señal recibida sea promediada a la salida, ver la figura II.40.

En receptores de detección directa, la potencia total recibida integrada sobre el área del fotodetector permanece prácticamente constante, aunque el detector se mueva sobre cientos de longitudes de onda. La principal causa de desvanecimiento en los sistemas infrarrojos es el sombreado.

Otros problemas a enfrentar cuando se diseñan sistemas infrarrojos difusos, son los siguientes: el ruido óptico causado por los sistemas de iluminación ya sea naturales o artificiales y las limitaciones de potencia óptica impuestas por cuestiones de seguridad ocular y por la poca disponibilidad de energía eléctrica en los dispositivos portátiles.

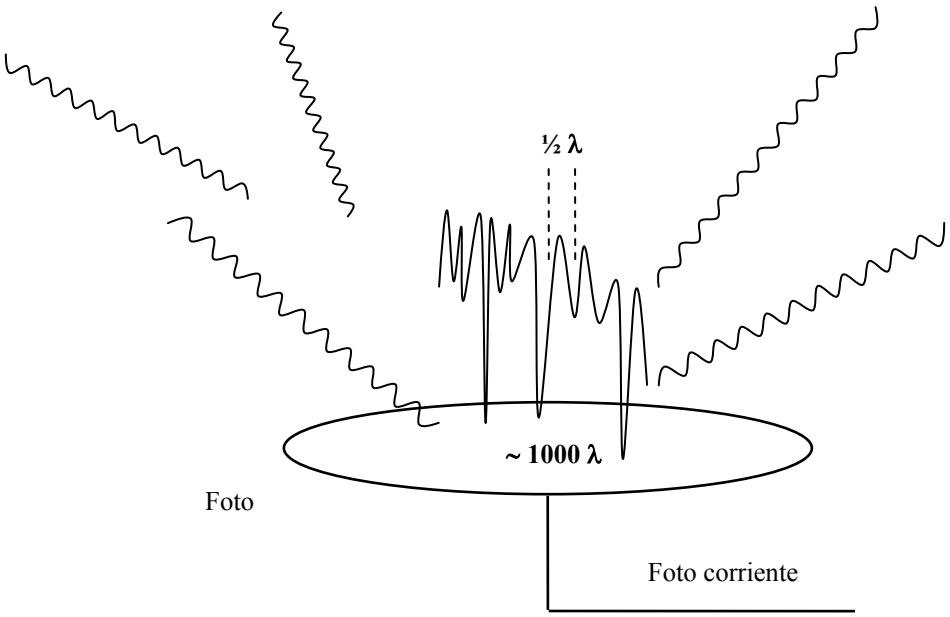


Figura II.40 *Efecto de las multitrayectorias en el foto detector de un sistema infrarrojo difuso*.

En general la propagación multitrayectoria en el canal infrarrojo difuso, queda completamente caracterizada por la respuesta al impulso h(t) de dicho canal porque, para una posición dada de emisor y del receptor, el canal puede considerarse estacionario ya que este varía muy lentamente comparado con la velocidad de transmisión de los símbolos.

La respuesta al impulso, puede ser interpretada como una función de retardo de potencia, y por lo tanto puede ser tratada como una función de densidad de retardo, produciendo información útil acerca de las características del canal. Por ejemplo

podemos calcular la desviación estándar de este perfil de retardo, que es referido como dispersión de retardo rms. El recíproco de esta dispersión de retardo rms, es una medida del ancho de banda coherente del canal.

II.1.5.6 SISTEMAS INFRARROJOS

Los sistemas de infrarrojos de corta apertura funcionan de manera similar a los controles remotos de los televisores. Mediante este sistema, el emisor debe orientarse hacia el receptor antes de transferir información, lo que supone que entre el transmisor y el receptor debemos tener linea de vista y lo que limita un tanto su funcionaldad a solo enlaces punto a punto y no móviles.

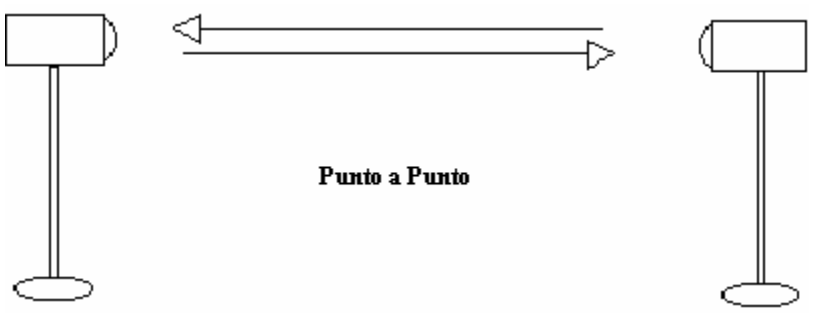


Figura II.41 *Enlace Infrarrojo Punto a Punto*

Los sistemas de gran apertura permiten la transmisión de información en un ángulo mucho más amplio, por lo que el transmisor no tiene que estar alineado con el receptor. Una topología muy común para redes locales inalámbricas basadas en esta tecnología, consiste en colocar en el techo de la oficina un nodo central llamado punto de acceso, hacia el cual los dispositivos inalámbricos dirigen su información, y desde el cual ésta es difundida hacia esos mismos dispositivos. A esta topología también es conocida como transmisión cuasi-difusa.

Desgraciadamente, la dispersión utilizada en este tipo de red hace que la señal transmitida rebote en techos y paredes, introduciendo un efecto de interferencia en el receptor que limita notablemente la velocidad de transmisión.

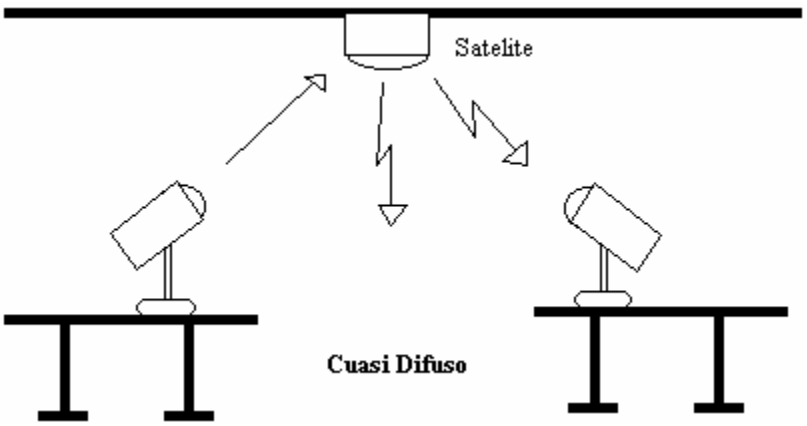


Figura II.42 *Enlace Infrarrojo Difuso*

II.1.5.7 FUNCIONAMIENTO DE LA CAPA FÍSICA PARA WLAN

FUNCIONALIDAD DE LA CAPA FÍSICA

La Capa Física es la interfase entre la capa MAC y el medio inalámbrico, la cual transmite y recibe tramas de datos sobre un medio inalámbrico compartido. La Capa Física provee tres niveles de funcionalidad: primero, la Capa Física provee un frame de intercambio entre la subcapa de MAC y la Capa Física, bajo el control de la subcapa PLCP (*physical layer convergence procedure*). Segundo, la Capa Física define las señales portadoras a utilizar y la modulación de los frames de datos a transmitir sobre el medio, lo cual es la función de la subcapa PDM (*physical medium dependent*). Y tercero, la Capa Física provee una señal de censado a la subcapa de MAC para verificar la actividad en el medio.

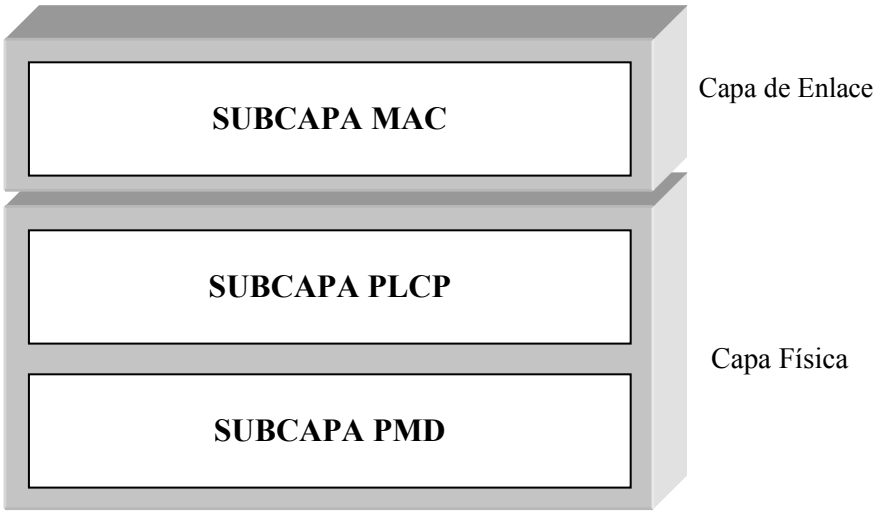


Figura II.43 *Modelo OSI para WLANs*

DIRECT SEQUENCE SPREAD SPECTRUM (DSSS)

El DSSS es usado en la banda de frecuencia de los 2.4GHz. La transmisión de los datos sobre el medio es controlado por la subcapa PDM así como por la subcapa PLCP. La subcapa PDM toma los bits binarios de información provenientes de la subcapa PLCP (*PLCP Protocol Data Unit* PPDU) y los transforma en señales de radio frecuencia y ponerlos en el medio utilizando la técnica de DSSS.

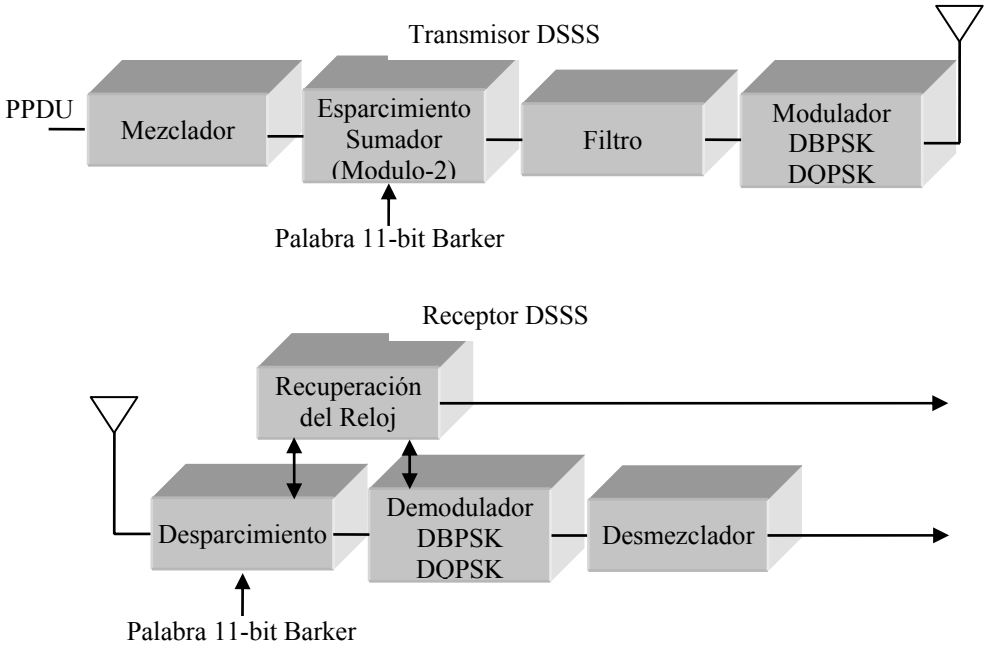


Figura II.44 *Transmisor y Receptor para DSSS*

El PPDU es único para la técnica de DSSS dentro de la capa Física. El frame PPDU consiste de un preámbulo del PLCP, un encabezado del PLCP y una unidad de información proveniente de la subcapa de MAC (*MAC protocol data unit* MPDU). El preámbulo PLCP y el encabezado PLCP son siempre transmitidos a 1 Mbps, y el MPDU puede ser enviado a 1 o 2 Mbps.

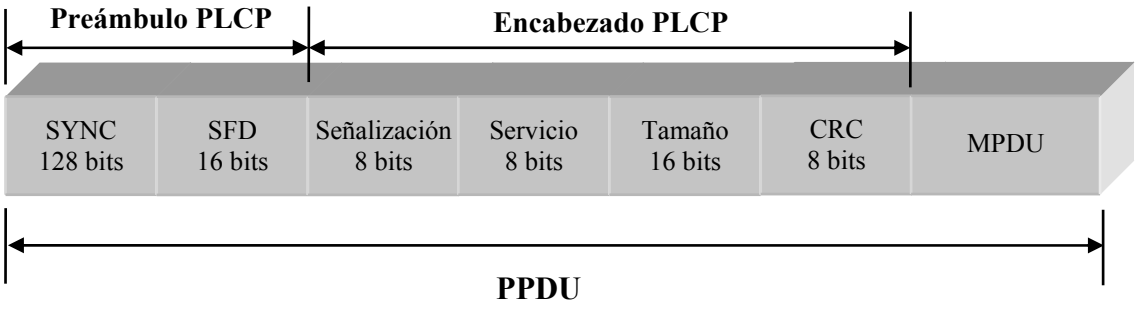


Figura II.45 *Preámbulo y Encabezado para DSSS*

Sync: Es un campo de 128 bits, el cual contiene un string de 1s, el cual son bits revueltos que son enviados previos a la transmisión. El receptor usa este campo para obtener la señal de llegada y sincronizar la señal del receptor y cronometrar antes de recibir el SFD *(Start of frame delimiter)*

SFD: Es el campo que contiene información que marca el inicio de un frame PPDU. El SFD comúnmente es la siguiente palabra hexadecimal F3A0 hex, la cual esta definida comúnmente para todos los radio trasmisores que trabajan bajo el 802.11 DSSS.

Signal: El campo de la señal define que tipo de modulación puede ser usada para recibir la llegada del MPDU. El valor binario en este campo es igual a la tasa de datos multiplicada por 100Kbit/s. Hay dos tasas que son soportadas la 0Ah para 1 Mbps para DBPSK y 14hex para 2Mbps para DQPSK.

Service: El campo de servicio esta reservado para usos futuros y por defecto es siempre 00h.

Length: El campo de distancia es un número no definido de 16 bits que indica el número de microsegundos necesarios para transmitir el MPDU. La capa de MAC usa este campo para determinar el fin de un frame PPDU.

CRC: El campo del CRC contiene los resultados de un calculo de un frame check que es enviado por la estación base. El algoritmo CRC-16 esta representado por la siguiente función polinomial $G(x) = x16 + x12 + x5 + x1$. EL receptor hace los cálculos de la señal de llegada, de loa campos de service y length y compara los

resultados con los valores transmitidos. Si un error es detectado, la capa MAC del receptor hace la decisión si el PPDU de llegada debe ser terminado.

FCS: Es el campo del MPDU que es la porción del PPDU que protege la información en la unidad de servicio del PLCP (PLCP service data unit PSDU). Con la técnica de DSSS la Capa Física no determina si hay errores presentes en el MPDU. La capa MAC hace una determinación similar al método usado por la capa Física.

MEZCLADO DE DATOS

Todos los bits de información que son transmitidos por el PMD son revueltos usando un self-synchronizing 7-bit polinomial.

El polinomio utilizado es $G(z) = z^{-7} + z^{-4} + 1$, el cual es utilizado para poner los datos aleatoriamente dentro del campo SYNC del PLCP .

MODULACIÓN DSSS

El PDM transmite el preámbulo PLCP y el encabezado a 1Mbps usando DBPSK. El MPDU es enviado a cualquiera de las dos tasas de transmisión 1Mbps en DBPSK o 2 Mbps DQPSK, dependiendo del contenido en el campo de la signal del encabezado PLCP. DPSK no es coherente, y la referencia de reloj no es necesaria para recobrar los datos. DBPSK es más tolerante a la interferencia intersimbolos causada por el ruido y las multitrayectorias sobre el medio; es por eso que BBPSK es usado para el preámbulo PLCP.

THE FREQUENCY HOPPING SPREAD SPECTRUM (FHSS)

La trasmisión sobre el medio es controlada por la subcapa PMD así como por la subcapa PLCP para la técnica de FHSS. La subcapa PMD toma los bits de información del PSDU y los transforma en señales de radiofrecuencia y los pone en el medio inalámbrico valiéndose de la modulación de la portadora y técnicas de FHSS.

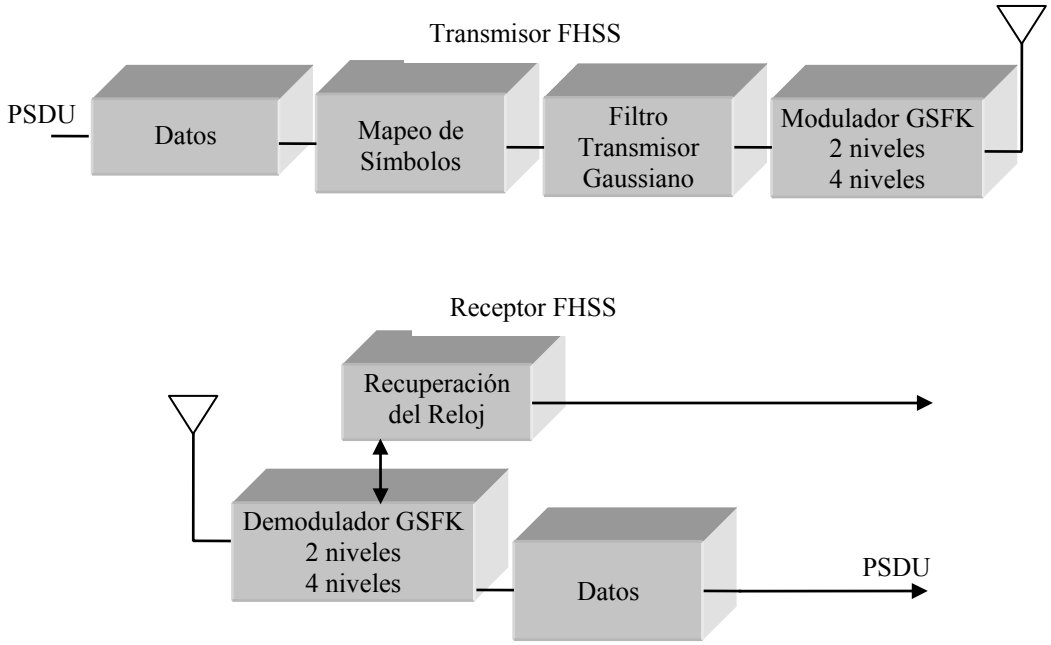


Figura II.46 *Elementos Básicos de un Transmisor y Receptor para FHSS*

SUBCAPA PLCP PARA FHSS

El preámbulo del PLCP es usado para obtener la señal entrante. Y sincronizar el demodulador del receptor.

Sync: Es el campo que contiene un string de un patrón de 1s y 0s que es usado por el receptor para sincronizar el reloj de los paquetes recibidos y la frecuencia correcta.

SFD: Es el ampo que contiene la marca de información del comienzo de un PSDU. Un SFD dentro de la IEEE 802.11 es especificado para todos los radios y usa el siguiente string de bits 0000110010111101.

PWL: Es el campo que especifica la longitud del PSDU en octetos y es usado por la subcapa MAC para detectar el fin de un frame PPDU.

***PSF* (*PLCP signaling fiels*):** Este campo identifica la tasa de transmisión del PSDU, que va de 1Mbps a 4.5Mbps en incrementos de 0.5Mbps.El preámbulo PLCP y el encabezado son transmitidos a una tasa de transmisión de 1Mbps. Y la tasa de transmisión para el PSDU opcional puede ser de 2Mbps.

Header Check Error: Este campo contiene los resultados de un calculo del frame que es sometido a un calculo de verificación y que es enviado por la estación

base. El algoritmo de detección de error CCIT CRC-16 es usado para proteger los campos de PSF y PLW. La subcapa MAC hace la determinación de la correcta recepción del frame PPDU comprobando el FCS que es incluido al final de la porción PSDU del PPDU.

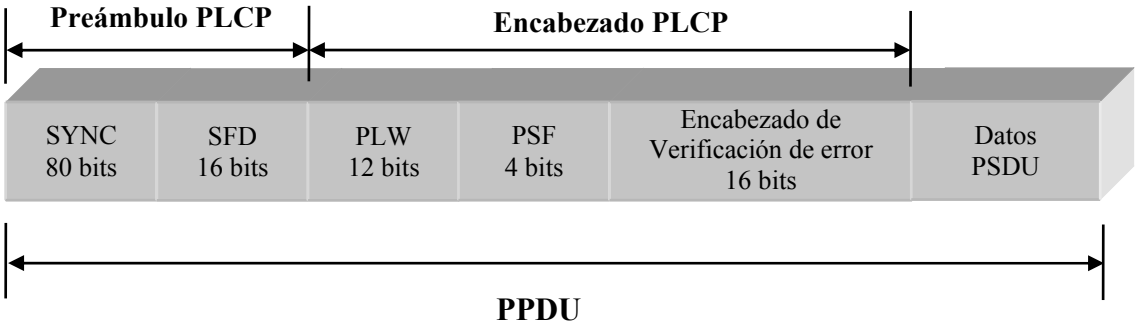


Figura II.47 *Preámbulo y Encabezado para FHSS*

BLANQUEADO DE LOS DATOS PSDU

Los datos son primeramente aplicados al PSDU antes de la transmisión para minimizar los perjuicios de DC en los datos en caso de que contenga largas series de 1s ó 0s. La capa Física llena un símbolo especial cada 4 octetos del PSDU en un frame PPDU. Una secuencia generadora de 127 bit que usa el polinomio $S(x) = x7 + x4 + 1$ y 32/33 supresión de perjuicio de algoritmo de codificación son usados para aleatorizar y decodificar los datos.

MODULACIÓN FHSS

El 802.11 usa 2 niveles de GFSK en el PMD para transmitir los PSDU a una tasa de transferencia de 1Mbps. El preámbulo del PLCP y encabezado son siempre transmitidos a 1Mbps. Sin embargo, 4 niveles de GFSK son utilizados como modulación opcional para transmitir los PSDU a tasas mayores. El valor contenido en el campo PSF del encabezado PLCP es usado para determinar la tasa de transferencia del PSDU.

GSFK es una técnica de modulación, la cual desvía la frecuencia a cualquiera de los dos lados del salto de la portadora, dependiendo si el símbolo binario del PSDU es un 1 o 0. Un ancho de banda usado para el periodo del bit es (Bt)=0.5. Los cambios en la frecuencia representan símbolos que contienen la información del PSDU.

Para 2 niveles del GFSK, un bit 1 representa una desviación superior en la frecuencia para el salto de la portadora, y un bit 0 representa una desviación inferior

de la frecuencia. El salto de frecuencia debe ser mayor que 110KHz. La desviación de la frecuencia de la portadora esta daba por:

Binary 1 = F*c* + f*d*
Binary 0 = F*c* – f*d*

Para 4 niveles de GFSK es similar a la de 2 GFSK y es usada para conseguir una tasa de transferencia de 2Mbps en el mismo ancho de banda ocupado. El modulador combina 2 bits del PSDU y los codifica dentro de un par de símbolos (10, 11, 01, 00). Los pares de símbolos generan 4 desviaciones de frecuencia de los saltos de la portadora, 2 superiores y 2 inferiores. Los pares de símbolos son transmitidos a 1Mbps, y para casa bit enviado el resultado es una tasa de transferencia de 2Mbps.

SALTO DE CANAL PARA FHSS

Una determinada secuencia de saltos esta definida por el IEEE802.11 para uso de la banda de frecuencia de los 2.4 GHZ. Los canales son igualmente espaciados con ancho de banda de 83.5MHz. El salto de los canales depende de cada ciudad.

El salto de los canales es controlado por la subcapa PMD. La subcapa PMD transmite los datos del PSDU por un salto de un canal a otro usando una de las secuencias de salto pseudoaleatoria.

II.2 CAPA DE ENLACE

La capa de enlace de datos asegura el direccionamiento por hardware de los dispositivos y entrega el frame "trama" al dispositivo correcto, así como traduce mensajes de datos de capas superiores a frames, provee control de flujo a la capa 2 y lleva a cabo una FCS Secuencia de Verificación de Tramas (*Frame Check Sequence*) para asegurarse de que el frame recibido es idéntico a el transmitido.

II.2.1 TECNICAS DE ACCESO AL MEDIO

Es una necesidad para el control de tráfico en un cable de red, evitar que los paquetes de datos choquen y sean destruidos. Al conjunto de reglas que gobiernan cómo la computadora pone los datos en el cable de red es llamado método de acceso. El método de acceso previene de accesos simultáneos al cable. El método de acceso usa tres principales sistemas para realizar esto:

- Un método de sensación y detección de colisión.
- Un método de token passing.
- Un método de prioridad de demanda.

Con el método CSMA/CD, las computadoras escuchan el cable de red, cuando no hay tráfico, envían datos. La detección de colisión es un método de contención, lo cual significa que la computadora compite por una oportunidad para enviar datos. CSMA/CD puede ser un método lento cuando hay tráfico pesado en la red. Con el método de evitar colisiones CSMS/CA, cada computadora envía una señal al intentar transmitir y justo antes de enviar los datos. Este método es mas lento que de detección.

En una red token passing, una computadora toma el control de un token cuando desea transmitir datos, los cuales anexa al token. Cuando recibe confirmación de que han sido recibidos los datos, libera un nuevo token. Solo una computadora a la vez puede usar el token, por lo tanto, no hay colisiones.

En el método prioridad de demanda, solo hay comunicación entre la computadora que envía, el hub y la computadora de destino. La transmisión es bajo un control centralizado del hub, y la señal no es distribuida a todas las computadoras en la red.

II.2.1.1 DE CONTENCIÓN

PROTOCOLO DE ACCESO AL MEDIO CSMA/CA Y MACA

El algoritmo básico de acceso al medio para wireles LAN es el llamado CSMA/CA (por sus siglas en ingles *Carrier Sense Multiple Access / Collision Advoidance*). Este algoritmo funciona tal y como se describe a continuación:

1. Antes de transmitir información una estación debe comprobar la disponibilidad del medio, o canal inalámbrico, para determinar su estado (libre / ocupado).

2. Si el medio no esta ocupado por ninguna otra trama la estación ejecuta una espera adicional llamada espaciado entre tramas (IFS por sus siglas en ingles *Interface Space*).

3. Si durante este intervalo temporal, o bien ya desde el principio, el medio se determina ocupado, entonces la estación debe esperar hasta el final de la transacción actual antes de realizar cualquier acción.

4. Una vez finaliza esta espera debida a la ocupación del medio la estación ejecuta el llamado algoritmo de *backoff*, según el cual se determina una espera adicional y aleatoria escogida uniformemente en un intervalo llamado ventana de contienda (CW por sus siglas en ingles *Continuos Wave*). El algoritmo de *backoff* nos da un número aleatorio y entero de ranuras temporales (*slot time*) y su función es la de reducir la probabilidad de colisión que es máxima cuando varias estaciones están esperando a que el medio quede libre para transmitir.

5. Mientras se ejecuta la espera marcada por el algoritmo de *backoff* se continúa escuchando el medio de tal manera que si el medio se determina libre durante un tiempo de al menos IFS esta espera va avanzando temporalmente hasta que la estación consume todas las ranura temporales asignadas. En cambio, si el medio no permanece libre durante un tiempo igual o superior a IFS el algoritmo de *backoff* queda suspendido hasta que se cumpla esta condición.

Cada retransmisión provocará que el valor de CW, que se encontrará entre CWmin y CWmax se duplique hasta llegar al valor máximo, por otra parte el valor del spot time es 20μseg.

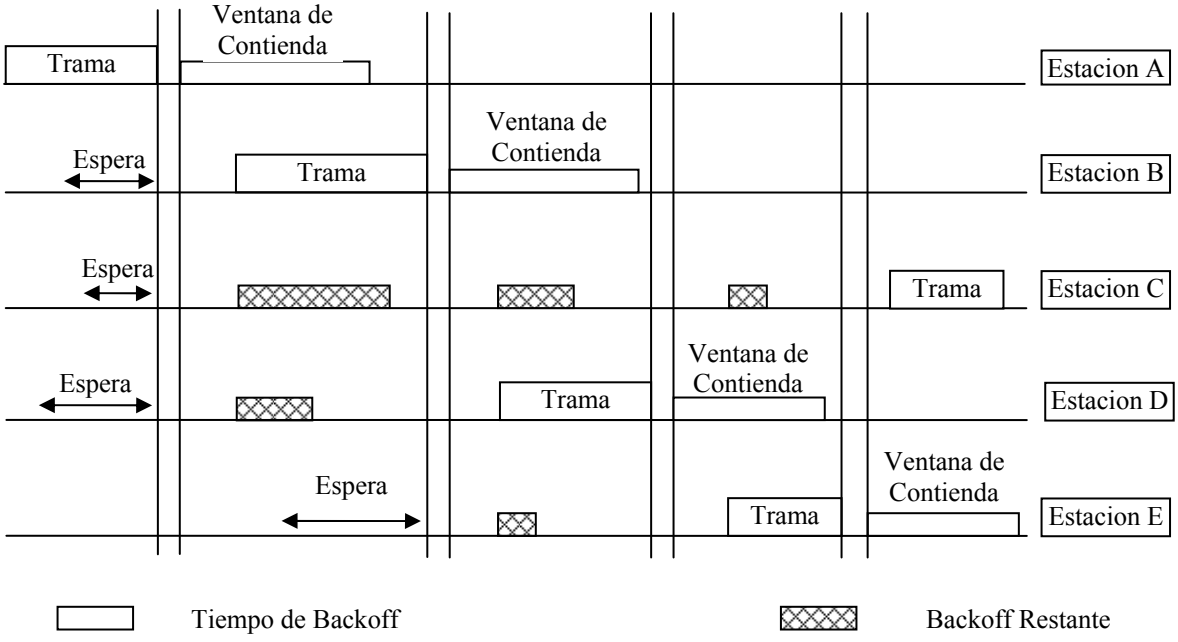


Figura II.48 *Funcionamiento de Acceso al Medio CSMA/CA*

Sin embargo, CSMA/CA en un entorno inalámbrico y celular presenta una serie de problemas que intentaremos resolver con alguna modificación. Los dos principales problemas que podemos detectar son:

- *Nodos ocultos.* Una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo que no oye.
- *Nodos expuestos.* Una estación cree que el canal está ocupado, pero en realidad está libre pues el nodo al que oye no le interferiría para transmitir a otro destino.

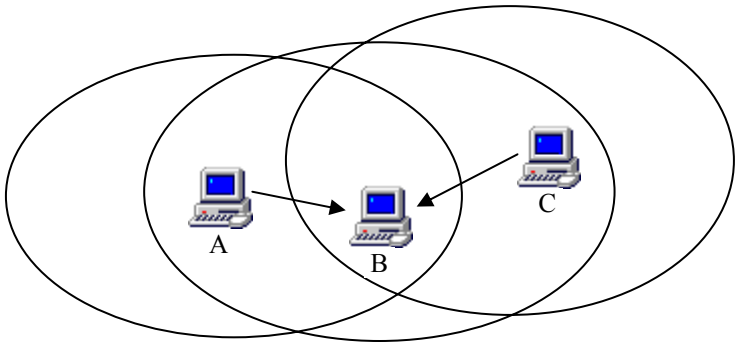


Figura II.49 *El problema del nodo oculto A y C no se alcanzan a escuchar entonces si ambos transiten al mismo tiempo a B las tramas pueden ser corrompidos*

La solución que se da a este problema es el protocolo MACA (*MultiAccess Collision Avoidance*)

Según este protocolo, antes de transmitir el emisor envía una trama RTS (*Request to Send*), indicando la longitud de datos que quiere enviar. El receptor le contesta con una trama CTS (*Clear to Send*), repitiendo la longitud. Al recibir el CTS, el emisor envía sus datos.

Los nodos seguirán una serie de normas para evitar los nodos ocultos y expuestos:

- Al escuchar un RTS, hay que esperar un tiempo por el CTS
- Al escuchar un CTS, hay que esperar según la longitud

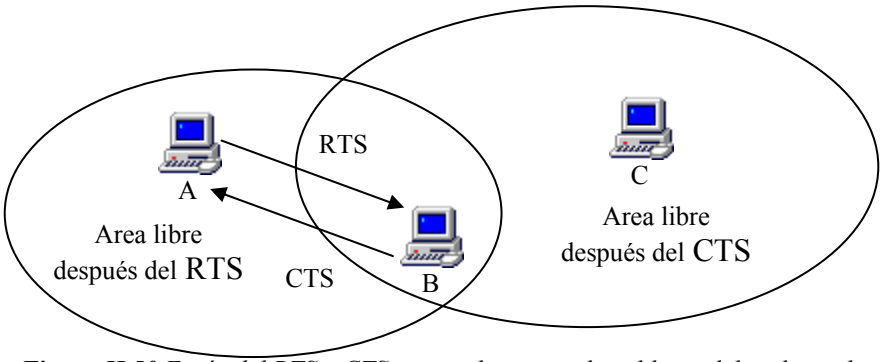


Figura II.50 *Envío del RTS y CTS para solucionar el problema del nodo oculto*

IEEE 802.3 CSMA/CD.

Fue a finales de los años 60 cuando la universidad de Hawai desarrolló el método de acceso CSMA/CD, empleado por primera vez en la red de área extendida ALOHA, en la que se basa la Ethernet actual. En 1972, Ethernet experimentó un fuerte desarrollo en Xerox, donde se conoció como Experimental Ethernet. Esta empresa pretendía unir 100 PC's en una distancia de 1 Km. El diseño tuvo mucho éxito y su popularidad creció.

DEFINICIÓN.

El procedimiento más probado para controlar una red de área local con estructura en bus es el acceso múltiple por escucha de portadora con detección de colisiones, CSMA/CD, que se puede clasificar como un sistema de prioridad y con detección de portadora. La versión más extendida de este método, es la de la especificación Ethernet. Está diseñado para cubrir redes de ordenadores de oficina, especializadas y de baja velocidad y grandes distancias, transportando datos a alta velocidad para distancias muy limitadas.

ETHERNET VS CSMA/CD.

Ambas LANs, Ethernet y IEEE 802.3 son redes de difusión, lo que significa que todas las estaciones ven todos los paquetes, sin tener en cuenta si representan un destino determinado. Cada estación debe examinar los paquetes recibidos para determinar si la estación es un destino. En este caso, el paquete se pasa a una capa de protocolo superior para su procesamiento adecuado.

Las diferencias entre LANs Ethernet y IEEE 802.3 son sutiles, Ethernet proporciona servicios correspondientes a las capas 1 y 2 del modelo de referencia OSI, mientras que IEEE 802.3 especifica la capa física (Capa 1) y la parte de acceso-canal de la capa de enlace (Capa 2), pero no define un protocolo de control de enlace lógico. Así como el resto de funciones de las capas 1 y 2, tanto Ethernet como CSMA/CD están implementadas en hardware, en general a través de una tarjeta de interfaz en un ordenador o a través de una placa principal en el propio ordenador.

Características	Ethernet	IEEE 802.3					
		10Base2	10Base5	1Base5	10BaseT	100BaseTx	100BaseT4
Velocidad (Mbps)	10	10	10	1	10	100	
Señalización	Banda Base	Banda Base	Banda Base	Banda Base	Banda Base	Banda Base	Banda Ancha
Tramos (m)	500	185	500	250	100	100	1800
Soporte físico	Coaxial grueso 50Ω	Coaxial fino 50Ω	Coaxial grueso 50Ω	Par trenzado sin blindar	Par trenzado sin blindar	Par trenzado con blindaje	Coaxial 75Ω
Topología	Bus	Bus	Bus	Estrella	Estrella	Estrella	Bus

Tabla II.25 *Características de IEEE 802.3*

Ethernet es muy similar a IEEE 802.3 10BaseT. Ambos protocolos especifican una red de topología de bus con un cable de conexión entre las estaciones finales y el soporte de red actual, en el caso Ethernet, es cable se denomina cable transceptor.

El cable transceptor conecta a un dispositivo transceptor conectado al soporte físico de la red, la configuración IEEE 802.3 es prácticamente la misma, a excepción de que el cable de conexión se denomina unidad de conexión de soporte (MAU). En ambos casos, el cable de conexión se conecta a la placa del interface (o a un circuito de interface) dentro de la estación final. La codificación que emplea Ethernet es de tipo Manchester Diferencial.

PROTOCOLO.

CSMA/CD Ethernet, está organizada en torno a la idea de protocolos estratificados por niveles, interviniendo el nivel de enlace-subnivel de acceso al medio y el nivel físico, el nivel de usuario es atendido por el de enlace y el físico.

NIVEL DE ENLACE.

El nivel de enlace es el encargado de proporcionar la lógica que gobierna la red CSMA/CD. Es independiente del medio, lo que quiere decir que no le afecta que la red sea de banda ancha o estrecha.

En este nivel se encuentra una entidad que se ocupa de encapsular-desencapsular los datos, y otra encargada de gestionar el acceso al medio, tanto para transmitir como para recibir.

La tarea de Encapsulado y desencapsulado consiste en establecer la trama CSMA/CD (trama MAC), proporcionando las direcciones fuente y destino. Además, calcula en el nodo emisor un campo para detección de errores, campo que también emplea en el nodo receptor para indicar la aparición de algún error. La tarea que recae sobre el control de acceso al medio (MAC) es:

- Transmitir y extraer la trama al nivel físico.
- Almacenar la trama en un buffer.
- Procurar evitar colisiones y gestionar las mismas, en el lado del emisor.

FUNCIONAMIENTO.

Cada estación, posee una parte emisora y otra receptora. Lógicamente, se usa la parte emisora cuando se desea enviar datos a otro ETD, Equipo Terminal de Datos, y la receptora cuando el cable transporta señales dirigidas a las estaciones de la red.

La entidad encargada del encapsulado, recibe los datos del usuario y construye una trama MAC, a la que añade un campo de comprobación de secuencia. Tras esto la envía a la entidad de gestión de acceso al medio, que la almacena en un buffer hasta que quede libre el canal.

En el nivel físico del nodo emisor, la entidad de codificación transmite el preámbulo, codifica los datos, usando un código Manchester con autosincronización, y se entrega la señal a la entidad de acceso al medio que se encarga de introducirla en el canal.

La trama CSMA/CD llega a todas las estaciones conectadas, ya que la señal se propaga desde el nodo origen hacia los demás nodos. Cuando una estación receptora detecta el preámbulo, se sincroniza con él y activa la señal que indica la detección de una portadora. Posteriormente la entidad de acceso al medio en recepción entrega la señal al descodificador de datos, que convierte de formato Manchester a binario, y entrega la trama al gestor de acceso al medio. El gestor de acceso al medio en recepción guarda esa trama en un buffer, hasta que la entidad de acceso al canal en recepción indique que se ha desactivado la señal de detección de portadora, lo cual indicará que han llegado todos los bits. A continuación, la entidad de gestión del acceso al medio puede entregar los datos a un nivel superior para su desencapsulado, durante el cual tiene lugar una comprobación de errores sobre los datos. Si no se ha producido ningún error de transmisión, se comprueba el campo de dirección para comprobar si esa trama iba dirigida a ese nodo.

Si realmente iba destinada par él, se entrega al nivel de usuario, agregando además la dirección de destino, la fuente y la unidad de datos LLC.

COLISIONES.

Como CSMA/CD posee una estructura de red de igual a igual, en el que todas las estaciones compiten por el uso del canal cuando tienen datos que transmitir, puede suceder que las señales de varias estaciones sean introducidas simultáneamente en el cable, lo que producirá una colisión y una distorsión mutua que hará que las estaciones no puedan recibirlas adecuadamente.

Las estaciones en una LAN CSMA/CD pueden acceder a la red en cualquier momento y, antes de enviar los datos, las estaciones CSMA/CD "escuchan" la red para ver si ya es operativa. Si lo está, la estación que desea transmitir espera. Si la red no está en uso, la estación transmite. Se produce una colisión cuando dos estaciones que escuchan el tráfico en la red no "oyen" nada y transmiten simultáneamente. En este caso, ambas transmisiones quedan desbaratadas y las estaciones deben transmitir de nuevo en otro momento. Los algoritmos Backoff determinan cuando deben retransmitir las estaciones que han colisionado. Las estaciones CSMA/CD pueden detectar colisiones y determinar cuando retransmitir.

La cantidad de tiempo que necesita una señal para propagarse por el canal hasta ser detectada por todas y cada una de las estaciones de la red, es la ventana de colisión.

Las colisiones evidentemente no son deseables, ya que producen errores en la red. La duración de la colisión es proporcional al tamaño de la trama transmitida. CSMA/CD afronta este problema en el nivel de gestión de acceso al medio en transmisión, interrumpiendo la transmisión de la trama justo al detectar la colisión.

Otra forma de ver las colisiones consiste en considerar ranuras de tiempo de duración igual al periodo que necesita una trama para recorrer todo el canal, sumado al retardo de captura del canal.

II.2.1.2 ROUND ROBIN

TOKEN PASSING

Este sistema evita la colisión pues limita el derecho a transmitir a una máquina. Esa máquina se dice que tiene el token (cospel). El token va pasando a intervalos fijos de una máquina a otra. La circulación del token de una máquina a la siguiente hace que, desde el punto de vista lógico, toda red basada en tokens sea un anillo. Debe notarse que un anillo lógico no implica un anillo físico. En efecto, si bien

IEEE 802.5 emplea un anillo físico, IEEE 802.4 especifica un bus y ARCnet usa una estrella.

Por la red circulan dos tipos de mensajes: los "tokens" y los "frames".

Un token indica que la red está disponible. El token incluye información de prioridad, de forma tal que el control de la red lo pueda tomar sólo una estación con igual o mayor prioridad. Hay un timer que asegura que ninguna estación retenga el token demasiado tiempo.

Un frame (marco) es un mensaje que contiene (entre otras cosas) la información que se quiere transmitir, las direcciones de las estaciones transmisora y receptora, y un CRC para manejo de errores.

COMPARACIÓN ENTRE CSMA/CD Y TOKEN PASSING

Ambos tipos de protocolo tienen uso generalizado. La ventaja del primero es que permite mayor performance, especialmente cuando hay pocas colisiones. Esto ocurre si la mayoría de las transmisiones se originan en la misma máquina o si hay relativamente poco tráfico en la red. Una ventaja del segundo es que puede asegurarse que, independientemente del tráfico en la red, una máquina va a poder transmitir antes de un tiempo predeterminado.

Esto tiene dos efectos positivos: uno es que la performance de la red no disminuye tanto al aumentar el tráfico; el otro (aunque su uso es menor) es en sistemas de control donde es importante asegurarse de que un mensaje llegue a destino antes de que pase cierto tiempo. Otra ventaja posible para el segundo es que soporta un esquema de prioridades para el uso de la red.

Por estas razones, el CSMA/CD es el preferido para oficinas, mientras que el Token passing es preferido para fábricas.

Para permitir la fácil interconexión de un gran número de máquinas, se simplifica al máximo el transmisor, receptor y cableado transmitiendo en forma serie. La norma RS 232 no sirve en este caso, pues contempla esencialmente la comunicación entre 2 equipos, y se complicaría notablemente si se tratara de extrapolar a esta situación. Por lo pronto, mediante un arbitraje adecuado, con sólo dos conductores (ya sea un par trenzado o algún coaxil) es posible comunicar decenas de máquinas.

Como ganar el permiso para transmitir demanda un cierto tiempo, no es eficiente transmitir sólo un byte; las redes arman grupos de bytes denominados

paquetes. Un paquete lleva los datos precedidos por bytes de sincronización, direcciones tanto del transmisor como del receptor e indicación del formato del paquete (por ej: cantidad de bytes) y termina con bytes para efectuar un CRC (por ej: en Ethernet son 4).

Para evitar problemas de interferencia y de circulación de corriente continua entre máquinas, generalmente los cables están aislados del resto de la computadora por medio de transformadores de pulsos.

El tipo de conductor viene dado por la elección de la placa de red. Debido al mayor ancho de banda obtenible, las redes que trabajan a mayor velocidad, usan coaxil, y las de menor velocidad, par trenzado. Las redes donde se emplea par trenzado en topología estrella (como StarLAN, IEEE 802.3 1 BASE 5), suelen ofrecer la ventaja de poder aprovechar pares sobrantes del tendido de la instalación telefónica.

Si bien lo más habitual es transmitir mediante conductores, hay otras alternativas. Cuando se requieren conexiones a distancias del orden del Km, inmunidad a interferencias, seguridad frente a conexiones clandestinas y total aislación entre equipos, se usan redes basadas en fibra óptica. Otra aplicación posible de la fibra óptica es en enlaces de gran ancho de banda, donde se aprovecha la instalación para transmitir audio y/o video.

II.2.1.3 DEMAND PRIORITY

El acceso de la prioridad de la demanda es un protocolo desarrollado para IEEE 802.12[3].It tiene todas las mejores características de ETHERNET tales como acceso simple, rápido y el del token ring tal como evitación de la colisión, control y calculado retrasa. El nivel del The de la prioridad alternadamente es determinado por su localización secuencial en red. El IEEE 802,12 lleva IEEE 802,3, el repetidor de Ethernet y de IEEE 802,5 Frames.Every tiene un mínimo de dos puertos locales y puede tener un puerto opcional de la cascada a conectar con un nivel más alto. Una red puede tener cinco niveles de repetidores.

802,12 fueron diseñados que mantenían la visión las necesidades de los establecimientos industriales del anuncio y de la luz.

El concepto implicado en un funcionamiento del protocolo puede ser entendido dividiéndolo en las varias funciones correlacionadas, las operaciones en el trun de las cuales se pueden describir por las máquinas del estado. La idea que es que cada máquina representa los límites de las funciones que consisten en mutuamente estados de la exclusiva y también con el condtion en que solamente un estado de una

función puede ser activo cualquier hora dada y varias funciones puede ser activa concurrentemente.

Pseudo Código: Los pseudo códigos se utilizan en definir las máquinas del estado que el pseudo código en 802,12 se escribe en construcciones de PASCAL y la ejecución de los bitss se considera instantánea.

REPRESENTACIÓN NUMÉRICA:

Todos los valores numéricos se pueden representar en la notación binaria, decimal o hexadecimal. Diagramas del espacio del tiempo:

La demostración del diagrama del espacio del tiempo las secuencias de las operaciones.

ARQUITECTURA DE LA PRIORIDAD DE DEMANDA

La arquitectura del LAN de la prioridad de la demanda utiliza tres componentes:

Nodos de 1 final: Son componentes, sitios de trabajo o servidor de archivo o analizadores o puentes personales o grandes del LAN.

2 repetidores: Controlan redes y son para withports configurados mayores que o igualan a dos en el número los nodos del extremo que conectan u otros repetidores.

3 acoplamientos: proporcionan medio de la interconexión entre un repetidor y terminan nodos.

El método de acceso de la prioridad de la demanda proporciona la ayuda para el formato del marco de ISO/IEC 8802-3 y los capítulos del mac. IEC 8802-5 se utilizan en intercambio de datos entre los nodos del final y durante marco de la inicialización ISO/IEC 8802,12 del acoplamiento el formato se utiliza en la construcción del paquete también que un marco vacío se define para una situación cuando el marco entrante no puede ser detectado.

CAMPOS DE DIRECCIÓN

Cada marco tiene dos campos de dirección: Dirección de la fuente de la dirección de destinación.

Los formatos de los campos de dirección se demuestran abajo:

Addres de Unicast : Una dirección única que reconoce cada nodo del final.

Dirección nula : Ésta es una dirección individual que contiene todo en ceros. Esto implica que el marco no está tratado a ningún nodo.

Dirección del grupo: Es una dirección asociada a 0 o más nodos del final en una red. Se asocian a un grupo de nodos lógicamente relacionados del final.

Dirección de la difusión : Es una dirección del grupo que indica el sistema de nodos del final en una red. Todos los 1s en la dirección de destinación se predefinen como dirección de la difusión.

Dirección del multicast : Es una dirección del grupo asociada a muchos nodos conectados lógicos del final.

El campo de dirección de la fuente: Esta identifica el nodo del final de el cual el marco origina. Esto contiene el siguiente:

Campo de la longitud : Contiene el campo 2-octetos, los pedacitos de el cual indican el número de los octetos de los datos del LLC en la zona de informaciones.

Zona de informaciones : Este campo contiene a 46-1500 octetos en el final de los datos del LLC

Bajo el punto de vista de la IEEE, la capa de enlace está dividida en dos partes; en la parte de abajo se encuentra la subcapa MAC Control de Acceso al Medio (*Media Access Control*) responsable de las técnicas de acceso al medio de transmisión y el direccionamiento físico de dispositivos; mientras que en la parte superior se ubica el estándar IEEE 802.2 o LLC Control de Enlace Lógico (*Logical Link Control*), que define las funciones lógicas de la capa de enlace, así como la disponibilidad de SAP's[1] para la adecuada transmisión o recepción de información a protocolos que operan en capas superiores del modelo de referencia OSI.

[1] SAP: Punto de Acceso al Servicio (*Service Access Point)*

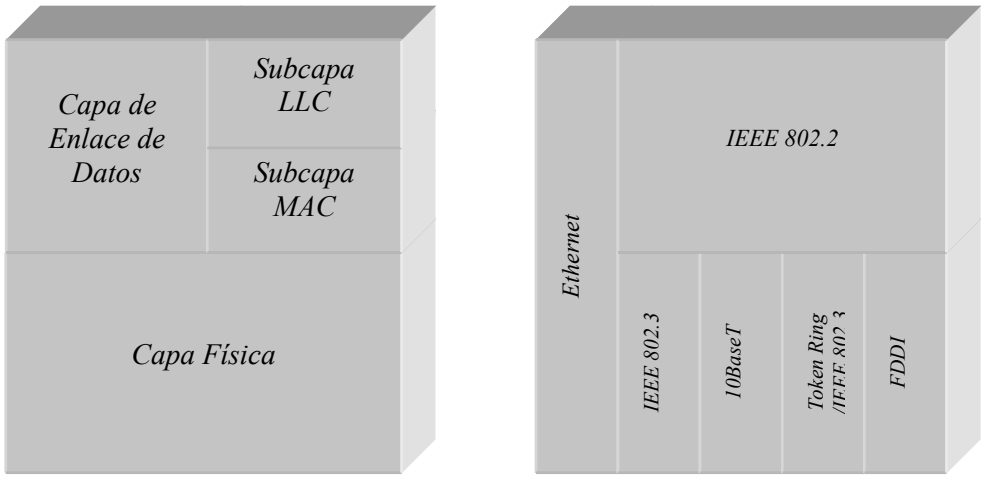


Figura II.51 *Subcapa MAC y estandar IEEE 802.3*

II.2.1.4 FORMATO DE LAS TRAMAS MAC

Es la subcapa de la capa de enlace de datos responsable de armar los frames. Este construye los frames de los 1s y 0s que la capa física recoge del cable.

Para la parte MAC existen diferentes técnicas de acceso al medio:

- Contención: Cuando un dispositivo necesita transmitir información, verifica primero que el medio esté libre, si es así, transmite inmediatamente, si no, esperará un tiempo finito hasta que el medio de transmisión este libre y así poder realizar su transmisión. En este tipo de estrategia no existe control sobre que dispositivo será el siguiente en ocupar el medio de transmisión. Tecnologías típicas que utilizan este esquema son Ethernet y derivadas.

- Round-robin: En éste todos los dispositivos que comparten un mismo medio de transmisión y tienen asignada una secuencia en tiempos o turnos para la transmisión de su información de forma rotatoria. Si el dispositivo en turno no tiene nada que transmitir, cede su lugar al siguiente dispositivo en la cola de transmisión. Tecnologías típicas que usan este esquema son Token-Ring, FDDI y 100VGanyLAN.

- Reservación: Se trata del uso de la técnica anterior, pero con la posibilidad de que un dispositivo reserve el siguiente turno de transmisión para si mismo. Tecnologías típicas que usan este esquema son Token-Ring, FDDI y 100VGany LAN.

El direccionamiento MAC más común para dispositivos de red, requiere seis bytes de acuerdo al siguiente esquema:

3 Bytes	3 Bytes
Código del fabricante	*Número de serie de la interfaz*

Tabla II.26 *Bytes del direccionamiento MAC*

Generalmente las direcciones MAC se representan con números hexadecimales, como por ejemplo 00.B1.00.23.A0.

Las tramas MAC contienen los siguientes componentes básicos:

- Una cabecera MAC, que comprende campos de control, duración, direccionamiento y control de secuencia
- Un cuerpo de trama de longitud variable, que contiene información específica del tipo de trama
- Un secuencia *checksum* (FCS) que contiene un código de redundancia CRC de 32 bits

Las tramas MAC se pueden clasificar según tres tipos:

- Tramas de datos.
- Tramas de control. Los ejemplos de tramas de este tipo son los reconocimientos o ACKs, las tramas para multiacceso RTS y CTS, y las tramas libres de contienda
- Tramas de gestión. Como ejemplo podemos citar los diferentes servicios de distribución, como el servicio de Asociación, las tramas de Beacon o portadora y las tramas TIM o de tráfico pendiente en el punto de acceso.

El formato de la trama MAC genérica tiene el siguiente aspecto:

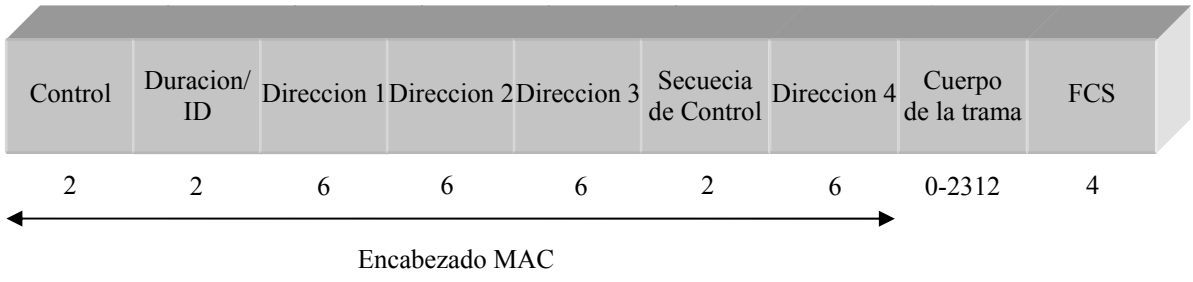


Figura II.52 *Formato de una trama MAC*

Los campos que componen esta trama son:

- Campo de control. Contiene toda la información de la trama MAC.
- Duration/ID. En tramas del tipo PS o Power-Save para dispositivos con limitaciones de potencia, contiene el identificador o AID de estación. En el resto, se utiliza para indicar la duración del periodo que se ha reservado una estación.
- Campos address1-4. Contiene direcciones de 48 bits donde se incluirán las direcciones de la estación que transmite, la que recibe, el punto de acceso origen y el punto de acceso destino.
- Campo de control de secuencia. Contiene tanto el número de secuencia como el número de fragmento en la trama que se está enviando.
- Cuerpo de la trama. Varía según el tipo de trama que se quiere enviar.
- FCS. Contiene el checksum.

Los campos de control de trama tienen el formato siguiente:

Versión del Protocolo	Tipo	Subtipo	Para DS	De DS	Mas Fragmentos	Reintento	Control de Potencia	Datos Pendientes	WEP	Orden
2	2	4	1	1	1	1	1	1	1	1
					bits					

Figura II.53 *Campo de Control de la trama MAC*

- Versión.
- Type/Subtype. Mientras tipo identifica si la trama es del tipo de datos, control o gestión, el campo subtipo nos identifica cada uno de los tipos de tramas de cada uno de estos tipos.
- ToDS/FromDS. Identifica si la trama si envía o se recibe al/del sistema de distribución. En redes ad-hoc, tanto ToDS como FromDS están a cero. El caso más complejo contempla el envío entre dos estaciones a través del sistema de distribución. Para ello situamos a uno tanto ToDS como FromDS.
- Más fragmentos. Se activa si se usa fragmentación.
- Retry. Se activa si la trama es una retransmisión.
- Power Management. Se activa si la estación utiliza el modo de economía de potencia.
- More Data. Se activa si la estación tiene tramas pendientes en un punto de acceso.
- WEP. Se activa si se usa el mecanismo de autenticación y encriptado.

- Order. Se utiliza con el servicio de ordenamiento estricto, en el cual no nos detendremos.

La subcapa de MAC también se encarga de implementar las siguientes funciones extras las cuales solo mencionaremos algunas de ellas:

- Sincronización.
- Gestión de potencia
- Asociación-Reasociación
- Utiliza el MIB o Management Information Base

II.2.1.5 WEP

Las redes inalámbricas WLAN carecen constantemente de la mínima privacia que provee una red LAN alambrica.

Para solucionar esto se ha desarrollado un mecanismo de seguridad adicional mediante el uso del algoritmo WEP (Wired Equivalent Privacy). WEP proporciona servicios de autenticación y codificación. El algoritmo WEP define el uso de una clave secreta de 40 bits para la autenticación y la codificación. Este algoritmo proporciona la mayor parte de la protección contra los posibles intrusos que podrían escuchar dentro de la red, así como de atributos de seguridad física que son comparables a una red alámbrica.

Las tramas de datos que son encriptados son enviados con el bit encendido de WEP en el campo de control de la trama del encabezado de MAC. El receptor desencripta la trama y pasa este a los protocolos de capas superiores.

El algoritmo de encripción usado en el RC4 desarrollado por Ron Rivest de RSA Data Security, INc. El RC4 es un flujo codificado simétrico que soporta una longitud variable de la clave (Para la IEEE se elige una longitud de 40 bits). Este es simétrico puesto que utiliza la misma clave, y el algoritmo es usado tanto para la encriptacion como para la desencriptacion. A diferencia de un bloque codificado que procesa un número fijo de bytes, un flujo codificado es un algoritmo que puede procesar un número variable de bytes.

Las claves pueden ser dadas para una sola estación y con estas hacer la labor de autentificación y codificación o bien estas pueden ser generadas por una estación particular para ser asignadas a cada una de las estaciones y estas puedan ser usadas por una sola estacion en particular.

Una limitación importante de este mecanismo de seguridad es que no se define un protocolo de administración de claves para la distribución de las mismas. Esto supone que las claves secretas compartidas se entregan a la estación inalámbrica a través de un canal seguro independiente. El reto aumenta cuando están implicadas un gran número de estaciones, como es el caso de un campus corporativo.

II.2.1.6 LLC, 802.2

Subcapa de la capa de enlace de datos provee flexibilidad para la capa de red y la subcapa MAC. Esta subcapa opera entre la capa de red y la subcapa MAC.

LLC provee los siguientes servicios a la capa de red:

- Modo sin conexión y sin reconocimiento (*Unacknowledged connectionless-mode*) definido como el Tipo 1 de operación. En éste los frames son enviados con la expectativa de que lleguen correctamente a su destino; es decir no existe ningún mecanismo de detección de errores y/o retransmisión de información.

- Modo orientado a conexión (*Connection-mode*) definido como el Tipo 2 de operación. En éste se establecen, usan, reinicializan y terminan conexiones a nivel enlace entre estaciones terminales, con objeto de poder efectuar la retransimisión de frames en caso de pérdida o transmisión errónea, así como el control de flujo entre estaciones.

  El formato del frame LLC se forma como se muestra a continuación:

1 Byte	1 Byte	1 ó 2 Bytes	N Bytes
DSAP	*SSAP*	*Control*	*Información*

Donde:
DSAP. SAP Destino
SSAP: SAP Origen
N: Entero mayor o igual a cero

II.2.1.7 HDLC

IBM desarrolló el protocolo SDLC Control de Enlace de Datos Síncrono (*Synchronous Data Link Control*), a mediados de los años 70. SDLC fue el primero de un importante conjunto de protocolos de capa de enlace basados en una operación síncrona y orientada a bit.

Después del desarrollo de SDLC, IBM sometió el protocolo a varios comités de estandarización. La ISO modificó el protocolo para crear HDLC Control de Enlace de Datos de Alto-Nivel (*High-Level Data Link Control*); la ITU-T subsecuentemente modifico HDLC para crear LAP Procedimiento de Acceso al Enlace (*Link Access Procedure*) y entonces LAPB Procedimiento de Acceso al Enlace, Balanceado (*Link Access Procedure, Balanced*). Posteriormente IEEE modificó HDLC para crear el estándar 802.2.

HDLC proporciona varias opciones para su implementación como son transmisiones del tipo semi-duplex o duplex, configuraciones punto a punto y multipunto, también tanto canales conmutados y no conmutados.

Para HDLC existen tres tipos de estaciones:

Estación Primaria: Tiene el control de enlace, cuya función es transmitir tramas con ordenes a las estaciones secundarias en el canal. A su vez recibe tramas de respuesta de esas estaciones. Si el enlace es multipunto, la estación primaria es responsable de mantener sesiones separadas con cada estación en el enlace.

Estación Secundaría: Actúa como esclava de la estación primaria. Envían respuestas a las órdenes de la estación primaria. Mantiene solo una sesión con la estación primaria, por lo que no tiene la responsabilidad del control del enlace.

Estaciones Combinadas: Estas estaciones transmiten órdenes y respuestas así como reciben órdenes y respuestas de otra estación combinada. Mantiene sesiones con otras estaciones de su tipo.

HDLC cuenta con tres modos de transferencia:

- ***NRM Modo de Respuesta Normal*** (*Normal Response Mode*): Este modo de transferencia las estaciones secundarias no pueden transmitir hasta que la estación primaria les ha dado permiso de hacerlo.
- ***ARM Modo de Respuesta Asíncrona*** (*Asynchronous Response Mode*): En este modo las estaciones secundarias pueden iniciar una transmisión con o sin el permiso de la estación primaria.

- ***ABM Modo de Balanceo Asíncrono*** (*Asynchronous Balanced Mode*): En este modo todas las estaciones pueden actuar como estaciones primarias o estaciones secundarias, dependiendo de la situación, aquí cualquier nodo puede iniciar la transmisión de información sin necesidad de permisos de cualquier otra estación.

FORMATOS DE LA TRAMA DE HDLC

Existen tres tipos de trama HDLC:

1. Formato de información: Se utiliza para transmitir datos de usuario final entre dispositivos.
2. Formato de supervisión.: Realiza funciones de control tales como el acuse de recibo de tramas, la solicitud de suspensión temporal de transmisión de las mismas.
3. Trama con formato no numerado: También se usa con fines de control, y es utilizada para llevar a cabo la inicialización o desconexión del enlace y otras funciones de control del mismo.

En la figura II.96 se muestran los campos que conforman la trama HDLC.

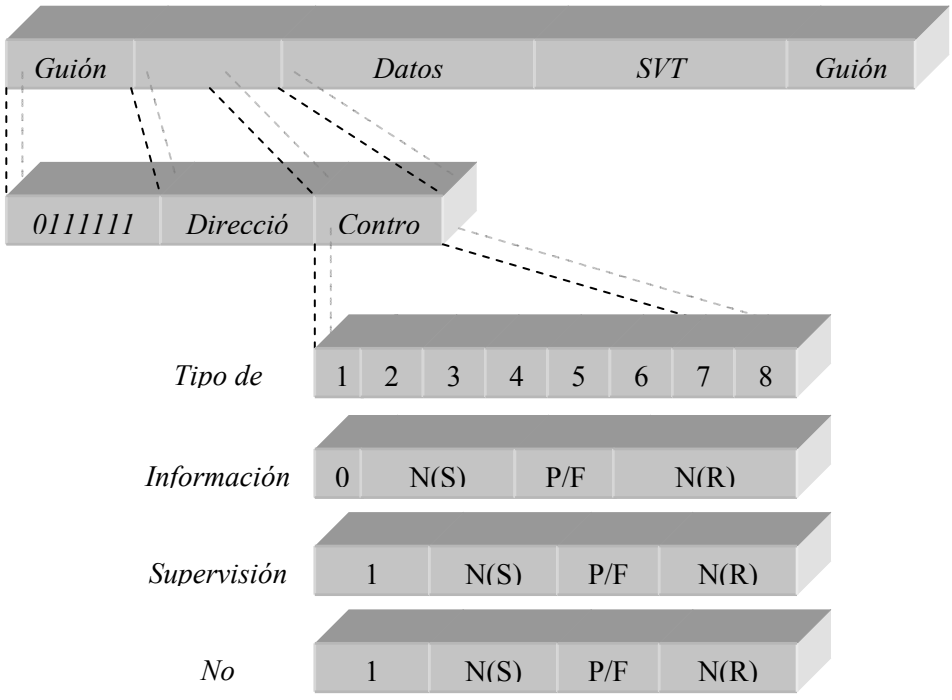


Figura II.54 *Trama HDLC*

II.2.1.8 PPP

El protocolo PPP Protocolo Punto a Punto (*Point-to-Point Protocol*), surgió originalmente como un protocolo de encapsulación para transportar trafico IP sobre enlaces punto a punto. PPP también estableció un estándar para la asignación y administración de direcciones IP, encapsulación asíncrona (arranque/parada) y síncrona orientada a bit, protocolo de multiplexaje de red, configuración de enlace,

prueba de calidad del enlace, detección de errores y opción de negociación, tal como capacidad de negociación con la dirección de capa de red y negociación de compresión de datos. PPP soporta todas esas funciones para proveer un extensible LCP Protocolo de Control de Enlace (*Link Control Protocol*) y una familia de NCPs Protocolos de Control de Red (*Network Control Protocols*) para negociar parámetros de configuración opcional y servicios. Adicionalmente para IP, PPP soporta otros protocolos incluidos los de Novell, tales como IPX[1] y DECnet[2].

PPP provee un método para transmitir datagramas sobre enlaces punto a punto. PPP tiene tres componentes principales:

1. Un método para encapsulado de datagramas sobre enlace seriales, PPP utiliza el protocolo HDLC como base para la encapsulación de datagramas sobre enlaces punto a punto.
2. Un extensible LCP para establecimiento, configuración y pruebas de conexión de enlace de datos.
3. Una familia de NCPs para establecimiento y configuración de diferentes protocolos de la capa de red. PPP esta diseñado para permitir el uso simultaneo de múltiples protocolo de la capa de red.

OPERACIÓN GENERAL

Para establecer comunicaciones sobre un enlace punto a punto, el protocolo PPP originado envía primero tramas LCP para configurar y (opcionalmente) probar el enlace de datos. Después el enlace se establece y servicios opcionales como las necesitadas por LCP tienen que ser negociadas, el protocolo PPP originado envía tramas NCP para elegir y configurar uno o más protocolos de la capa de red. Cuando se eligen los protocolos de la capa de red, tienen que ser configurados, empaquetados y enviados sobre el enlace, desde cada protocolo de la capa de red. El enlace deberá permanecer configurado para la comunicación hasta que las tramas LCP o NCP explícitamente cierren el enlace, o hasta que algún evento externo ocurra (por ejemplo, un reloj inactivo expire o un usuario intervenga).

REQUERIMIENTOS DE LA CAPA FÍSICA

PPP es capaz de operar a través de cualquier interfaz DTE/DCE. Incluidas por ejemplo las vistas en el capitulo II “Capa Física”, tales como EIA/TIA-232-C (conocida formalmente como RS-232-C), EIA/TIA-422 (formalmente RS-422), EIA/TIA-423 (formalmente RS-423), y la Unión Internacional de

[1] IPX: Intercambio de Paquetes entre Redes (*Internetwork Packet Exchange*)
[2] DECnet: Corporación de Equipos Digitales (*Digital Equipment Corporation*)

Telecomunicaciones Sector de Estandarización de Telecomunicaciones (ITU-T) (formalmente conocida CCITT) V.35. El único requerimiento absoluto impuesto por PPP es la disposición de un circuito duplex, cualquier dedicado o conmutado, que pueda operar en cualquier modo asíncrono o síncrono, para PPP es transparente para las tramas de la capa de enlace. PPP no impone ninguna restricción respecto a la tasa de transmisión, ya que esta impuesta por la interfaz DTE/DCE en particular en uso.

CAPA DE ENLACE PPP

PPP utiliza las principales terminologías y estructuras de tramas de la Organización Internacional para Estandarización (ISO) HDLC. El formato de la trama PPP se muestra en la figura II.97.

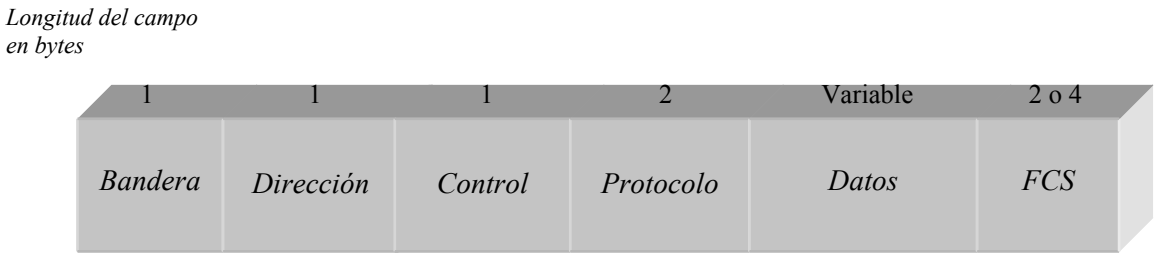


Figura II.55 *Trama PPP*

La siguiente descripción sumariza los campos de la trama PPP ilustrada en la figura anterior:

- *Bandera*: Un solo byte que indica el comienzo o final de la trama, consiste de una secuencia binaria 011111110.

- *Dirección*: Un solo byte que contiene la secuencia binaria 11111111, la dirección estándar de broadcast.

- *Control*: Un simple byte que contiene la secuencia 00000001, la cual llama para la transmisión de los datos de usuario en una secuencia de tramas.

- *Protocolo*: Dos bytes que identifican el protocolo de encapsulado en la información de la trama.

- *Datos*: Cero o más bytes que contienen el datagrama para el protocolo especificado en el campo de protocolo, la longitud máxima por default del campo de información es de 1500 bytes.
- *FCS:* Secuencia de Verificación de Trama (*Frame Check Sequence*), normalmente de 16 bits (2 bytes), por acuerdo, consentido para la implementación de PPP, puede utilizar 32 bits (4 bytes), para mejorar la detección de errores.

II.2.1.9 PAP Y CHAP

Con el PPP, cada sistema puede obligar al otro ordenador a identificarse usando alguno protocolo de autentificación disponible. Unos de los mas utilizados son el PAP (Por sus siglas en ingles *Password Authentication Protocol*), y el CHAP (por sus siglas en *ingles Challenge Handshake Authentication Protocol*).

Su funcionamiento es el siguiente. Cuando se establece una conexión, cada extremo puede pedir al otro que se autentifique, independientemente de que sea el cliente (autentificado) o el servidor (autentificador). Un demonio PPP puede pedir a la otra máquina autentificación enviando otra petición más de configuración de LCP indicando el protocolo de autentificación deseado.

El PAP trabaja básicamente de la misma forma que el procedimiento normal de autentificación del *login*. El cliente se autentifica a sí mismo enviando un nombre de usuario y una contraseña (opcionalmente encriptada) al servidor, la cual es comparada por el servidor con su base de datos de claves. Esta técnica es vulnerable a los intrusos que pueden intentar obtener la contraseña escuchando en una línea de serie y a otros que hagan sucesivos intentos de ataque por el método de prueba y error.

El CHAP no tiene estos defectos. Con el CHAP, el autentificador (el servidor) envía una cadena de **reto** al cliente la cual es generada aleatoriamente, junto a su nombre de ordenador. El cliente utiliza el nombre del ordenador para buscar la clave apropiada, la combina con el reto, y encripta la cadena utilizando una función de codificación de un solo sentido. El resultado es devuelto al servidor junto con el nombre del ordenador cliente. El servidor realiza ahora la misma computación, y advierte al cliente si llega al mismo resultado.

Otra característica del CHAP es que no solicita autentificación al cliente solamente al comienzo de la sesión, sino que envía retos a intervalos regulares para asegurarse de que el cliente no ha sido reemplazado por un intruso, por ejemplo cambiando la línea telefónica.

II.2.1.10 QoS CALIDAD DE SERVICIO (QUALITY OF SERVICE)

Se entiende por calidad de servicio la posibilidad de asegurar una tasa de datos en la red, sus características son: ancho de banda, retardo y confiabilidad. El desempeño de las características de QoS incluye:

- **Ancho de Banda**: PDR Tasa de Datos Pico (*Peak data Rate*), SDR Tasa de Datos Sustentada (*Sustained Data Rate*), MDR Tasa de Datos Mínima (*Minimum Data Rate*).
- **Retardo:** Punto a Punto o Retardo de Ida y Vuelta, Variación del Retardo (Jitter).
- **Confiabilidad:** Disponibilidad (con % de tiempo arriba), (MTBF/MTRH) Promedio Entre Tiempo de Falla / Promedio de Tiempo de Reparación (*Mean Time Between Failures/ Mean Time To Repair*), Errores y Paquetes perdidos.

Dichos valores estan acotados a los valores contratados con el cliente. En las redes Frame Relay o ATM la calidad de servicio se garantiza mediante un contrato de CIR Velocidad de Información Suscrita (*Commited Information Rate*) con el usuario.

Para disponer de una calidad de servicio aceptable en redes soportadas en protocolo IP se han diseñado herramientas como son los RTP Protocolos de Transporte en Tiempo-Real (*Real-Time Transport Protocol*) y de reservación RSVP Protocolo de Reservación de Recursos (*Resource Reservation Protocol*). Por otro lado, un problema evidente es que cuando se soporta un servicio de voz sobre IP (VoIP) por ejemplo, los paquetes son cortos y el encabezado es largo comparativamente. En este caso se requiere un encabezado reducido y un proceso de fragmentación e intercalado como LFI Indicador de Ultimo Archivo (*Last File Indicator*). Mediante QoS se tiende a preservar los datos.

Los servicios tradicionales de Internet (SMTP o FTP) disponen de una calidad denominada "*best effort*"; es decir que la red ofrece el mejor esfuerzo posible para satisfacer los retardos mínimos; lo cual no es mucho pero es suficiente para servicios que no requieren ser transmitidos en tiempo-real como el web. Para servicios que requieren ser transmitidos en tiempo-real como voz y vídeo, se requiere una latencia mínima.

VARIANTES DE SERVICIOS

Los servicios de datos y multimedia tienen distintos requerimientos de calidad referido a latencia y Jitter. Para satisfacer los requerimientos de calidad se acude al manejo de las colas de paquetes, la reservación de ancho de banda y la gestión del

tráfico. Para obtener estos objetivos en diversos ámbitos se han definido variantes de servicios.

En las siguientes tablas II.43 y II.44 se encuentran las variantes de servicios: Clase de Servicio en Redes LAN, Tipo de Servicio sobre protocolo IP y Calidad de Servicio sobre redes IP. Por otro lado se han definido las características de la calidad de servicio que se entregan, en la misma Tabla: servicio garantizado (mediante reservación de ancho de banda), diferenciado (mediante prioridad de tráfico) y por el "mejor esfuerzo".

Variantes en capa 2, 3 y 4	
CoS	CoS Clase de Servicio (*Class of Service*) se logra mediante 3 bits que se ingresan en un campo adicional de 4 Bytes (etiqueta denominada Tag o Label) dentro del protocolo MAC. Estos 3 bits permiten definir prioridades desde 0 (máxima) a 7 (mínima).
IEEE 802.1p	Este estándar tiene un esquema de prioridades. Los paquetes con bajo nivel de prioridad no son enviados, si los paquetes en cola tiene un nivel de prioridad mayor. Este protocolo otorga un control en la red por prioridades para todos los paquetes y así prevenir congestionamientos en la red.
IEEE 802.1Q	Servicio de VLAN para realizar enlaces troncales punto-a-punto en una red de switch.
IEEE 802.3x	Este estándar examina el control de flujo en enlaces Ethernet del tipo full-dúplex. Se aplica en enlaces punto-a-punto (Fast y Gigabit Ethernet). Si existe congestión se emite hacia atrás un paquete llamado "pause frame" (pausa de trama) que detiene la emisión por un período de tiempo determinado. Una trama denominada "time-to-wait zero" (tiempo de espera nulo) permite reiniciar la emisión de paquetes.
IEEE 802.1D	Define el protocolo STP Protocolo Puenteo de Arbol (*Spanning-Tree Protocol*). Se diseñó para permitir que en una red de bridge y switch de muchos componentes se formen enlaces cerrados para protección de caminos. Se intercambia información de la topología de la red que permiten construir el árbol. De esta forma se crean puertas redundantes en el cableado, el protocolo STP deshabilita automáticamente una de ellas y la habilita en caso de falla de la otra.
ToS	ToS Tipo de Servicio (*Type of Service*). Es similar a CoS en capa 3. Sobre el protocolo IP se define el ToS con 3 bits (del segundo byte del encabezado IP) para asignar prioridades. Se denomina señal de procedencia.
QoS	QoS Calidad de Servicio (*Quality of Service*). En redes IP se define la tasa de acceso contratada CAR Tasa de Acceso Comprometida (*Committed Access Rate*) en forma similar al CIR Velocidad de Información Suscrita (*Committed Information Rate*) de Frame Relay y ATM. La calidad de servicio se ve garantizada mediante protocolos de reservación RSVP y de tiempo real RTP.

Tabla II.27 *Variantes de Calidad de Servicio*

Clasificacion de la QoS	
Garantizada	El servicio garantizado es utilizado para requerir un retardo máximo extremo-a-extremo. Se trata de un servicio análogo al CBR Velocidad de Bits Constante (*Constant Bit Rate*) en ATM. Se puede aplicar un concepto de reservación de tasa de bit (RSVP). Al usuario se le reserva un ancho de banda dentro de la red para su uso exclusivo aún en momentos de congestión. Se lo conoce como Hard QoS.
Diferenciado	El servicio diferenciado utiliza la capacidad de particionar el tráfico en la red con múltiples prioridades o ToS. Se dispone de 3 bits de precedencia para diferenciar las aplicaciones sensibles a la congestión (se brindan mediante el encabezado del protocolo IPv4). Es por lo tanto un Soft QoS. Se puede soportar la función CAR permite administrar el ancho de banda (política de tráfico). La primera línea de defensa frente a la congestión es el uso de buffer de datos; lo cual implica el armado de una cola de espera y el retardo correspondiente dependiendo de la prioridad asignada en dicha cola.
Mejor Esfuerzo	El servicio por el mejor esfuerzo "Best-Effort", es un servicio por default que no tiene en cuenta las modificaciones por la QoS. Se trata de un buffer de memoria del tipo FIFO. Por ejemplo, el software Microsoft NetMeeting para aplicaciones multimedia utiliza la norma H.323; trabaja sobre redes LAN y redes corporativas. Esta norma no tiene previsto garantizar la calidad de servicio QoS.

Tabla II.28 *Clasificación de Calidad de Servicio*

II.2.1.11 CLASE DE SERVICIO COS

La Clase de Servicio (*Class of Service*). CoS se logra mediante 3 bits que se ingresan en un campo adicional de 4 Bytes (etiqueta denominada *Tag* o *Label*) dentro del protocolo MAC. Estos 3 bits permiten definir prioridades desde 0 (máxima) a 7 (mínima) y ajustar un umbral en el buffer de entrada y salida de un switch LAN para la descarga de paquetes.

El mecanismo que se define para la CoS (clase 0 a 7 desde alta a baja prioridad) se compone de las colas de recepción y transmisión. El umbral para extraer los paquetes de la cola de recepción son:

- Clase de servicio CoS 0/1: umbral del 50% (máxima prioridad).
- CoS 2/3: umbral al 60%.
- CoS 4/5: umbral al 80%.
- CoS 6/7: umbral al 100% (mínima prioridad).

En transmisión existen dos colas la de alta y baja prioridad. Su relación con la CoS es la siguiente:

- Cola de baja prioridad (corresponde al umbral del 80%) y CoS 0/1: umbral al 40%; con CoS 2/3: umbral al 100%.
- Cola de alta prioridad (corresponde al umbral del 20%) y CoS 4/5: umbral al 40%; con CoS 6/7: umbral al 100%.

Por ejemplo, una puerta del switch que no fue configurada para CoS tiene un valor por default de umbral del 100%. Un servicio clase CoS=2/3 en el buffer de recepción (entrada al switch) tiene un umbral al 60% para la extracción de paquetes, mientras que en el de transmisión se coloca en alta prioridad (umbral al 20%) y con CoS=2/3 tiene una prioridad adicional del 80%.

II.3 CAPA DE RED

II.3.1 IP V4 PROTOCOLO DE INTERNET VERSIÓN 4

El protocolo IP es el conjunto de protocolos de sistema abierto (no propietario) más popular del mundo, porque puede ser utilizado para comunicarse a través de cualquier conjunto de redes interconectadas, ya sea para comunicaciones LAN o WAN. El protocolo de Internet consiste de un conjunto de protocolos de comunicación, de los cuales los dos son mejor conocidos como TCP Protocolo de Control de Transmisión (*Transmission Control Protocol*) y el IP Protocolo de Internet (*Internet Protocol*). El conjunto de protocolos de Internet no solamente incluye protocolos de capas inferiores (tales como TCP e IP), pero también especifica aplicaciones comunes tales como correo electrónico, emulación de terminal y transferencia de archivos.

El protocolo IP es un protocolo de la capa de red que contiene información de direcciones y alguna información de control que permite a los paquetes ser enrutados, IP especifica que la unidad básica de transferencia de datos en el conjunto de protocolos TCP/IP es el datagrama. Dichos datagrama puede ser: retrasados, perdidos, dedicados, enviados en una secuencia incorrecta intencionalmente. Cabe mencionar que en algunas situaciones en las que se presentan errores en el datagrama estos son descartados sin mandar ningún mensaje de error, mientras que en otras situaciones los mensajes de error son recibidos por la máquina origen.

IP representa el corazón de los protocolo de Internet, y tiene dos principales responsabilidades: proveer servicios no orientados a conexión, entrega al mejor esfuerzo de datagramas a través de una red; y realizar la fragmentación y reensamblaje de los datagramas para soportar enlaces de datos con distintas MTU Unidad Máxima de Transmisión (*Maximum Transmission Unit*)

II.3.1.1 FORMATO DEL PAQUETE IP

Un paquete IP contiene muchos tipos de información, como se ilustra en la figura II.56.

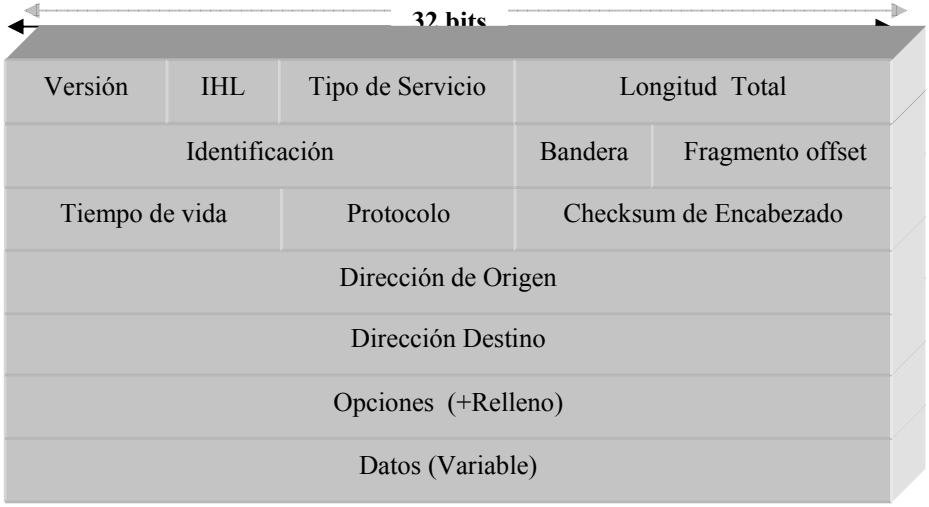


Figura II.56 *Estructura del Datagrama IP*

A continuación se describe los campos del paquete IP, ilustrado en la figura II.98:

- **Versión:** Indica la versión de IP que se esta utilizando.

- **IHL Longitud de Encabezado IP (*IP Header Length*)**: Indica la longitud del encabezado del datagrama en palabras de 32 bits.

- **Tipo de Servicio:** Especifica como el protocolo de capa superior puede manejar el datagrama y asigna niveles de importancia a los datagramas.

- **Longitud Total:** Especifica la longitud en bytes de el paquete IP entero, incluyendo el encabezado y los datos.

- **Identificación:** Contiene un número entero que identifica el datagrama. Este campo se utiliza para juntar las piezas del datagrama fragmentado.

- **Bandera:** Consiste de un campo de 3 bits del cual los 2 bits menos significativos son para control de la fragmentación. El bit de más bajo orden especifica si el paquete puede ser fragmentado. El bit de en medio especifica si el paquete es el ultimo fragmento de la serie de paquetes fragmentados. El tercer bit o el de alto orden no es utilizado.

- **Fragmento Offset:** Indica la posición de los fragmentos de datos relativo al comienzo de los datos en el datagrama original, el cual permite a ala IP destino procesar una apropiada reconstrucción del datagrama original.

- **Tiempo de vida:** Mantiene un contador que gradualmente decrece hasta llegar a cero, con el cual apunta a un datagrama que debe ser descartado. Estos paquetes mantiene un loop infinito.

- **Protocolo:** Indica cual es protocolo de capa superior que recibe el paquete de llegada, después de esto el proceso es completado.

- **Checksum de Encabezado:** Ayuda a segurar la integridad del paquete IP.

- **Dirección de Origen:** Especifica el nodo que envía.

- **Dirección Destino:** Especifica el nodo que recibe.

- **Opciones:** Permite a IP soportar varias opciones, tales como seguridad.

- **Datos:** Contiene información para capas superiores.

II.3.1.2 DIRECCIONAMIENTO IP

Como con cualquier otro protocolo de la capa de red, el esquema de direcciones IP es integral al proceso de ruteo de datagramas IP a través de la red. Cada dirección IP tiene componentes específicos que siguen un formato básico. Las direcciones IP pueden ser subdivididas inutilizadas para crear direcciones de subredes.

Cada host sobre una red TCP/IP es asignado a una única dirección lógica de 32 bits que es dividida dentro de dos partes principales: el número de red y el número de host. El número de red identifica una red y debe ser asignada por la InterNIC[1] si la red será parte de la Internet. Un ISP[2] puede obtener bloques de direcciones de redes desde la InterNIC puede asimismo asignar espacios de direcciones como lo necesite. El número de host identifica un host sobre una red y es asignada por el administrador local de la red.

[1] InterNIC Centro de Información de la Red de Internet (*Internet Network Information Center*)
[2] ISP: Proveedor de Servicios de Internet (*Internet Service Provider*)

II.3.1.3 FORMATO DE DIRECCIONES IP

Los 32 bits de una dirección IP está agrupada a su vez en segmentos de 8 bits, separados por puntos, representado en formato decimal (conocido como *notación punteada decimal*). Cada día en el octeto tiene un peso binario (128, 64, 32, 16, 8, 4, 2, 1), el valor mínimo para un octeto es 0, y el valor máximo para un octeto es 255.

La figura II.99 ilustra el formato básico de una dirección IP.

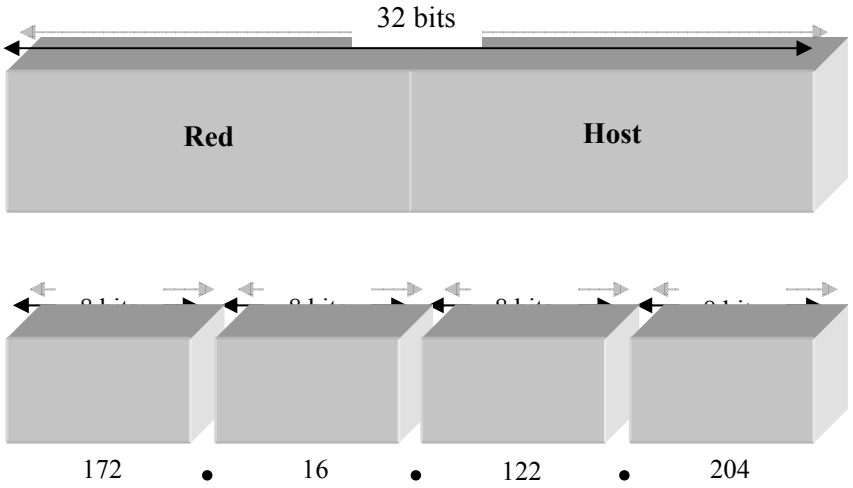


Figura II.57 *Formato de dirección IP y su agrupación en octetos*

II.3.1.4 CLASES DE DIRECCIONES IP

Existe cinco diferentes clases de direcciones: A, B, C, D y E. Solo las clases A, B, y C, son disponibles para uso comercial. El primer bit a la izquierda (bit de alto orden), indica la clase de red. La tabla II.44 indica la información referente a las cinco clases de direcciones IP.

Clase de Dirección IP	Formato	Propósito	Bit de Mayor Orden	Rango de direcciones	N° de Bits Red/Host	N° Máximo de Host
A	N.H.H.H[1]	Organizaciones Grandes	0	1.0.0.0 a 126.0.0.0	7/24	2^{24}-2
B	N.N.H.H.	Organizaciones Medianas	1,0	128.1.0.0 a 191.254.0.0	14/16	2^{16}-2
C	N.N.N.H	Organizaciones Relativamente Pequeñas	1,1,0	192.0.1.0 a 223.255.254.0	24/8	2^{8}-2
D	N/A	Grupos Multicast	1,1,1,0	224.0.0.0 a 239.255.255.255	No para uso comercial	N/A
E	N/A	Experimental	1,1,1,1	240.0.0.0 a 254.255.255.255	N/A	N/A

Tabla II.29 *Clases de direcciones IP*

Nota: Cabe mencionar que se le quitan dos bits al número máximo de host, ya que la primer dirección del rango esta reservada para la red y la ultima para el broadcast.

La clase de la dirección puede determinarse fácilmente examinando el primero octeto de la dirección y mapeando el valor a la clase del rango. En una dirección IP 172.31.1.2, por ejemplo el primero octeto es 172. Porque 172 está entre 128 y 191, 172.3.1.2 es una dirección clase B.

II.3.1.5 DIRECCIONES DE SUBRED IP

Las redes IP pueden ser divididas dentro de pequeñas redes llamadas subredes (subnets). El subneteo provee al administrador de red muchos beneficios, incluyendo flexibilidad extra, un uso más eficiente de las direcciones de red, y la capacidad de encerrar tráfico de broadcast.

Las subredes están bajo administración local. Por lo cual a los ojos del mundo una organización con una sola red no tiene que dar a conocer en detalle la organización de la estructura interna.

Una dirección de red dada puede ser segmentada dentro de muchas subredes. Por ejemplo las direcciones, 172.16.1.0, 172.16.2.0, 172.16.3.0 y 172.16.4.0 son todas subredes dentro de la porción de una dirección de red especificada.

[1] N: Red, H: Host

II.3.1.6 RUTEO DE INTERNET

Los dispositivos de ruteo de Internet tradicionalmente son llamados gateways (puerta de acceso). Hoy en día sin embargo el término gateway se refiere específicamente a un dispositivo que desempeña una interpretación de los protocolos de la capa de aplicación entre dispositivos. Los Gateway Interiores se refieren a dispositivos que desempeñan funciones de protocolos entre máquinas o redes bajo el mismo control administrativo o autoridad, tal como una corporación o una red interna. Es desconocido como sistemas autónomos. Los Gateway Exteriores desempeñan funciones de protocolos entre redes independientes.

Los ruteadores dentro de Internet están organizados jerárquicamente. Los ruteadores se utilizan para intercambiar información con sistemas autónomos llamados ruteadores internos, los cuales utilizan una variedad de IGPs Protocolos de Gateway Interior (*Interior Gateway Protocols*) para cumplir este propósito. El protocolo RIP Protocolo de Información de Enrutamiento (*Routing Information Protocol*) es un ejemplo de un IGP.

Los ruteadores que mueven información entre sistemas autónomos son llamados ruteadores exteriores. Esto ruteadores utilizan un EGP Protocolo de Gateway Exterior (*Exterior Gateway Protocol*) para intercambiar información entre sistemas autónomos. El BGP Protocolo de Gateway Fronterizo (*Border Gateway Protocol*) es un ejemplo de un protocolo de gateay exterior.

II.3.1.7 PROTOCOLOS DE RUTEO

Como se mencionó anteriormente existen protocolos de ruteo interior cuya función es la de intercambiar información necesaria para poder localizar algún equipo dentro del sistema autónomo. Como también se indicó también existen los llamados protocolos de ruteo externo cuya función es permitir la comunicación entre sistemas autónomos.

A continuación se muestra una clasificación de los protocolos de ruteo tan internos como externos, así como una breve descripción de ellos:

- **IGPs:** Estos protocolos encargan de intercambiar la información necesaria para poder localizar algún equipo dentro de un sistema autónomo. Por ejemplo entre los más usuales tenemos: RIP, IGRP, EIGRP y OSPF.

- **EGPs**: Estos protocolos son utilizados para mover información entre sistemas autónomos. Solamente los ruteadores que conecten sistemas autónomos con otros necesita soportarlos. Por ejemplo: BGP.

- **RIP**: Es un protocolo de ruteo interior que utiliza el algoritmo de ruteo de vector distancia, es decir utiliza una selección de rutas con base a una métrica en la cantidad de saltos. El máximo número de saltos permitidos es de 15 y la actualización de las tablas se realiza cada 30 segundos por default. Este protocolo fue diseñado para ambientes con pocas máquinas con características idénticas.

- **IGRP**[1]: Este protocolo utiliza el algoritmo de vector distancia y fue desarrollado por CISCO, incluye el uso de variables métricas del tipo: ancho de banda, retardo, carga, confiabilidad. Este protocolo hace sus anuncios de ruteo en periodos de 90 segundos, así mismo es escalable para funcionar en redes muy grandes. Una diferencia con RIP es la formación de las métricas y el uso de las redes por default.

- **EIGRP**[2]: El IGRP Mejorado representa una evolución de su predecesor IGRP. Esta evolución resulta de los cambios en interconexión de redes y la demanda de redes de gran escala. EIGRP integra la capacidad de los protocolos de estado de enlace dentro de los protocolos vector distancia.

- **OSPF**[3]: Para permitir el crecimiento y hacer las redes de una localidad fáciles de manejar, el OSPF permite que una localidad divida sus redes y ruteadores en subconjuntos llamados áreas, OSPF incluye un ruteo de *servicio de tipo*. Los administradores pueden instalar múltiples rutas hacia un destino dado, uno por cada tipo de servicio. OSPF proporciona *balanceo de carga*, así como también especifica que todos los intercambios entre ruteadores deben ser *autenticados.*

- **BGP**[4]**:** Protocolo de enrutamiento entre dominios que reemplaza a EGP, es un protocolo de un sistema autónomo el cual puede contener múltiples dominios de direccionamiento, cada uno con su propio protocolo interno de sistema autónomo.

II.3.2 IPX

El protocolo IPX (*Internetwork Packet eXchange*) fue desarrollado por Novell a mediados de los 80's basandose en el protocolo XNS desarrollado por Xerox. El protocolo IPX fue el protocolo dominante en la epoca de los 80's y principios de los 90's.

[1] IGRP: Protocolo de Enrutamiento de Gateway Interior (*Interior Gateway Routing Protocol*)
[2] EIGRP: IGRP Mejorado (*Enhaced IGRP*)
[3] OSPF : Abre Primero la Ruta mas Corta (*Open Shortest Path First*)
[4] BGP: Protocolo de Gateway Fronterizo (*Border Gateway Protocol*)

En la figura se muestra la trama e un datagrama IPX el cual tiene un formato parecido al de IP con la diferencia que este contiene los *sockets* de fuente y destino. Estos campos tienen el mismo proposito que los numeros de puerto de UDP, distinguiendo las diferentes aplicaciones de un sistema.

El encabezado de IPX no soporta varias de las opciones que tiene IP. En particular no realiza la fragmentacion, ni tampoco ruteo de destino o seguridad.

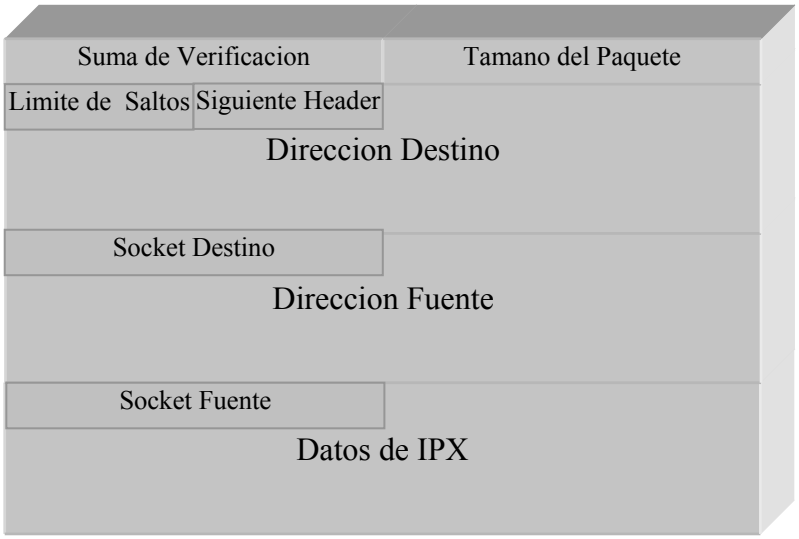


Figura II.58 *IPX*

II.3.2.1 DIRECIONAMIENTO IPX

IPX tiene una direccion de 80 bits. Los primeros 32 bits representan la direccion de red y los ultimos 48 bits representan la dirección del nodo. La dirección de red es seleccionada por el administrador. La direccion del nodo es tomada de la direccion de la interfaz MAC. Para uan interface serial, la direccion del nodo es tomada la primera intefaz de la LAN.

II.3.3 APPLE TALK

Appletalk , una habitación del protocolo desarrollada por la computadora de Apple en los años 80 tempranos, fue desarrollado conjuntamente con la computadora de Macintosh. De Appletalk tales como propósito era permitir que los usuarios múltiples compartan recursos, de los archivos y las impresoras. Los dispositivos que proveen estos recursos se llaman los servidores, mientras que los

dispositivos que hacen uso estos recursos (tales como computadora de Macintosh de un usuario) se refieren como clientes. Por lo tanto, Appletalk es una de las puestas en práctica tempranas de un sistema client/server distribuido del establecimiento de una red.

Appletalk fue diseñado con un interfaz transparente de la red -- es decir, entre la interacción las computadoras del cliente y los servidores de la red requiere poca interacción del usuario. Además, las operaciones reales de los protocolos de Appletalk son invisibles terminar a los usuarios, que ven solamente el resultado de estas operaciones. Dos versiones de Appletalk existen: Fase 1 de Appletalk y fase 2 de Appletalk.

La fase 1 de Appletalk, que es la primera especificación de Appletalk, fue desarrollada en los años 80 tempranos terminantemente para el uso en workgroups locales. La fase 1 por lo tanto tiene dos limitaciones dominantes: Sus segmentos de la red pueden contener no más de 135 anfitriones y 135 servidores, y puede apoyar solamente redes no extendidas.

La fase 2, que de Appletalk es el segundo realzó la puesta en práctica de Appletalk, fue diseñada para el uso en internetworks más grandes. La fase 2 trata las limitaciones dominantes de la fase 1 de Appletalk y ofrece un número de mejoras sobre la fase 1.

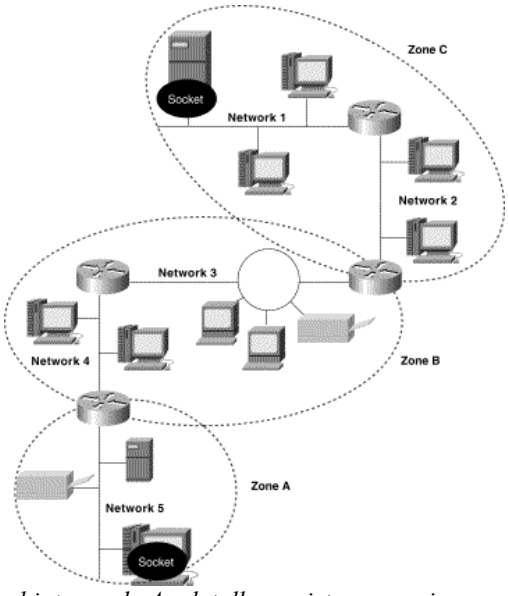


Figura II.59 *La red interna de Appletalk consiste en una jerarquía de componentes*

II.3.3.1 ZÓCALOS

Un zócalo de Appletalk es una localización única, direccionable en un nodo de Appletalk. Es el punto lógico en el cual los procesos del software de Appletalk de la capa superior y el protocolo de la entrega del datagrama de la capa de red (DDP) obran recíprocamente. Estos procesos de la capa superior se conocen como clientes del zócalo. Los clientes del zócalo poseen unos o más zócalos, que utilizan enviar y recibir datagramas. Los zócalos se pueden asignar estáticamente o dinámicamente. Los zócalos estáticamente asignados son reservados para el uso por ciertos protocolos u otros procesos. Los zócalos dinámicamente asignados son asignados por DDP a los clientes del zócalo por requerimiento. Un nodo de Appletalk puede contener hasta 254 diversos números del zócalo. En la figura se ilustra la relación entre los zócalos en un nodo de Appletalk y un DDP en la capa de red.

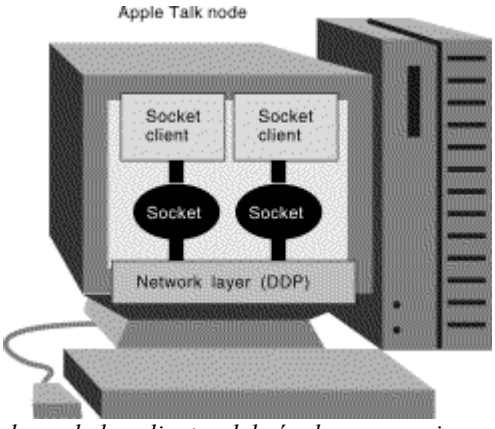


Figura II.60 *Zócalos del uso de los clientes del zócalo para enviar y para recibir datagramas*

II.4 CAPA DE TRANSPORTE

II.4.1 DATAGRAMAS

La unidad de datos que se transmite entre máquinas es el datagrama. Toda la información recibida por la capa IP, proveniente de la capa servicios y de las aplicaciones, es colocada en paquetes para ser enviada a través de la red. Cada uno de estos paquetes es un datagrama, que contiene toda la información referencial para que pueda ser enviado entre dos máquinas de la Red.

Al inicio del paquete, se encuentra el encabezado (header) que contiene:

Version: Versión del IP.

***IHL*:** Longitud del encabezado en palabras (32 bits c/u).

***TOS*:** Tipo de servicio.

***Total length*:** Longitud del datagrama en bytes.

***Identification*:** Identificador de un datagrama para la fragmentación.

***Flags**:* Banderas para controlar la fragmentación y el reensamblaje.

***Offset**:* Ubicación de un fragmento dentro de un paquete.

Time to live: Tiempo de vida del paquete en segundos.

Type: El protocolo de servicio que está haciendo uso de este paquete.

Checksum: Cuenta para verificar la integridad del encabezado.

Source Address: Dirección IP origen.

Destination Address: Dirección IP destino.

Padding: Bits de relleno

DATAGRAMAS Y SESIONES.

El servicio de datagramas ofrece una conexión no estable entre una máquina y otra. Los paquetes de datos son simplemente enviados o difundidos (broadcasting) de una máquina a otra, sin considerar el orden en que estos llegan al destino, o si han llegado todos. El uso de datagramas no incrementa tanto el trafico de la red como el uso de sesiones, aunque pueden echar abajo una red si se usan indebidamente (¿Te acuerdas de la difusión de la resolución de nombres de antes?) Los datagramas, por tanto, son empleados para enviar rápidamente sencillos bloques de datos a una o más máquinas. El servicio de datagramas comunica usando las primitivas simples mostradas en la Tabla II.45.

Primitivas de Datagramas.	
Primitiva	**Descripción**
Send Datagram	Envía paquete datagrama a máquina o grupos de máquinas.
Send Broadcast Datagram	Difunde (broadcast) datagrama a cualquier máquina, esperando un datagrama de acuse de recibo.
Receive Datagram	Recibe un datagrama de una máquina.
Receive Broadcast Datagram	Espera por un datagrama de difusión.

Tabla II.30 *Primitivas de datagramas*

El servicio de sesiones es más complejo. Las sesiones son un método de comunicación que, en teoría, ofrece la capacidad de detectar conexiones problemáticas o inoperativas entre dos aplicaciones NetBIOS. Esto lleva a pensar en una sesión NBT en términos de una llamada telefónica. Una conexión full-duplex es abierta entre una máquina que llama y una máquina que es llamada, y la conexión debe permanecer abierta durante la duración de la conversación. Cada parte implicada conoce a la otra máquina, y pueden comunicar con las primitivas que se muestran en la Tabla II.46.

Primitivas de Sesiones.	
Primitiva	**Descripción**
Call	Inicia una sesión con una máquina que está a la escucha bajo un nombre específico.
Listen	Espera una llamada de un llamante conocido o cualquier otro.
Hang-up	Termina una llamada.
Send	Envía datos a la otra máquina.
Receive	Recibe datos de la otra máquina.
Session Status	Obtiene información sobre sesiones pedidas.

Tabla II.31 *Primitivas de sesiones*

Las sesiones son el troncal de la compartición de recursos en una red NBT. Son normalmente usadas para establecer conexiones estables desde máquinas clientes a unidades de disco o impresoras compartidas en un servidor. El cliente "llama" e inicia la conversación, enviando información del tipo qué ficheros desea abrir, qué datos quiere intercambiar, etc. Estas llamadas pueden durar mucho tiempo -horas, incluso días- y todo esto ocurre dentro del contexto de una única conexión. Si se produce un errorerror, el software de sesión (TCP) retransmitirá hasta que los datos

sean recibidos correctamente, a diferencia del "envía-y-reza" del servicio de datagramas (UDP).

En realidad, mientras que las sesiones se supone están para manejar comunicaciones problemáticas, normalmente no lo hacen. Como probablemente habrás descubierto al usar redes Windows, es un serio problema el usar sesiones NBT. Si la conexión es interrumpida por la razón que sea, la información de sesión que está abierta entre dos computadoras puede fácilmente volverse inválida. Si esto ocurre, la única forma de restablecer la sesión para las dos mismas máquinas es llamar de nuevo y comenzar desde ceero.

Sin embargo, hay dos cosas importantes a recordar aquí:

- Las sesiones siempre ocurren entre dos máquinas NetBIOS -ni más ni menos. Si un servicio de sesión es interrumpido, se supone que el cliente ha almacenado la suficiente información de estado como para restablecer la comunicación. Sin embargo, en la práctica, es raro el caso.
- Los datagramas pueden ser difundidos a múltiples máquinas, pero son inestables. Dicho de otro modo, no hay forma para el emisor de saber si los datagramas que ha enviado han llegado correctamente a los destinatarios.

ENCAPSULACIÓN DE DATAGRAMAS.

Tamaño máximo de los datagramas = 2^{16}= 65,535 bytes (depende de la versión).

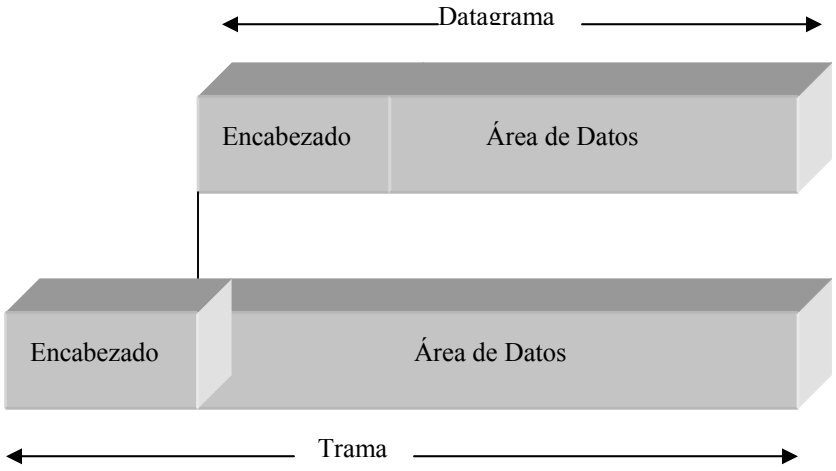


Figura II.61 *Encapsulación de un Datagrama en una Trama.*

IP fue diseñado para ajustarse a medios de transmisión poco confiables. Estos medios pueden ser desde enlaces seriales sobre redes telefónicos hasta enlaces de alta velocidad tipo LAN (Ethernet). Es posible que el medio subyacente emplee algún esquema similar. En Ethernet por ejemplo, la información es colocada, por pedazos, en los llamados marcos (frames) para su transmisión. La independencia entre IP y los niveles inferiores puede causar que un datagrama IP sobrepase la capacidad de un marco Ethernet. En tales casos, se recurre a la fragmentación por el remitente y el reensamble en el destino.

CABECERA

En la cabecera hay una parte fija de 20 bytes y una parte opcional de longitud variable. En la siguiente figura se puede ver el formato de la cabecera IP.

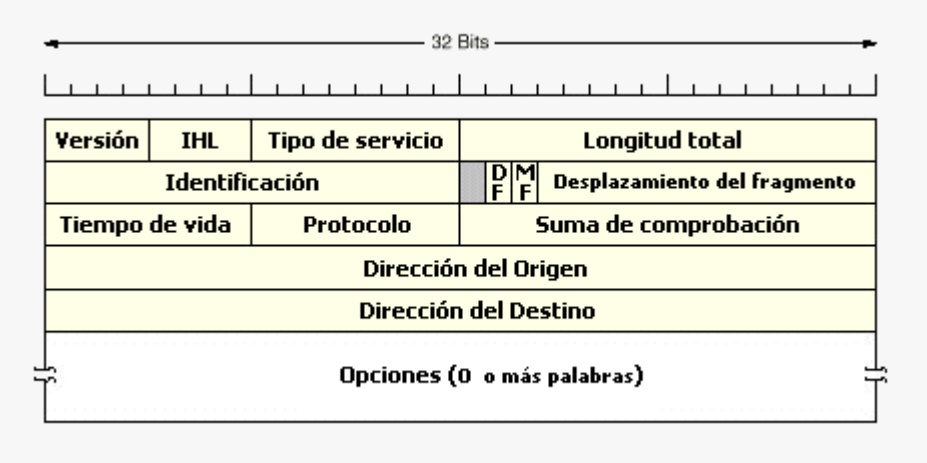


Figura II.62

II.4.2 TCP

En esta parte se introduce el segundo servicio más importante y mejor conocido de nivel de red, entrega de flujo confiable, así como el protocolo TCP Protocolo de Control de Transmisión (*Transmission Control Protocol*), que lo define. Veremos que el TCP añade una funcionalidad sustancial a los protocolos que ya hemos analizado, pero también veremos que su implantación es sustancialmente más compleja.

Aunque aquí se presenta el TCP como parte del grupo de protocolos de Internet TCP/IP, es un protocolo independiente de propósitos generales que se puede adaptar para utilizarlo con otros sistemas de entrega. Por ejemplo, debido a que el TCP

asume muy poco sobre la red subyacente, es posible utilizarlo en una sola red como Ethernet así como en una red de redes compleja.

II.4.2.1 NECESIDAD DE LA ENTREGA DE FLUJO

En el nivel más bajo, las redes de comunicación proporcionan una entrega de paquetes no confiable. Los paquetes se pueden perder o destruir cuando los errores de transmisión interfieren con los datos, cuando falla el hardware de red o cuando las redes se sobrecargan demasiado. Las redes que rutean dinámicamente los paquetes pueden entregarlos en desorden, con retraso o duplicados.

En el nivel más alto, los programas de aplicación a menudo necesitan de evitar grandes volúmenes de datos de una computadora a otra. Utilizar un sistema de entrega sin conexión y no confiable para la transferencia de gran volumen, se vuelve tedioso y requiere que los programadores incorporen, en cada programa de aplicación, la detección y solución de errores.

Tener un solo protocolo de propósito general es útil para aislar los programas de aplicación de los detalles del trabajo con redes y permite la definición de una interfaz uniforme para servicio de transferencia de flujo.

II.4.2.2 FAMILIA DE PROTOCOLOS TCP/IP

TCP/IP es un conjunto de protocolos que actúan en diferentes niveles del modelo de referencia OSI. El nivel de transporte está regido ya sea por el protocolo TCP o UDP, la diferencian en ambos es, el TCP proporciona un servicio orientado a conexión, mientras que UDP proporciona un servicio no orientado a conexión; TCP tiene la capacidad de proporciona un servicio confiable entre dos máquinas, mientras que UDP permite transmitir datos a una o varias máquinas sin necesidad de establecer una conexión. En UDP los datagramas se envían sin esperar confirmación de recepción. En resumen UDP es utilizado en redes donde los medios de transmisión son bastante confiables y los parámetros de confiabilidad, como controles de flujo, temporizadores, son innecesarios. Dichas redes pueden ser LAN manejando aplicaciones con protocolos de estratos superiores como FTP. En cambio TCP al proporcionan un servicio orientado a conexión y debido a la confiabilidad que puede manejar implica un aumento significativo en el encabezado del datagrama para el manejo de control de flujo, temporizadores y para la confirmación de recibido y entregado.

II.4.2.3 DESCRIPCIÓN DEL TCP

El TCP es complejo, por lo que no hay una descripción sencilla. El protocolo especifica el formato de datos y los acuses de recibo que intercambian dos computadoras para lograr una transferencia confiable, así como los procedimientos que la computadora utiliza para lograr una transferencia confiable, así como los procedimientos que la computadora utiliza para asegurar que los datos lleguen de manera correcta. También, especifica como el software TCP distingue el correcto entre muchos destinos en una misma máquina, y cómo las máquinas en comunicación resuelven errores como la pérdida o duplicación de paquetes. El protocolo también especifica como dos computadoras inician una transferencia de flujo TCP y cómo se ponen de acuerdo cuando se completa.

Asimismo, es importante entender lo que el protocolo no incluye. Aunque la especificación TCP describe cómo utilizan el TCP los programas de aplicación en términos generales, no aclara los detalles de la interfaz entre un programa de aplicación y el TCP.

II.4.2.4 CARACTERÍSTICAS FUNCIONALES DE TCP

A continuación se listan las características mas importantes de TCP:

- La unidad básica de transferencia utilizada por el TCP es el segmento.
- Se encuentra definido en los RFCs 793 y 1122
- TCP se utiliza para hacer que la transferencia de datagramas se vuelva solida y confiable de aplicación a aplicación.
- La función de TCP es la de asegurar que la transferencia de datos se realice de manera confiable, en secuencia sin confusiones o errores.
- TCP provee los mecanismos de control de flujo para que el receptor pueda regular la cantidad de información que el transmisor le esta enviando.

DESCRIPCIÓN DEL FUNCIONAMIENTO DE TCP

1. La aplicación envía a TCP los datos que desea transmitir

2. TCP los ensambla en segmentos y les asigna un número de secuencia y un

3. número de *checksum*, para chequeo de errores.

4. La longitud del segmento la establece TCP.

5. Antes de enviar la información para su enrutamiento, TCP establece un Circuito Virtual, para garantizar la comunicación en los dos sentidos.

6. TCP verifica si los paquetes se encuentren libres de errores (Checksum), si es así envía una confirmación de recibido (ACK[1]).

7. Se encarga de acomodar los paquetes de acuerdo al número de secuencia.

8. En caso de recibirse un mensaje duplicado o con error, lo descarta.

II.4.2.5 FORMATO DEL SEGMENTO TCP

La unidad de transferencia entre el software TCP de dos máquinas se conoce como segmento. Los segmentos se intercambian para establecer conexiones, transferir datos, enviar acuses de recibo, anunciaron los tamaños de ventanas y para cerrar conexiones. En la figura II.105 se muestra el formato del segmento TCP.

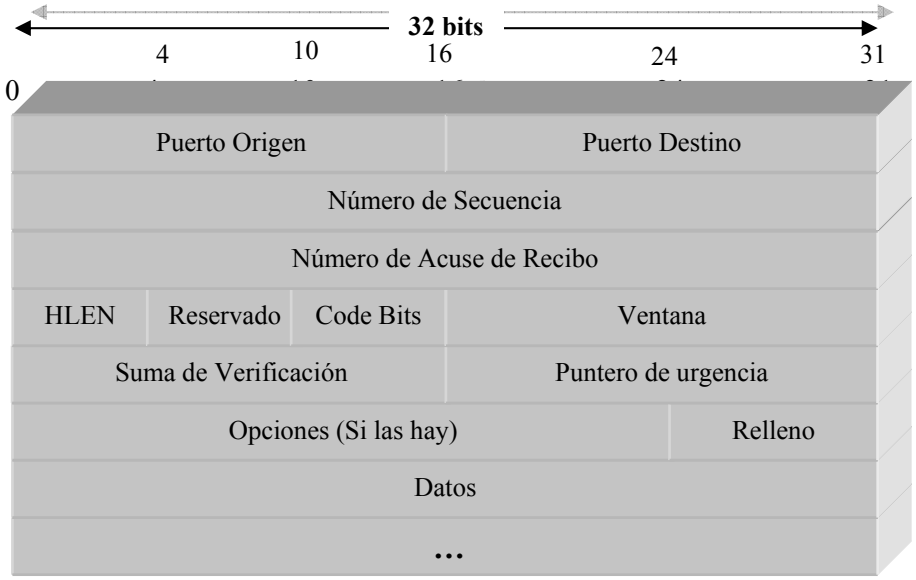


Figura II.63 *Formato del segmento TCP*

En la figura II.107 se describió el formato de un segmento TCP con un encabezado TCP seguido de datos. Los segmentos se utilizan para establecer conexiones, así como para transportar datos y acuses de recibo. En la estructura del segmento TCP en donde los campos más importantes se consideran: el identificador del puerto fuente y el identificador del puerto destino, número de secuencia y número de acuses de recibo.

[1] ACK Acuse de Recibo (*Acknowledgement*)

II.4.3 UDP

El Protocolo de Datagrama de Usuario o (UDP *User Datagrab Protocol* por sus siglas en ingles) proporciona el mecanismo primario que utilizan los programas de aplicación para enviar datagramas a otros programas de aplicación. El UDP proporciona puertos de protocolo utilizados para distinguir entre muchos programas que se ejecutan en la misma maquina. Esto es, además de los datos, cada mensaje UDP contiene tanto el número de puerto de destino como el número de puerto de origen, haciendo posible que el software UDP en el destino entregue el mensaje al receptor correcto y que este envié una respuesta.

El UDP utiliza el Protocolo Internet subyacente para transportar un mensaje de una maquina a otra y proporciona la misma semántica de entrega de datagramas, sin conexión y no confiable que el IP. No emplea acuses de recibo para asegurarse de que lleguen mensajes, no ordena los mensajes entrantes, ni proporciona retroalimentación para controlar la velocidad a la que fluye la información entre las maquinas. Por lo tanto, los mensajes UDP se pueden perder, duplicar o llegar sin orden. Además, los paquetes pueden llegar mas rápido de lo que el receptor los puede procesar.

En general el protocolo de datagrama de usuario (UDP) proporciona un servicio de entrega sin conexión y no confiable, utilizando el protocolo IP para transportar mensajes entre maquinas. Emplea IP para llevar los mensajes, pero agrega la capacidad para distinguir entre varios destinos dentro de una computadora anfitrión.

Un programa de aplicación que utiliza UDP acepta toda la responsabilidad por el manejo de problemas de confiabilidad, incluyendo la perdida, duplicación y retraso de los mensajes, la entrega fuera de orden y la perdida de conectividad. Por desgracia, los programadores de aplicaciones a menudo olvidan estos problemas cuando diseñan software. además, como los programadores a menudo prueban el software de red utilizando redes LAN que son altamente confiables y de baja demora, el procedimiento de pruebas puede no evidenciar las fallas potenciales, Por lo tanto, muchos programas de aplicación que confían en el UDP trabajan bien en un ambiente local, pero fallan dramáticamente cuando se utilizan en redes mas grandes.

II.4.3.1 FORMATO DE LOS MENSAJES UDP

Cada mensaje UDP se conoce como datagrama de usuario. Conceptualmente, un datagrama de usuario consiste de dos partes: un encabezado UDP y un área de datos UDP. Como se muestra en la figura, el encabezado se divide en cuatro campos de bits, que especifican el puerto desde el que se envió el mensaje, el puerto para el que se destina el mensaje, la longitud del mensaje y una suma de verificación UDP.

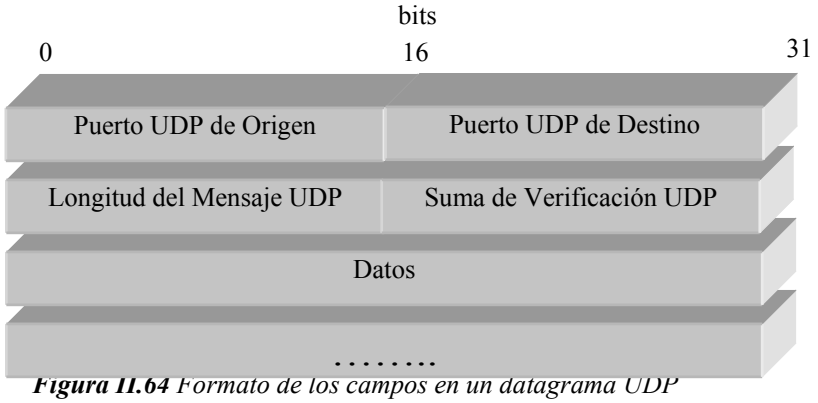


Figura II.64 *Formato de los campos en un datagrama UDP*

Los campos Puerto de orien y Puerto Destino contienen los numeros de puerto del protocolo UDP utilizados para el demultiplexado de datagramas entre los procesos que los esperan recibir. El puerto Origen es opcional. Cuando se utioliza, especifica la parte a la que se deben en viar las repuestas, de lo contrario, puede tener valor de cero.

El campo de longitud contiene un conteo de los octetos en el datagrama UDP, incluyendo el encabezado y los datos del usuario UDP. Por lo tanto, el valor minimo para el campo longitud es de ocho, que es la longitud del encabezado.

La suma de verificacion UDP es opcional y no es necesario utulizarla; un valor de cero en el campo Suma de Verificacion significa que la suma nmo se computo. Los diseñadores decidieron hacer opcional la suma de verificacion a fin de permitir que las implantaciones operen con poco trabajocomputacional cuando utilice UDP en una red LAN altamente confiable. Sin embargo, recuerde que el protocolo IP no computa unasuma de verificacion de la porcion de datos de un datagramaIP. Asi que, la suma de verificacion UDP proorciona la unica manera de garantizar que los datos lleguen intactos, por lo que se debe utilizar.

II.4.3.2 ENCAPSULAMIENTO DE UDP Y ESTRATIFICACION POR CAPAS DE PROTOCOLOS

El UDP proporciona es un protocolo de transporte. Dentro del modelo OSI, el UDP reside en la capa 4. Conceptualmente, los protocolos de los programas de aplicación accesan el UDP, que utiliza a su vez IP para enviar y recibir datagramas como se muestra en la figura siguiente.

Figura II.65 *Estratificacion conceptual por capas de UDP entra aplicación e IP*

Estratificar por capas el UDP por encima de IP significa que un mensaje UDP completo, incluyendo el encabezado UDP y los datos, se encapsulan en un datagrama IP mientras viaja a traves de una red, tal como se muestra en la figura.

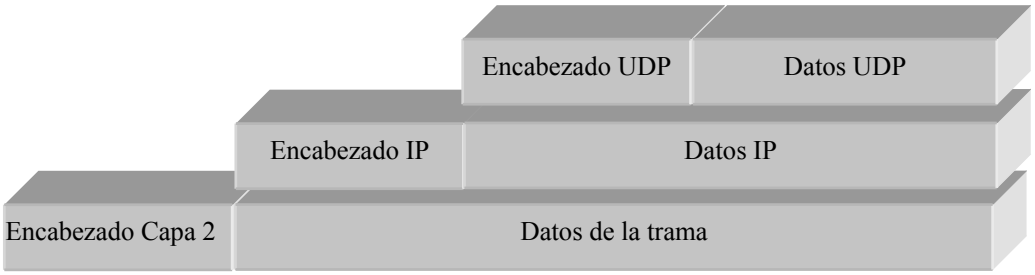


Figura II.66 *Datagrama UDP encapsulado en un dataraga IP para su transmision a traves de la red*

Para los protocolos que hemos examidado, la encapsulacion significa que el UDP adjunta un encabezado a los datos que un usuario envia y lo pasa al IP. La capa IP adjunta un encabezado a loque recibe del UDP, Y por ultimo, la capa de interfaz de red introduce el datagrama en una trama antes de enviarlo de una maquina a otra. El formato de la trama depende de la tecnologia subyacente de la red. Por lo general, las tramas de red incluyen un encabezado adicional.

En la entrada, un paquete llega en la capa mas baja del software e red y comienza su asenso a traves de capas sucesivamentem mas altas. Cada capa quita un encabezado antes de pasar el mensaje para que, en el momento en que el nivel mas alto pasa los datos al proceso receptor, todos los encabezados se hayan removido. Por lo tanto, el encabezado exterior corresponde a la capa mas baja de protocolo y el encabezado interior a la mas alta de protocolo. Cuando se considera como se insertan y remueven os encabezados, es importante rener en cuenta el pricipio de la estratificacion por capas. En lo particular, observe que este principio se aplica al UDP, asi que el datagrama UDP que recibio el IP en la maquina de destino es identico al datagrama que el UDP paso al IP en la maquina de origen. Tambien, los datos que el UDP entraga a un proceso usuario en la maquina receptora sreran los mismos que un proceso usuairo pase al UDP en la maquina transmisora.

La division de funciones entre varias capas de protocolos es inflexible y clara: La capa de IP solo es responsable de transferir datos entre un par de anfitriones dentro de una red, miestras que la capa UDP solamente es responsable de diferenciar entre varias fuentes o destinos dentro de un anfitrion.

Por lo tanto, solo el encabezado IUP identifica los anfitriones de origen y destino solo la capa UDP identifica los puertos de origen y destino dentro de un anfitrion.

II.4.3.3 MULTIPLEXADO, DEMULTIPLEXADO Y PUERTOS DE UDP

El software UDP proporciona el multiplexado y demultiplexado. Acepta datagramas UDP de muchos programas de aplicación y los pasa a IP para su transmision, tambien acepta datagramas entrantes UDP del IP y los transfiere al programa de aplicación apropiado.

Conceptualmente, todo el multiplexado y el demultiplexado entre el software UDP y los programas de aplicación acorre a traves del mecanismo de puerto. En la practica, cada programa de aplicación debe negociar cpon el sistema operativo para obtener un puerto el protocolo y numero de puerto asociado, antes de poder enviar un datagrama UDP. Una vez que se asigna el puerto, cualquier datagrama que envie el programa de aplicación a traves de el, trendra el numero de puerto en el campo de puerto de origen UDP.

Mientras procesa la entrada, el UDP acepta datagramas entrantes del software IP y los demultiplexa, basandose en el puerto de destino UDP, como se muestraen la figura II.109.

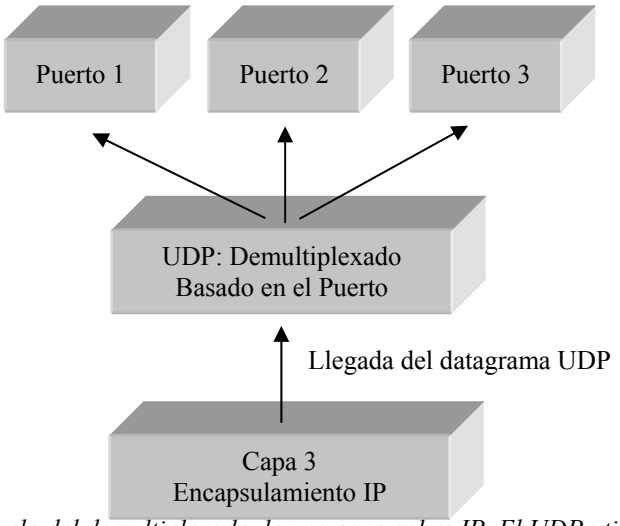


Figura II.67 *Ejemplo del demultiplexado de una capa sobre IP. El UDP utiliza el numero de puerto UDP de destino para selelccionar el puerto apropiado de destino para los datagramas entrantes.*

La forma mas facil de pensar em um puerto UDP es en una cola de espera. En ,la mayor parte de la implantaciones, cuando un programa de aplicación negocia con el sistema operativo la utilizacion de cierto puerto, el sistema operativo crea una cola de espera interna que puede almacenar los mensajes que lleguen. A menudo, la aplicación puede especificar o modificar el tama;o de la cola de espera. Cuandpo el UDP recibe un datagrama, verifica si el numero de puerto de destino scorresponde a uno de los puertos que estan en uso. Si no envia mensaje de error ICMP de puerto no accesible y descarta el datagrama. Si encuentra una correspondencia, el UDP pone en cola de espera el nuevo datagrama, en el puerto en que lo pueda accesar un programa de aplicación. Por supuesto, ocurre un error si el puerto se encuentra lleno y el UDP descarta el datagrama entrante.

II.4.3.4 NUMERO DE PUERTOS UDP RESERVADOS Y DISPONIBLES

Existen dos enfioques fundamentales para la asignacion de puertos. El primero se vale de una autoridad central. Todos se ponen de acuerdo en permitir que una autoridad central asigne los numeros de puerto conformese necesitan y publique la lista de todas las asignaciones. Entonces, todo el software se dise;a de acuerdo con la lista. Este enfoque, a veces, se conoce como enfoque universal y a las asignaciones de puerto especificadas por la aotoridad se conocen como asignaciones bien conocidas de puerto.

El segundo enfooque para la asignacion de puertos emplea la treansformacion dinamica. En este enfoque, los puertos no se conocen de manera global. En vez de eso, siempre que un rograma necesita un uerto, el software de red le asigna uno. Para conocer la asignacion actual de puerto en otra computadora, es necesario enviar una solicitud que pregunte que puerto esta utilizando el servicio de transferencia de archivos., asi la maquina objetivo responde al proporcionar el numero de puerto correcto a utilizar. Los diseñadores adoptaron un enfoque hibrido que preasigna algunos numeros de puerto, pero que deja muchos de ellos disponibles para los sitios locales o programas de aplicación. Los numeros de puerto asignados comienzan con valores bajos y se extienden hacia arriba, dejando disponibles valores de numeros enteros altos para la signacion dinamica. En la tabla siguiente se listan algunos de los numeros de puerto UDP actualmente asignados. La segunda columna contiene palabras clave asignadas como estanadar de Internet y la tercera contiene palabras clave utilizadas en la mayor parte de los sistema UNIX.

Decimal	Palabra clave	Palabra clave UNIX	Descripcion
0	-	-	Reservado
7	ECHO	Echo	Eco
9	DISCARD	Discard	Descartar
11	USERS	Systat	Usuarios Activos
13	DAYTIME	Daytime	Hora del dia
15	-	Netstat	Quien esta ahí o netstat
17	QUOTE	Qotd	Cita del dia
19	CHARGEN	Chargen	Generador de caracteres
37	TIME	Time	Hora
42	NAMESERVER	Name	Servidor de nombres de anfitriones
43	NICNAME	Whois	Quien es
53	DOMAIN	Nameserver	Servidor de nombres de dominios
67	BOOTPS	Bootps	Servidor de protocolo bootstrap
68	BOOTPC	Bootpc	Cliente de protocolo bootstrap
69	TFTP	Tftp	Transferencia trivial de archivos
111	SUNRPC	Sunrpc	RPC de Sun Microsystems
123	NTP	Ntp	Porotocolo de tiempo de red
161		Snmp	Monitor de red SNMP
162		Snmp-trap	Interrupciones SNMP
512		Biff	Comsat UNIX
513		Who	Rwho daemon UNIX
514		Syslog	Conexión de sistema
525		Timed	Daemon de hora

Tabla II.32 *Puertos asignados para UDP*

III

REDES DE ALTA DISPONIBILIDAD

Hoy en día las redes modernas han llegado a ser cruciales en nuestras vidas. Los departamentos de policía, hospitales, los negocios y virtualmente de cualquier organización, dependemos del buen funcionamiento de sus sistemas de computadoras conectadas a una red, y mientras más dependemos de estos sistemas, más nos afectan cuando estos dejan de funcionar.

Para todos aquellos que están envueltos en la planificación, diseño, construcción, y funcionamiento de estas redes, es necesario que sepan y puedan predecir problemas que afecten o que puedan afectar los tiempos activos de la red. Predecir los problemas nos permite reducir el impacto de estos, y con las predicciones de la disponibilidad de la red, nosotros podemos asegurar que dichas redes van a dar un servicio eficiente a la gente antes de que se empiece la construcción de estas, y por otra parte aseguramos que los usuarios puedan utilizar en cualquier momento los beneficios y recursos que dichas redes ofrecen.

III.1 INTRODUCCIÓN A LAS REDES DE ALTA DISPONIBILIDAD

Recientemente, el crecimiento de Internet y el uso de sistemas de cómputo para los negocios han florecido en cierto modo más de lo que se tenía esperado. En 1990, fue posible contactar a individuos de algunas compañías (principalmente compañías de cómputo) vía correo electrónico, y solo una década después, miles de compañías estaban ofreciendo a los consumidores la disponibilidad de comprar productos de sus sitios Web en Internet. Este crecimiento fantástico de Internet y de las redes de datos tiene y está cambiando nuestra vida de muchas maneras.

Como Internet y las redes de datos se vuelven parte de nuestras vidas, nosotros nos estamos volviendo dependientes de estas, y para que nosotros confiemos en estas, necesitamos hacer que estas sean muy confiables. Cuando se dice que se quiere una red muy confiable, se está diciendo que se quiere una red para trabajar en cualquier momento, y se requiere que este siempre disponible.

III.1.1 PORQUE NECESITAMOS LA ALTA DISPONIBILIDAD

Nosotros hemos venido a depender del uso de computadoras, el acceso al Internet, y la ayuda de nuestros sitios favoritos de Internet. Muchas personas compran regularmente las cosas en Internet, y ellos esperan poder acceder a Internet para ir de compras 24 horas por día, siete días por semana.

Las redes de hoy no solo llevan simplemente transacciones de ventas e información de un negocio. De hecho en algunos lugares, se puede utilizar un teléfono, marcar un número telefónico, y la llamada telefónica pasa sobre una red de datos en lugar de la infraestructura de la compañía de teléfono tradicional, así el tráfico de voz también está volviéndose otra parte de las redes de datos, y las redes de datos están comenzando a ser parte del sistema telefónico.

En algunas ciudades, los consumidores pueden comprar su servicio telefónico a una compañía de cable en lugar de una compañía de telefonía tradicional, y estas personas dependen del equipamiento de la redes para hacer uso de los servicios de emergencia, por ejemplo imagínese si se levanta el teléfono para marcar un numero de emergencia y no se obtuvo tono de marcado. Cuando alguna vida depende de una red, la disponibilidad de la red es crucial y puede ser una cuestión de vida o muerte, y es por esto que la disponibilidad de la red se convierte ahora en un miembro de un club exclusivo en hospitales, ambulancias, y de doctores que pueden salvar alguna vida.

III.1.2 MAYOR CONFIABILIDAD DE LAS REDES EN LA ACTUALIDAD

La forma en que las compañías y las organizaciones hacen uso de las redes ha cambiado con el transcurso del tiempo. Mientras que en algún momento se pudo asumir que los proyectos de Tecnología de Información (IT[1]) eran mayormente de naturaleza interna, como se menciono en capítulos anteriores, las iniciativas actuales pueden llegar a enfatizar una conectividad externa, tal vez con intranets que conectan varias localidades corporativas o con extranets que se conectan con clientes y proveedores. Este tipo de *networking* permite una comunicación directa, independientemente del lugar en que se encuentren, así como obtener una cadena de suministro mucho más efectiva. Las intranets fomentan de manera significativa la eficiencia de los empleados, a la vez de permitir un despliegue más rápido de las nuevas aplicaciones comerciales en comparación con el pasado.

Estas nuevas demandas han igualado los cambios en las tecnologías de computación y de red, y a su vez han generado la necesidad de la introducción de PC's, así como también la caída en la centralidad de la estructura principal de las PC´s y de las redes multi-protocolares. Como resultado de estos cambios, se ha recurrido a la intervención y a la confiabilidad de las redes propietarias, así como de los proveedores de servicio de redes debido a que las aplicaciones comerciales críticas dependen más que nunca de las redes en áreas amplias. En efecto, para muchas compañías actuales una red confiable y siempre disponible, puede significar su éxito en el mercado y en algunos casos su supervivencia.

III.1.3 COSTOS REALES POR LOS DESPERFECTOS DE REDES

Las fallas de las redes y la incapacidad resultante de los usuarios de acceder a las aplicaciones comerciales son siempre irritantes, pero también hay que tener en cuenta la posible pérdida de dinero. No todas las fallas implican una total interrupción de las operaciones, pero incluso un desperfecto limitado puede afectar significativamente una actividad comercial. Los porcentajes de alta disponibilidad pueden también generar grandes agujeros, por ejemplo el 99,9 por ciento de disponibilidad de una red se refleja en más de 8 horas de tiempo inactivo.

La tabla III-1 muestra las cifras de porcentaje de disponibilidad en días, horas, minutos y segundos reales de tiempo inactivo que estas cifras representan. El cuadro comprende las cifras desarrolladas por *The Meta Group*, quien estuvo a cargo del estudio de las cifras de ingresos por hora de varias industrias como forma de

[1] IT: Tecnología de Información (*Information Technology*)

entendimiento del costo del dólar por cualquier falla de las aplicaciones comerciales conectadas por red. La cifra muestra que el costo real por los desperfectos de red guarda poca relación con los cargos al proveedor de servicio de redes por la red WAN, ya que está sujeto a la pérdida de la continuidad comercial y de ingresos (y, por supuesto, a la pérdida de la reputación comercial). En otras palabras, debido a que las aplicaciones comerciales son más críticas para el éxito de una compañía, la confiabilidad de los servicios de red esenciales también se torna crítica.

% DE DISPONIBILIDAD	TIEMPO INACTIVO ANUAL EQUIVALENTE	PERDIDAS ANUALES EXPRESADO EN DOLARES ESTADOUNIDENSES (PROMEDIO INDUSTRIALES FUENTE: THE META GROUP)		
		Energía	***Fabricación***	***Finanzas/Bancos***
99,0	*87 horas, 36 min.*	*$247M*	*$141 M*	*$131 M*
99,5	*43 horas, 48 min.*	*$123 M*	*$70 M*	*$65 M*
99,9	*8 horas, 46 min.*	*$2 M*	*$14 M*	*$13 M*
99,95	*4 horas, 23 min.*	*$13 M*	*$7 M*	*$6.9 M*
99,99	*53min*	*$2.5 M*	*$1.4 M*	*$1.3 M*
99,999	*5 min.*	*$235.000*	*$134.000*	*$125.000*
99,9999	*30 seg.*	*$23.500*	*$13.500*	*$12.500*

Tabla III.1 *Factores de Disponibilidad y Pérdidas Anuales*

III.1.4 PRESENTANDO Y DESCRIBIENDO LOS METODOS DE ALTA DISPONIBILIDAD

Hay dos maneras principales de expresar la disponibilidad de una red: el método del porcentaje y el método de defectos por millón. Los dos métodos usan los términos de MTBF[1] y MTTR[2] para poder ser expresados.

III.1.4.1 MTBF Y MTTR

Para predecir la disponibilidad de un dispositivo en particular, es necesario entender como el MTBF y el MTTR son determinados.

La industria de las telecomunicaciones ha determinado un método estándar para determinar el MTBF, el cual es conocido como Telcordia Método de Conteo de Partes. El método de conteo es descrito en los documentos técnicos Bellcore TR-332 y otro más amplio es el estándar Mil-Hdbk-217, el cual es utilizado por la industria eléctrica.

[1] MTBF *Mean Time Between Failure* (Tiempo Medio Entre Falla)
[2] MTTR *Mean Time to Repair* (Tiempo Medio de Reparación)

Dichos cálculos no serán cubiertos debido a que no están dentro del enfoque de esta tesis, como se vio, solamente se tratarán los aspectos a considerar de estos cálculos.

III.1.4.2 CALCULANDO EL MTBF : MÉTODO TELCORDIA (TR-332)

Cuando contabilizan los dispositivos para determinar el MTBF de una tarjeta con circuitos, esto asume, que si cualquier componente suelto (por ejemplo, circuitos integrado, fusible, capacitor, resistor) falla, entonces la tarjeta con circuitos (dispositivo) fallará. El ambiente en el que los componentes se encuentran, también debe ser considerado. Los siguientes factores deberán ser considerados:

- Temperatura
- Estrés eléctrico
- Calidad
- Ambientación

Bellcore TR-332 hace las recomendaciones de cómo incluir cada uno de estos factores. Asumiendo estas consideraciones dentro del conteo, el proceso de contabilizar el desempeño de los componentes se vuelve más simple.

Para cada componente de una tabla de circuitos, un número FIT[1] es determinado. Un FIT es una falla por diez billones de horas de tiempo en operación. Un dispositivo puede tener un FIT de 3, lo cual significa que en promedio este dispositivo puede tener 3 fallas por diez billones de horas de operación. Este escenario muestra el curso a asumir cuando se reemplace o reparé un dispositivo después de una falla.

Una vez que se tiene el FIT de cada componente de una tabla de circuitos, simplemente sumamos todas, para que nos de el total de FITs, por lo cual el calculo del MTBF es solo un simple calculo aritmético.

Es importante recordar, que la mayoría de las compañías de la industria en telecomunicaciones utilizan el método Bellcore para calcular el MTBF de sus productos. Sin embargo algunas compañías de electrónicos utilizan la especificación Mil-Hdbk-217, la cual también es aceptable.

[1] FIT: Falla en Diez Billones (*Failure In Ten Billion*)

III.1.4.3 CALCULANDO EL MTTR

Existe una variedad de caminos para calcular el MTTR. Para efectos de nuestra tesis, se mostrará una forma muy simple de hacerlo, que es exacto y que satisface nuestro propósito.

Hagamos dos suposiciones:

- El tiempo actual para reemplazar un dispositivo de red con falla en un corto tiempo.
- El tiempo en llegar al lugar adecuado, con la parte correcta a reemplazar, es una parte del tiempo que se consume para arreglar la falla en un dispositivo.

Por ejemplo, si tenemos una disminución que genera una falla en una tarjeta de un ruteador, las cuatro horas que toma reemplazarla es mucho mayor a los cinco minutos que tomaría ejecutar el cambio. Por lo cual, debemos asumir que el MTTR para cada dispositivo en la red es igual al tiempo que toma conseguir el reemplazo de la parte y que el personal especializado llegue para realizar la reparación. Si se tiene un contrato de servicio de reemplazo de partes o reparación de cuatro horas, se puede utilizar las cuatro horas como el MTTR por cada producto cubierto bajo el contrato.

En algunos casos, es prudente considerar un par de horas extras, si se anticipa el hecho de que la reparación puede tomara más tiempo del considerado originalmente. O si se tiene un contrato de garantía o mantenimiento de "próximo día", se puede considerar que hay fallas que se llevarían hasta una semana en ser reparadas.

La predicción del MTTR, frecuentemente es un ejercicio de intuición, ya que queda libre el hecho de agregar o sustraer horas de la base pensada. Si se considera un MTTR de cuatro horas en la disponibilidad de un diseño de red, se deberá considerar el mismo MTTR para un diseño alterno. Naturalmente diferentes dispositivos pueden tener diferentes MTTRs resultantes. Como las cifras de MTBF y MTTR son promedios que incluyen media y varianza.

III.1.5 EL MÉTODO DEL PORCENTAJE

Muchas veces hemos escuchamos el término de cinco nueves en relación a la disponibilidad de una red. Cuando alguien dice esto, realmente está diciendo que el dispositivo o la red es 99.999% disponible. De hecho, 99.999% de disponibilidad es una señal segura de que la persona está usando el método del porcentaje.

El uso esencial del porcentaje de disponibilidad es entender cuánto tiempo va a estar fuera de servicio en un período de un año, y el tiempo de fuera de servicio se determina multiplicando el número de minutos en un año por el porcentaje de disponibilidad. Esto nos da los minutos por año que la red será operacional. El equilibrio es el tiempo fuera de servicio que podemos esperar.

Dado que hay 365 días por año, 24 horas por día, y 60 minutos por hora, nosotros podemos calcular que hay 525,600 minutos por año. Sin embargo, esto no responde a los años que tienen un día extra. La manera que nosotros responderemos a estos años, los cuales pasan cada cuarto año, es agregar un cuarto de día a todos los años. Esto produce 525,960 minutos por año que es el número que se usaran en todos los cálculos para este método.

Además del número de minutos por año, debe entenderse como la *fiabilidad anual*. La fiabilidad anual es el número de veces que hay una falla en el dispositivo cada año. Cuando se conoce el MTBF para un dispositivo, se puede dividir ese MTBF por el número de horas en un año (8766) para predecir el número promedio de fallas por año. Se usarán estos conocimientos cuando predecimos cuantos minutos una red está fuera de servicio mientras se cambia de un dispositivo averiado a un dispositivo activo en una situación redundante.

Y como nosotros sabemos el número de minutos en un año y dado que nosotros entendemos ahora que la disponibilidad es un porcentaje, nosotros podemos ahora calcular el tiempo fuera de servicio durante un año basado en el número de la disponibilidad. La tabla III.2 describe cómo el número de nueves relaciona al tiempo activo y tiempo fuera de servicio.

Como se puede ver, para cada 9 en el porcentaje de disponibilidad, se logra un aumento significante en el funcionamiento de la red. Algo significativo que se dice a menudo y que hay que tomar en cuenta es que después del segundo 9, cada 9 logrado tiene un costo adicional dos veces más caro.

NÚMERO DE NUEVES	PORCENTAJE DE DISPONIBILIDAD	MINUTOS DE TIEMPO ACTIVO POR AÑO (PORCENTAJE 525,960)	MINUTOS FUERA DE SERVICIO POR AÑO (525,960 TIEMPO ACTIVO)	TIEMPO FUERA DE SERVICIO ANUAL
1	*90.000%*	*473,364*	*52,596*	*36.5 días*
2	*99.000%*	*520,700.4*	*5259.6*	*3.5 días*
3	*99.900%*	*525,434.0*	*525.96*	*8.5 horas*
4	*99.990%*	*525,907.4*	*52.596*	*1 hora*
5	*99.999%*	*525,954.7*	*5.2596*	*5 minutos*
6	*99.9999%*	*525,959.5*	*0.52596*	*32 segundos*

Tabla III.2 *Número de 9s: Tiempo activo y tiempo fuera de servicio*

III.1.6 EL MÉTODO DE DEFECTOS POR MILLÓN

La segunda manera de declarar la disponibilidad usa el método de defectos por millón (DPM). Usando este método, nosotros describimos el número de fallas que han ocurrido durante un millón de horas por un dispositivo o una red. Es común usar este método para las grandes redes.

Con el método de DPM, podemos informar problemas de fiabilidad que el método del porcentaje tendría dificultad para encontrarlos. Porque DPM se usa a menudo para las redes existentes, nosotros podemos usarlo para medir los paros de las redes tanto parciales como totales. Nosotros también podemos medir los millones de horas de funcionamiento de la red, las horas de funcionamiento de los dispositivos, o quizás incluso las horas de uso que los usuarios reciben de la red.

III.1.7 MTBF, MTTR, Y DISPONIBILIDAD

MTBF es un número que generalmente se ve en la documentación del producto o en alguna otra especificación para un producto. Este número describe el número de horas entre fracasos para un dispositivo particular. Un término similar es el Tiempo Medio de Falla MTTF[1], y describe la cantidad de tiempo para poner un dispositivo en servicio hasta que el dispositivo falle.

Técnicamente, la ecuación matemática para disponibilidad que nosotros usaremos usará el termino MTTF, según las normas. Por otra parte se podrá casi siempre conseguir el número de MTBF sobre los productos que se desean comprar, ya que es más difícil encontrar los números de MTTF del producto. Técnicamente, es muy probable que las compañías que declaran el MTBF sobre sus productos estén dándole el MTTF y no lo sepa.

Siguiendo esta vigilancia de la industria menor y para simplificar nuestros cálculos, usaremos MTBF en lugar de MTTF y descartar MTTF completamente porque representará una diferencia muy pequeña en nuestros cálculos.

MTTR es la cantidad de tiempo (en promedio) que pasa entre una falla de la red y la restauración de la misma. En la mayoría de los casos, MTTR incluye el pequeño tiempo que se tarda en notar que la red ha fallado. Entonces esto incluye el tiempo para diagnosticar el problema. Finalmente, MTTR incluye el tiempo para realizar la acción apropiada para arreglar la red y una cantidad pequeña de tiempo en las reparaciones para traer a la red a su actividad apropiada. Para un caso ideal el tiempo para descubrir, diagnosticar y reparar un problema de la red se medirá en minutos.

[1] MTTF: Tiempo Medio de Falla (*Mean Time to Failure*)

Sin embargo, a veces las cosas pasan por la noche y nadie lo nota durante horas. A veces el primer diagnóstico es incorrecto y se gastan horas arreglando algo que no está dañado. El punto importante aquí es recordar que hay tres fases a solucionar en un problema de la red:

- La detección
- El diagnóstico
- Las reparaciones

Se puede calcular el porcentaje de disponibilidad directamente si se conoce el MTBF y el MTTR para un dispositivo particular, como el mostrado en la ecuación de disponibilidad en la ecuación III.1.

$$Disponibilidad = \frac{MTBF}{MTBF + MTTR} \qquad \text{III.1}$$

III.1.8 RELACIONANDO EL PORCENTAJE Y MÉTODOS DE DPM

Con el MTBF y el MTTR, es posible convertir entre el porcentaje y los métodos de DPM. Dado que la disponibilidad es un porcentaje y DPM no lo es, necesitamos el MTTR para hacer la conversión del MTBF, esto ayudará porque nosotros lo usamos para llegar al número de disponibilidad en porcentaje.

Para predecir el tiempo fuera de servicio anual que usa el método del DPM, nosotros determinamos la cantidad total de tiempo fuera de servicio sobre un millón de horas y entonces convertimos este al tiempo de fuera de servicio anual.

Para el método del porcentaje, nosotros tomamos simplemente el MTBF proporcionado por el fabricante del producto o productos en cuestión. Entonces nosotros estimamos el MTTR basado en el contrato que nosotros firmamos con el proveedor de la red. De esto nosotros podemos estimar la disponibilidad de la red o dispositivo de la red.

III.1.9 ANALIZANDO EL TIEMPO PERDIDO EN LOS PAROS DE LA RED

Primero se debe saber el tipo y cantidad de dispositivos en la red. Se debe decidir qué se quiere medir. Y para cada vez que la red tenga un paro de cualquier

clase, se debe anotarlo y se categorizarlo. Se necesita recolectar la información siguiente para cada paro:

- El dispositivo (incluyendo modelo, número de serie, versión del hardware, versión del software, etc.).
- La naturaleza del paro (falla completa o el paro parcial).
- El tiempo en el que el paro comenzó.
- El tiempo en que el paro fue reconocido.
- El tiempo en que el paro fue diagnosticado.
- El tiempo en la que la solución fue llevada a cabo.
- El tiempo que la red se restauró totalmente al funcionamiento normal.

De esta información, se puede derivar información estadística suficiente sobre los tiempos y esto nos ayudara en la reducción de tiempo fuera del servicio de la red.

La primera cosa es calcular el DPM contando el número de fallas contra las horas acumuladas de operación. Después, tomamos la distancia promedio de los paros (en horas) para determinar el MTTR para ese tipo de dispositivo en particular. Esto nos da los datos básicos que permiten que comparar el funcionamiento del tiempo activo de la red.

Luego, se comparan los diferentes dispositivos y nos aseguramos que sólo los dispositivos con el mejor funcionamiento serán usados en la red. Si se encuentra que algunos routers tienen un porcentaje de falla más alta que otros routers, entonces posiblemente se debe cambiar a un modelo más fiable.

Otra manera de mejorar la disponibilidad es mejorar los procesos para ocuparse de las fallas de la red. Dentro de un tipo particular de equipo y paro, analice cada uno de los segmentos de tiempo entre el fracaso y la restauración. Lo que se está buscando es el promedio y el rango para cada uno de los segmentos. Si un segmento particular muestra un rango grande, se considera sospechoso. Se compara la restauración rápida (dentro de este segmento de tiempo) con los casos de una restauración lenta para ver por qué estos son tan diferentes. La razón para estas diferencias es obvia.

III.2 MATEMÁTICAS BÁSICAS DE LA ALTA DISPONIBILIDAD

El cálculo de la disponibilidad requiere de las matemáticas. Como la investigación de la disponibilidad aumenta, la dificultad de la matemática utilizada también aumenta y sus ecuaciones se hacen aun más complejas, es por ello que solo aquí

utilizaremos las ecuaciones mas sencillas con el fin de ilustrar algunos ejemplos ya que lo que nos interesa es introducir al concepto de alta disponibilidad, así como interpretar el resultado de estas y no su desarrollo.

III.2.1 DETERMINANDO LA DISPONIBILIDAD DE LOS DISPOSITIVOS QUE COMPONEN LA RED

Para calcular la disponibilidad de una red, se tiene que calcular la disponibilidad de cada uno de los dispositivos que la componen. Y para calcular la disponibilidad de un dispositivo de la red, se tiene que calcular la disponibilidad de sus componentes. El cálculo de la disponibilidad de los componentes de los dispositivos es el punto de partida de la matemática de la disponibilidad.

El Método de Cuenta de Partes se describe en el documento de la Referencia Técnico TR-332, procedimiento de predicción de "Fiabilidad para el Equipo Electrónico de 1997".

El TR-332 describe que el método usado para determinar la fiabilidad de cada componente en un circuito como son los capacitores, resistencias, u otros componentes. Cada componente es asociado con una FIT[1], que representa las fallas por billón de horas. El TR-332 incluye factores con los cuales se puede influir en el número de FITs de un componente particular, basado en la temperatura, ambiente y procesos de control de calidad.

III.2.1.1 ESTIMANDO MTTR DE UNA RED

Como vimos anteriormente el MTTR es otro componente importante de la disponibilidad. Lo que ahora hay que ver es que se puede medir el MTTR de una red existente tomando el tiempo promedio en el que la red está inactiva por cada falla que se presente y el MTTR se puede predecir basándose en una variedad de métodos.

Para nuestros propósitos el MTTR será arbitrario y se supondrá que el número que se use esta basado en el contrato de servicio que se realice con el vendedor. Para nuestras necesidades de ejemplificación usaremos una variedad de valores del M'I'TR con los cuales se pueda entender el impacto a corto y largo de los MTTRs en la disponibilidad de una red.

[1] FIT Failures 10^9

III.2.1.2 La Ecuación de Disponibilidad y Componentes de Dispositivos de Red

Para calcular la disponibilidad, debemos usar la ecuación de disponibilidad. La ecuación de disponibilidad (mostrada de nuevo en ecuación III.2) describe cómo se usa el MTBF y el MTTR para encontrar como resultado un porcentaje:

El porcentaje de tiempo activo del tiempo total

En otras palabras, el porcentaje de disponibilidad es igual a la cantidad de tiempo activo dividido por el tiempo total durante algún período de tiempo *t*. El tempo *t* consistirá tanto por el tiempo activo como el tiempo inactivo de la caja o dispositivo.

$$Disponibilidad = \frac{MTBF}{MTBF + MTTR} \qquad \text{III.2}$$

Como se puede ver, cuando se tiene el MTBF y el MTTR, se puede calcular la disponibilidad con una simple calculadora.

III.2.1.3 La Disponibilidad y Tiempo Activo/Inactivo

Cuando se tiene un porcentaje de disponibilidad, se puede calcular el tiempo activo y el tiempo inactivo. Recíprocamente, si se tiene el tiempo activo o el tiempo inactivo se puede calcular la disponibilidad.

Dado que la disponibilidad es un porcentaje que representa el tiempo activo dividido por el tiempo total, se puede multiplicar cualquier período de tiempo por el número de disponibilidad y obtener la cantidad de tiempo activo de ese período. Claro, la diferencia en el tiempo total y el tiempo activo es el tiempo inactivo.

En la mayoría de los casos, se va a querer obtener el tiempo inactivo por año, entonces lo que hay que hacer es substraer la disponibilidad a la unidad 1 y multiplicar el resultado por el número de minutos en un año.

III.2.2 DETERMINANDO LA DISPONIBILIDAD DE UN SOLO COMPONENTE

Si se quisiera calcular la disponibilidad de un componente en particular, se usa la ecuación de disponibilidad con el MTBF y el MTTR para ese componente. Si el

componente en cuestión tenía un MTBF de 100,000 horas y un MTTR de 6 horas, entonces nosotros podríamos calcular la disponibilidad para ser 0.99994. El tiempo fuera de servicio resultante sería aproximadamente 31.5 minutos por año para ese componente como se muestra en la figura III.1.

$$Disponibilidad = \frac{MTBF}{MTBF + MTTR}$$

MTBF = 100,000 horas

MTTR = 6 horas

$$Disponibilidad = \frac{100{,}000}{100{,}000 + 6} = 0.99994$$

Tiempo fuera de servicio anual = (1 - .99994)*525,960 = 31.5576 minutos

Figura III.1 *Tiempo fuera de servicio de un componente simple*

III.2.3 DETERMINANDO LA DISPONIBILIDAD DE COMPONENTES MÚLTIPLES

Para calcular la disponibilidad de componentes múltiples, se deben entender más ecuaciones: la ecuación de serie y la ecuación de disponibilidad paralela. Una cosa importante para recordar es que los componentes pueden ser los componentes del sistema (como los circuitos) o componentes de la red (como routes o switches).

Se usará la ecuación de disponibilidad serie siempre que todas las partes deban trabajar para el sistema (o red). La ecuación III.3 muestra la ecuación de disponibilidad serie.

$$Disponibilidad.serie = \prod_{i=1}^{n} Componentededisponibilidad_{(i)} \qquad \text{III.3}$$

i representa el componente numérico
n representa el número de componentes

En un sistema serie, si cualquier componente falla entonces el sistema entero falla. Por ejemplo, si un producto consiste en una fuente de poder y un de circuito, se tiene un sistema de serie. Si falla la fuente de poder, entonces el sistema falla, y si un circuito falla, entonces el sistema falla.

A veces los componentes en un sistema están en paralelo, o redundante. Aunque hay diferentes diseños paralelos, la ecuación III.4 muestra la ecuación paralela básica. Esta ecuación se aplica en situaciones en dónde dos dispositivos son paralelos entre sí.

$$Disponibilidad.paralela = 1 - \left[\prod_{i=1}^{n} (1 - componentededisponibilidad_{(i)}) \right] \qquad \text{III.4}$$

i representa el componente numérico
n representa el número de componentes

En un sistema paralelo, se combinan dos o más componentes, tal que el sistema trabajará con tal de que cualquiera de los componentes paralelos todavía este trabajando. Si se tienen dos componentes paralelos y uno de ellos las falla, el sistema continúa (o por lo menos debe continuar) para correr sin falla. La mayoría de los sistemas que también incluyen componentes paralelos incluye componentes serie.

Para calcular la disponibilidad de componentes múltiples, se debe entender las ecuaciones de disponibilidad serie y paralelo.

III.2.3.1 DISPONIBILIDAD SERIE

Para estimar la disponibilidad de un sistema serie, solo es necesario multiplicar la disponibilidad de cada uno de los componentes. Por ejemplo, en el sistema con un solo circuito y una fuente de poder, se multiplica la disponibilidad de la fuente de poder por la disponibilidad del circuito. La figura III.2 muestra estos cálculos.

Suministro de poder = 99.999% disponibilidad = 0.99999
Circuito = 99.994% disponibilidad = 0.99994
Disponibilidad del sistema = 0.99999 * 0.99994 = 0.99993

Figura III.2 *Disponibilidad serie en un sistema de dos componentes*

Como se puede ver, dos componentes con la disponibilidad de 99.999% y 99.994% combinada en una configuración serie proporcionan 99.993% de disponibilidad del sistema total.

Dado que la mayoría de los sistemas contienen más de dos componentes, nosotros necesitamos usar una ecuación que trabaja para algún número (N) de componentes. Donde la ecuación mostrada en la figura III.3 expresa que hay que multiplicar la disponibilidad de cada uno de los componentes juntos, como el sistema de la figura III.2.

$$sistema.de.disponibilidad = \prod_{i=1}^{n} disponibilidad_{(i)}$$

suministro de poder = 99.999%
Circuito 1 = 99.994%
Circuito 2 = 99.98%
Sistema de disponibilidad = .99999*.99994*.9998 = .99973

Figura III.3 *Disponibilidad serie de un sistema de N componentes*

III.2.3.2 DISPONIBILIDAD PARALELA SIMPLE

Para encontrar la disponibilidad paralela simple, se multiplica la indisponibilidad de cada una de las partes paralelas. El resultado de la multiplicación de las indisponibilidades se substrae a la unidad 1 para obtener el resultado de la disponibilidad.

En la figura III.4, se muestra la ecuación para obtenerla disponibilidad en paralelo. Como con la ecuación serie, esta expresa que hay que multiplicar cada "indisponibilidad del componente (I) "por cada otra hasta el N componente de indisponibilidad (I)s" hasta que han sido multiplicadas juntas.

$$Disponibilidad.paralelo = 1 - \left[\prod_{i=1}^{n} (1 - disponibilidad_{(i)}) \right]$$

N – número de componentes en paralelo
i – componente numérico

Figura III.4 *Disponibilidad en un sistema paralelo*

Para clarificar la ecuación, observemos un ejemplo pequeño. Asuma que se tiene un sistema y dentro del sistema hay dos componentes en paralelo. Para simplicidad, nosotros diremos que los dos componentes son idénticos y los dos tienen una disponibilidad de 99.9 por ciento (es decir, 0.999 de disponibilidad). La figura III.5 muestra cómo combinaríamos estos dos componentes para conseguir su disponibilidad paralela.

Componente 1 = 99.9% disponibilidad
Componente 2 = 99.9% disponibilidad

$$disponibilidad.paralela = 1 - \left[\prod_{i=1}^{2} (1 - disponibilidad_{(i)}) \right]$$

= 1- [(1 - .999)*(1 - .999)] = 1 – [1 – 0.000001] = .999999
Porcentaje de disponibilidad = .999999*100 = 99.9999%

Figura III.5 *Disponibilidad Paralela en un sistema de dos componentes*

Es importante que nosotros tomemos nota de un par de cosas sobre la disponibilidad paralela. Primero, los sistemas normalmente diseñados con los componentes paralelos tienen algún método para el cambio del componente fallido al componente restante. Este rasgo se llama mecanismo contra-falla (*fail-over* por sus siglas en inglés). En veces los mecanismos contra-falla también llegan a fallar. Nosotros vamos a excluir esa probabilidad para poder continuar analizando las necesidades de la disponibilidad.

III.2.3.3 N + 1 DISPONIBILIDAD PARALELA

Nosotros hemos discutido cómo calcular la disponibilidad cuando los dispositivos están con arreglos paralelos simples. En otros términos, si nosotros tenemos cualquier número de dispositivos en paralelo, nosotros sabemos calcular la disponibilidad con tal de que cualquier dispositivo permanezca operacional. Este método se lleva a cabo más a menudo en la vida real teniendo dos dispositivos cuando usted necesita sólo un dispositivo.

En el mundo real, nosotros podríamos necesitar más de un dispositivo para mantener una red funcionando. Un ejemplo es donde nosotros necesitamos por lo menos dos fuentes en nuestro router. En esa situación, nosotros podríamos escoger tener una sola fuente de poder auxiliar en lugar de dos fuentes de poder de apoyo. Este método de redundancia se llama, N + la redundancia de M. N representa el número requerido y M representa el número instalado.

El fondo de N + M se da incluyendo el SHARC[1]. Esa herramienta puede calcular N + la redundancia de N para usted. Cuando se encuentran con N + 1, se calcula usando la ecuación III.5.

$$A = nA^{(n-1)} * (1 - A) + A^n \qquad \text{(III.5)}$$

A – disponibilidad total
n – número de dispositivos

NOTA: Nosotros asumimos una disponibilidad es igual para cada componente.

III.2.3.4 DISPONIBILIDAD SERIE/PARALELO

La mayoría de los sistemas (y redes) contienen tanto componentes en serie como paralelo. El método que para calcular la disponibilidad serie/paralelo simplemente involucra dos pasos:

[1] SHARC Sistema de Hardware y Calculadora Confiable *(Sistem Hardware and Reability Calculador)*

Paso 1 Se calcula la disponibilidad paralela para todos los componentes paralelos.

Paso 2 Se combina los resultados del paso 1, junto con todos los componentes serie, usando el método de disponibilidad serie.

Para realizar estos cálculos, se necesita un poco de conocimiento sobre el sistema o red. Se debe entender el camino a través del cual los datos viajarán (topología de red), así como entender qué componentes son críticos o redundantes. La disponibilidad de un sistema o una red depende de la disponibilidad del camino entre los puntos A y B por donde los datos deben circular.

Ya con la ecuación paralela y la ecuación serie, construiremos las ecuaciones serie/paralelo y el proceso.

III.2.4 DETERMINANDO EL FLUJO DE DATOS EN UNA RED: ANÁLISIS DEL CAMINO

La situación más común que ocurrirá en los estudios de disponibilidad será la combinación de componentes serie y paralelos en un sistema grande. Además, no todos los componentes serán requeridos para el flujo de datos en el escenario que estemos interesados. Muchos dispositivos de red conectan un gran número de redes juntas. Si se esta considerando la disponibilidad de sólo las primeras dos redes que el dispositivo une, entonces no estamos considerando algún otro componente fallido que lleva el tráfico a la tercera red.

Esta consideración de flujo de datos es llamada análisis del camino. El análisis del camino hace posible usar las mismas ecuaciones que nosotros hemos estado usando por calcular la disponibilidad de un sistema, para calcular la disponibilidad de una red. En los cálculos de disponibilidad de red, nosotros usamos los dispositivos de la red, como los routers y switches. En los cálculos de la red, nosotros podríamos usar el análisis del camino para determinar el camino de los datos a través de un router y usar esos componentes para analizar la disponibilidad. Una vez que ese cálculo está completo, nosotros usaríamos el resultado como un componente en un análisis de la red.

III.2.4.1 USANDO LA CONFIABILIDAD DE LOS DIAGRAMAS DE BLOQUE PARA EL ANÁLISIS DE CAMINO

Para realizar un análisis del camino, es una buena idea crear un diagrama de bloque de disponibilidad.

Por ahora, nosotros consideraremos un ejemplo muy simple de una red, usando un gran router con componentes que no son importantes para nuestros cálculos. Nosotros necesitamos eliminar aquéllos cálculos y realizar el análisis de disponibilidad para algo que nosotros cuidamos. En la figura III.6, un dispositivo de la red se conecta a tres redes. Nosotros sólo queremos saber la disponibilidad de la red 1 a la red 2. Por consiguiente, el hardware que apoya la conexión para Conectar una red de computadoras 3 puede eliminarse de nuestros cálculos.

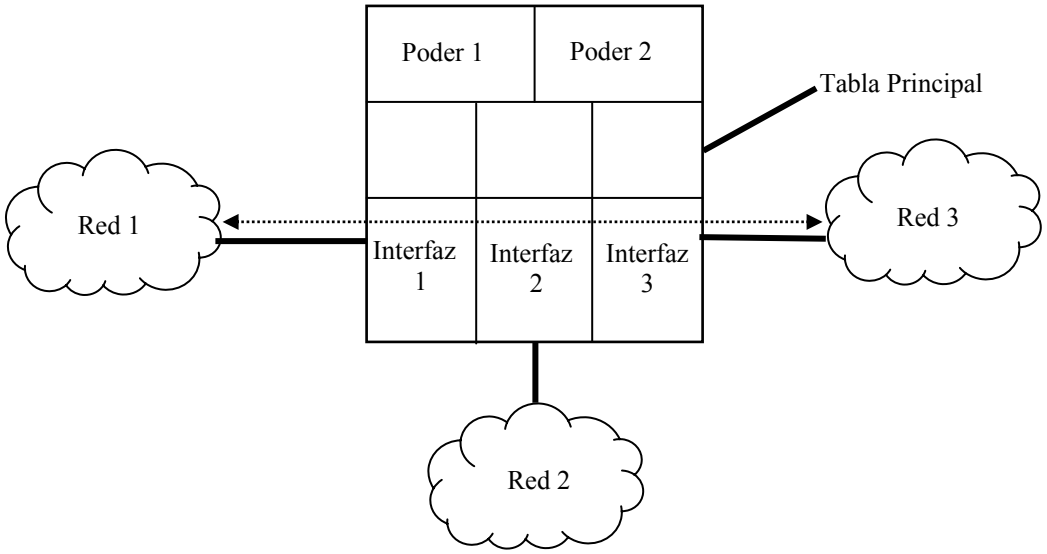


Figura III.6 *Analizando el camino de la Red 1 a la Red 2*

Como se puede ver en la figura III.6, nuestro dispositivo incluye dos fuentes de poder redundantes fuente de poder 1 y fuente de poder 2. Varios pasos están envueltos en calcular la disponibilidad de un dispositivo (o red) qué tiene componentes serie y paralelo.

En este caso nuestros pasos son:

Paso 1 Determine la disponibilidad de cada componente
Paso 2 Calcular la disponibilidad de la fuente de poder dual
Paso 3 Multiplicar la disponibilidad de todos los componentes con el resultado del paso 2

La figura III.7 muestra el análisis de disponibilidad de la red 1 con la red 2.

Suministro de poder = 99.9%
Tarjeta madre = 99.994%
Tarjetas de interfaz = 99.95%

Paso 1: Cálculos paralelo

Poder = 1 - [(1 - .999)*(1 - .999)] = .999999

Paso 2: Cálculos serie

Poder = .999999
Tarjeta madre = .99994
Interfaz 1 = .9995
Interfaz 2 = .9995

Disponibilidad del sistema = .999999*.99994*.9995*.9995
= .998939
= 99.8939%

Figura III.7 *Análisis del camino: Disponibilidad de la red 1 a la red 2*

Usamos 99.9 por ciento para la fuente de poder, 99.994 por ciento para la tarjeta madre, y 99.95 por ciento para cada una de las interfaces. Después de que todos los cálculos fueron completados, el resultado de 99.8939 por ciento describe la disponibilidad de la red 1 a la red 2 vía el dispositivo mostrado en el diagrama. Nota que la interfaz 3 no esta incluida en los cálculos porque no era un componente requerido. De los 525,960 minutos usados por año y nuestro método normal para el cálculo, nosotros tenemos aproximadamente 9.3 horas por año de tiempo fuera de servicio. Incluso con las fuentes de poder redundantes, este sistema causaría una cantidad considerable de tiempo fuera de servicio en una red.

III.3 TOPOLOGÍAS FUNDAMENTALES DE RED

Las topologías paralelas proporcionan alta disponibilidad porque aun cuando los dispositivos de la red fallan, la red todavía funciona. Las topologías serie reducen la disponibilidad en comparación con las topologías en paralelo porque la entrada de la red depende de que todos los dispositivos trabajen. Una red simple aumenta su disponibilidad mientras al mismo tiempo limitan tu habilidad de hacer todas las partes al mismo tiempo paralelas.

Debido a este equilibrio complejo entre la simplicidad y redundancia, el plan de la red es casi un arte. Toda la matemática en el mundo mostrará que la solución paralela es más fiable. Sin embargo, si los mecanismos de contra falla fallan debido a algún bicho de software, el diseño paralelo creado para más cosas fallara.

Aunque la topología puede ser un gran tema, la construcción básica de los bloques de una red son topologías serie, paralelo y topologías serie/paralelo.

Limitando nuestros estudios a estas tres topologías nos permitirá que enfoquemos en nuestra meta importante de aprender a predecir la disponibilidad.

III.3.1 TOPOLOGÍA SERIE

Cada dispositivo en una topología serie toma algunos datos de una dirección y los mueve a otro lugar. Aunque topologías serie a menudo ejecutan protocolos de ruteo o switcheo, estos normalmente no son usados para ayudar a la red cuando falla algún dispositivo de red. En una topología serie, los protocolos de switcheo o ruteo se ejecutan para segmentar el trafico de la red y aseguran que los bits correctos vayan a los nodos correctos.

La figura III.8 muestra unos dispositivos de red colocados en una topología serie. Si alguno de estos dispositivos falla, un paro mayor en la red ocurriría. Adicionalmente, los dispositivos están ejecutando un protocolo de ruteo para asegurar que el tráfico vaya al lugar correcto. Aunque un protocolo de ruteo este corriendo, una falla no producirá que otro router tome el tráfico del router que fallo.

En la figura III.8 se puede ver que cualquier dato que viaje entre el segmento de ruteo A y cualquier otro lugar en la red viajaría en exactamente por un camino. Nótese que los segmentos de ruteo en el diagrama son segmentos IP (Capa de 3 segmentos) y así, el switch no divide el segmento de ruteo en partes. Llamaremos estos segmentos de ruteo solamente segmentos.

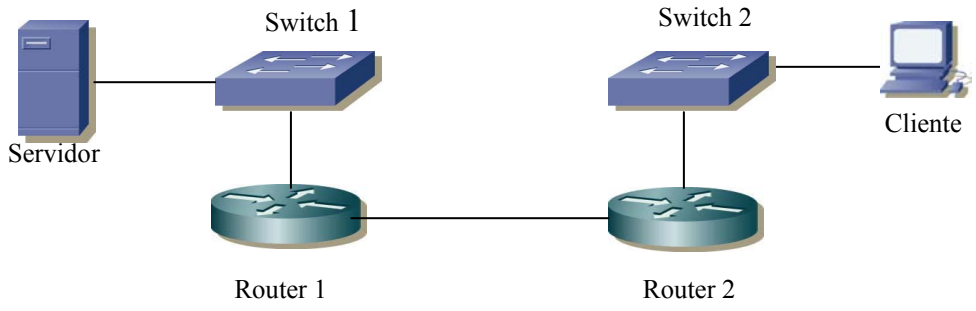


Figura III.8 *Topología serie simple*

III.3.2 TOPOLOGÍA PARALELA

Al contrario de en la topología serie, el mecanismo de contra falla es crucial en el funcionamiento de una topología paralela. Si el mecanismo de contra falla es un

protocolo de puenteo, protocolo de ruteo, o algún otro método, se necesitaría considerarlo cuidadosamente mientras se realizan los cálculos de disponibilidad. Después, vamos a asumir que los mecanismos de contra falla toman una cierta cantidad de tiempo y entonces nosotros vamos a agregar ese tiempo a nuestros cálculos.

Para ilustrar la topología paralela y su disponibilidad asociada, nosotros usaremos la figura III.9 la cual muestra una red de topología paralela muy simple.

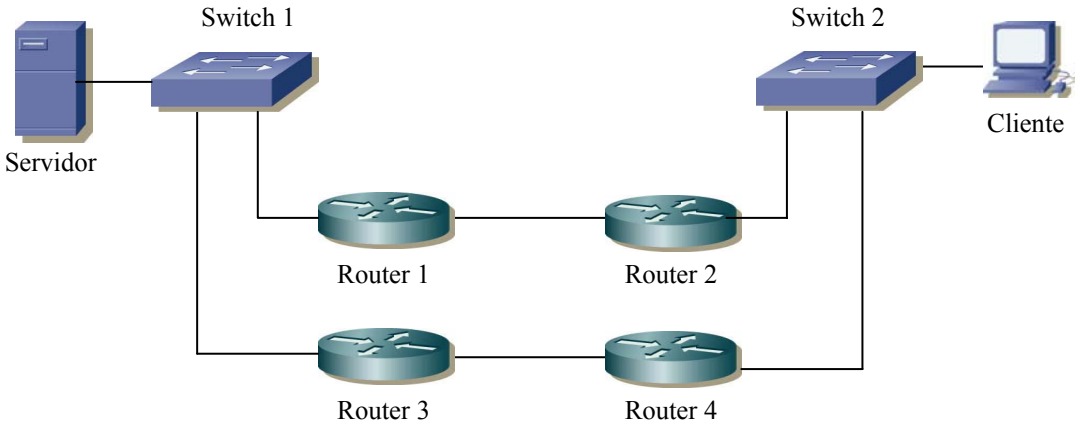


Figura III.9 *Topología de red paralela simple*

III.3.3 TOPOLOGÍA SERIE/PARALELO

Como se puede haber notado en la figura III.9, crear una red con toda una topología serie o una topología paralela es improbable. Incluso en las redes más redundantes por los proveedores de servicio grandes, la última milla es raramente redundante. Para calcular la disponibilidad de estas redes, se necesita combinar la disponibilidad resultante serie y ponerla en ecuaciones paralelas, y también se necesitará combinar los resultados paralelos y ponerlos en ecuaciones serie.

En orden para realizar los cálculos serie/paralelo y terminar los cálculos punto a punto, se realizaran los pasos siguientes:

Paso 1 Se calcula la disponibilidad para cada componente de la red.
Paso 2 Se calcula la disponibilidad de componentes paralelos que serán incluidos en los cálculos de fin a fin serie.
Paso 3 Se calcula las ecuaciones serie punto a punto.

III.4 PREDICIENDO LA DISPONIBILIDAD

La confiabilidad y la disponibilidad son términos que por lo general son utilizados (incorrectamente) de manera intercambiable. La confiabilidad se basa en la habilidad de un dispositivo o de un sistema de operar sin ninguna falla. (Esta falla se mide generalmente mediante el intervalo promedio entre fallas, o el tiempo promedio entre fallas "MTBF"). Estadísticamente, el 63 por ciento de los productos fallan, al menos, una vez durante el MTBF.

Debido a que algunos tipos de fallas probablemente ocurran en algún punto determinado, la velocidad a la que dicho servicio puede restaurarse también afecta. Ante un desperfecto, el proveedor de servicio de redes o el encargado de dicha red, debe diagnosticar, separar, remover y cambiar la pieza afectada, y luego restaurar la funcionalidad al sistema o a la red. De este modo, el segundo parámetro importante de disponibilidad es el tiempo promedio para reparar o "MTRR".

Por ejemplo, supongamos que se cuenta con un equipo con un MTBF de 45.000 horas y un MTTR esperado de 4 horas cuando ocurre un desperfecto. El tiempo inactivo para el equipo será entonces de 4 horas cada 45.000 horas. La disponibilidad puede ser calculada como MTBF / (MTBF + MTTR) ó, 45.000/45004 = 99,991 por ciento.

La tabla III.3 muestra el impacto de cambiar un MTTR en dos casos de MTBF diferentes. Telecordia (antes denominada Bellcore) asume un MTTR de dos horas para el equipo ubicado en la casa matriz, y de 24 horas para el equipo ubicado en una de las oficinas del cliente ó abonado (es decir, equipo en las instalaciones del cliente o CPE[1]).

MTBF (HORAS)	MTTR (HORAS)	DISPONIBILIDAD = MTBF / (MTBF + MTTR)
45.000	2	99,996%
45.000	8	99,982%
45.000	24	99,947%
90.000	2	99,998%
90.000	8	99,991%
90.000	24	99,973%

Tabla III.3 *Efecto de un MTTR en Términos de Disponibilidad*

[1] CPE: Equipo Terminal de Abonado (*Customer Premises Equipment*)

III.4.1 FACTORES QUE AFECTAN LA DISPONIBILIDAD

Muchos conceptos erróneos existen respecto a que se necesita considerar, cuando se diseña una red de alta disponibilidad. Muchos diseños de redes consideran únicamente la disponibilidad del hardware. Es difícil recordar que el software también puede ser causante de fallas en la red, aun cuando el producto claramente especifica el estado de predicción MTBF para dicho producto, pero omite completamente cualquier referencia de la disponibilidad del software. Lo anterior dificulta una buena propuesta documentada para una instalación, mantenimiento y actualización de una red sin que tenga un efecto criticó sobre la disponibilidad de la red.

La filosofía comercial y las acciones específicas de los proveedores de servicio de redes pueden influenciar en gran medida en ambos parámetros (MTBF y MTTR) y la manera en que el servicio al cliente se ve afectado. Esto se lleva a cabo mediante la toma de decisiones y de acciones en cinco áreas principales:

1. Diseño de red y de instalaciones (consideraciones ambientales)
2. Políticas de suministro de servicios
3. Elección de elementos de red (hardware y software)
4. Instalación y configuración de red
5. Operaciones, mantenimiento de red y errores humanos

Sino se consideran cada uno de estos factores la estimación que se haga en el diseño será menos precisas de cómo se quisiera.

La contribución del hardware en fallas de la red, es el factor más sencillo de controlar porque cualquiera que considere la disponibilidad de la red tendrá que considerar las fallas del hardware. Este es el mayor contribuyente comúnmente calculado para una red fuera de servicio y es el más fácil de predecir.

Cualquiera que piense en el diseño de una red de alta disponibilidad sabe que el software siempre incluye defectos del sistema (*bugs*). Asumiendo que el resultado de lo anterior, lógicamente son algunas fallas en la red, derivando en tiempo fuera de servicio. La parte difícil de estimar la disposición del software, es determinando cuales actualmente constituyen una deficiencia en la red y cuáles no.

Fallas catastróficas ocurren por ejemplo cuando un ruteador deja de trabajar inesperadamente como resultado de un problema de software y tiene que ser reiniciado para que vuelva a operar. Este tipo de fallas son más notables en una red, porque cuando ocurren en las estaciones de administración de la red se alarman los equipos hasta que se vuelve a restablecer el equipo. También este tipo de fallas

causan que todo el tráfico a través de ruteador se detenga; mientras que una falla parcial solamente provocaría que se detuviera el tráfico de una parte particular.

Fallas parciales son más fáciles de manejar y detectar que las fallas catastróficas. Algunas veces una falla en el sistema del software puede causar ciertos tipos de fallas de datos o alentar el tráfico. Usuarios pueden pensar que la red está congestionada pese a que solamente algunos usuarios están utilizando la red. Esto puede traducirse en pérdidas de productividad.

Interrupciones en el servicio son otro tipo de fallas de software. Es posible que una red pueda continuar funcionando a toda velocidad con respecto a la cantidad de datos, pero algunos procesos de control tales como características de seguridad, fallen. Puede provocar que parezca que la red trabaja adecuadamente, pero al haber un corte del servicio, este no se registrará en el momento de una falla imposibilitando saber donde, cuando y por quien ocurrió la falla. Una vez fuera el servicio, se vuelve incapaz de reestablecer la red en forma aparente, lo que puede transformarse en disturbios en la red e incluso ponerla fuera de servicio.

El diseño de redes incluye la selección de topología y protocolos. En el diseño de una red, se puede considerar varios protocolos ruteados y protocolos de respaldo en espera (*hot standby*), que afectarán directamente la disponibilidad de la red y con esto se elegirá la opción más adecuada.

Es de esperarse que la topología de red sea un factor crucial para las consideraciones de diseño que afectan directamente la disponibilidad en una red. Por otro lado al referirnos a cerca de formas en que el ambiente puede infringir descontrol en una red, las posibilidades son infinitas. Podríamos considerar terremotos, inundaciones, actividad volcánica, así como un montón de cosas. Además, podemos considerar cosas más simples como temperatura y humedad. Para no perder el enfoque con las consideraciones ambientales simplemente nos enfocaremos en la perdida de las fuentes de poder de los dispositivos.

Por que la pérdida de energía puede ser planeada, y así podemos discutir métodos que incrementen la disponibilidad, implementando soluciones de respaldo, tales como baterías de respaldo ó generadores de energía.

Sin embargo la disponibilidad de una red también esta ligada directamente a los errores humanos, que son un factor muy importante a considerar cuando se requiere una red de alta disponibilidad, de hecho los errores humanos son a menudo la causa principal de poner las redes grandes, fuera de servicio.

Cada uno de estos temas será tratado con mayor profundidad a continuación.

III.4.2 COMO DISEÑAR UNA RED CONFIABLE

El primer principio para diseñar una red confiable es esperar lo inesperado. En otras palabras, se debe anticipar cualquier modo de falla posible y establecer las características de diseño ya sea para eliminar o para minimizar el efecto de cualquier falla. ¿Qué debe anticiparse? Las fallas de hardware, los problemas de software (especialmente aquellos relacionados con la instalación de nuevas versiones), las interrupciones de energía u otros problemas del entorno, los desperfectos en las instalaciones (por ejemplo: la retroexcavadora mediante el cable óptico), las cargas de tráfico inesperadas o congestión, los cambios de configuración accidentales u otros errores operativos, así como también ataques deliberados por parte de los *"hackers"*; todo esto debe tenerse en cuenta.

Los tres principios esenciales relacionados con un diseño de red de alta confiabilidad son: el aumento de la modularidad (y de este modo, la redundancia), la reducción de la complejidad (este tema será tratado en profundidad más adelante) y la obtención de consistencia (en procedimientos de operación, etc.).

III.4.2.1 MECANISMOS DE FAIL-OVER EN EL DISEÑO DE RED.

Una de las consideraciones que son importantes de tomar en cuenta dentro de las causas de tiempo inactivo de la red son los mecanismos *fail-over* (mecanismos contra falla).

Los protocolos de ruteo, protocolos de *hot standby*, protocolos de puenteo son ejemplos de mecanismo de *fail-over*. Nosotros debemos pensar sobre dos consideraciones cuando predecimos la disponibilidad en un diseño de una red o un segmento en particular en el cual se tienen mecanismos de *fail-over*. En primero, debemos anotar los tiempos que toma en reaccionar los mecanismos de *fail-over*. Segundo, debemos anotar la posibilidad de que estos mecanismos de *fail-over* fallen. Nosotros asumiremos que los mecanismos de *fail-over* funcionen y tomaremos el tiempo que le toma al mecanismo de *fail-over* reaccionar y asociar el tiempo de inactividad.

Para nuestro nivel de propuestas introductorias, no veremos con detalle los diferentes mecanismos de contra falla. Sin embargo, una daremos una pequeña descripción apropiada. Consecuentemente comenzaremos esta sección con una rápida discusión en los dos mayores grupos de mecanismos de contra falla: los *load sharing y standby* (los de balanceo o suplente).

III.4.2.2 REDUNDANCIA CON BALANCEO DE CARGAS (LOAD SHARING)

La característica importante de la redundancia con balanceo de cargas "*sharing*" es que dos o más sistemas tendrán constantemente carga no mayor al 50 % de la carga total. Si uno de los dispositivos llega a fallar el dispositivo o dispositivos restantes deben ser capaces de levantar la carga con una pequeña o sin interrupción de los servicios. Los productos más comunes de compartir carga y que vemos en la industria de las redes son las fuentes de poder. Casi todo producto redundancia de fuentes de poder trabaja con unos mecanismos de comparición de cargas. Si un gran router requiere de 100 watts de potencia, muy probablemente habrá dos fuentes de poder capaces de suministrar 110 watts de potencia al router. En una normal operación cada una de las fuentes trabajaría al 45 por ciento de su capacidad total. En caso de alguna falla, la fuente que sobre debe de ser capaz de continuar proveyendo energía al sistema completo. La fuente dañada puede ser remplazada en cualquier momento conveniente.

III.4.2.3 REDUNDANCIA POR DISPOSITIVOS SUPLENTES

La característica principal de los mecanismos de *fail-over* por redundancia o suplente, es que al menos un dispositivo estará esperando que el dispositivo primario falle. Una vez que el dispositivo primario falle, el suplente o el aparato de respaldo, toma las funciones del dispositivo primario. Los dispositivos que están mas comúnmente conectados en esta configuración son los routers, los cuales el router de respaldo esta monitoreando al primer router, en caso de alguna falla en el router primario el router de respaldo comienza a pasar el tráfico en unos cuantos segundos.

III.4.3 HARDWARE

El hecho de evitar una "simple falla" constituye un objetivo importante-deberían existir pocas instancias en donde ocurre una sola falla de cualquiera de estos elementos-routers, switches, servidores, máquinas intermedias, etc., y vías que conecten todos estos elementos. Los servidores deberían ser bidireccionales (*dual homed*) hacia switches Ethernet múltiples. Los puntos de presencia (POPs[1]) deberían ser bidireccionales hacia centros de datos múltiples, o mejor aún, deberían estar conectados a todos los centros de datos de los proveedores de servicio de redes a través de una red mallada.

[1] POP : Punto de acceso a Internet (*Point of Present*)

Otro factor a tener en cuenta es si se debe especificar el equipo con módulos redundantes o si se debe especificar la redundancia en el nivel de la base (o ambos). El primer enfoque puede permitir intercambios de tarjetas en servicio más fáciles o mejoras pero, por otro lado, puede prolongar los tiempos de falla. Asimismo, el hecho de garantizar que el módulo "disponible" está operando de manera adecuada puede algunas veces, convertirse en un problema (por ejemplo: las rutinas de diagnóstico subordinado de software ¿operan constantemente en un módulo disponible?). Por otro lado, la redundancia del nivel-base puede evitar los asuntos de espera activa, pero con esta comunicación de falla de diseño se debe realizar a través de un protocolo, y de este modo la coordinación de mejoras puede resultar más compleja.

Además, se debería considerar la asignación de ruta física de las conexiones de *carriers*[1]. El hecho de contar con dos cables, ambos ruteados mediante el mismo conducto, no necesita una mayor protección contra cualquier daño físico.

III.4.4 EVENTOS DINÁMICOS

Una vez distribuidos los elementos de red con la redundancia adecuada, se debe tener en cuenta aquellos eventos dinámicos que puedan dar alcance al diseño de red inicial. El balance de carga de los servidores constituye un ejemplo evidente y los switches con "conocimiento de contenido" (es decir, entienden las aplicaciones en uso así como también los parámetros específicos del usuario, tales como sesiones y *cookies*) operan bajo mejores condiciones que un switch ethernet convencional. Estas capacidades permiten una degradación importante del desempeño de la red en vez de un colapso rápido, en aquellos casos en que las cargas de tráfico exceden los niveles esperados o recorren la red en direcciones inesperadas.

Además del equilibrio de carga entre servidores, los mejores proveedores de servicio de redes poseen a menudo varios servidores extras en su "*server farm*[2]" y brindan la posibilidad de que los sistemas de balanceo de carga repitan automáticamente el "*hot content*[3]" en ellos. En efecto, esta situación aumenta provisionalmente el número de servidores que manejan una serie de datos particulares. Un ejemplo sería un aumento repentino de tráfico a un sitio en la Web sobre noticias, seguido por la colisión aérea o por cualquier otra catástrofe significativa. Este tipo de aumento inesperado de tráfico se conoce algunas veces como el fenómeno "*flash crowd*[4]", debido a que no sólo se trata de un pico de tráfico inesperado sino que se desarrolla muy rápidamente.

[1] carrier : Empresa portadora de datos a nivel WAN generalmente son las mismas empresas de telefonía local
[2] Server Farm : Granja de Servidores
[3] Hot Content : Contenido Frecuente
[4] Flash Crowd : Crecimiento Masivo

III.4.5 INSTALACIONES

En cuanto al aspecto de diseño de las instalaciones, un proveedor de servicio de redes indica su postura de confiabilidad mediante el tipo de centro de datos que construye y opera. Los puntos más importantes a evaluar se encuentran resumidos a continuación:

- Buscar alimentaciones de energía múltiples para el edificio, un Sistema de Suministro de Energía Ininterrumpible (UPS[1]) con un tamaño adecuado y una serie de generadores, así como también aire acondicionado con capacidad para un centro totalmente desarrollado.

- Preguntar acerca de los sistemas de detección y extinción de incendios, detección de agua bajo pisos elevados y arrostramiento físico para terremotos, tornados, etc.

- Tener en cuenta qué tan fácil resulta para las visitas ingresar al edificio, qué documentos de identidad se requieren, si las visitas deben ser acompañadas, qué registros se archivan y qué tipo de sistemas de vigilancia por vídeo existe en el lugar.

Por lo general, se supone que las interrupciones del servicio de energía constituyen la causa principal de las fallas de red. Aunque una pérdida de energía puede apagar completamente una computadora o una red. Recientemente una empresa líder en el mercado de las telecomunicaciones descubrió a través de un estudio reciente que las interrupciones del servicio de energía implican un porcentaje menor al 2% del tiempo inactivo en una red típica. La importancia de un sistema UPS adecuado puede observarse en la tabla III.4, que ilustra los cortes de energía sin el sistema antes mencionado y la posible mejora con las diferentes cantidades de capacidad de reserva de batería.

	SIN UPS	SOLO UPS; BATERIAS DE 5 MINUTOS	SOLO UPS; BATERIAS DE 1 HORA	UPS CON BATERIAS DE 1 HORA MÁS GENERADOR DE RESERVA
Casos Anuales de Cortes de Energía	15	1	0,15	0,01
Tiempo de interrupción del Servicio Anual (minutos)	189	109	10	1
Disponibilidad de Energía	99,96%	99,979%	99,996%	99,9998%

Fuente: American Power Convension Company, Nota Técnica N°26

Tabla III.4 *Efecto del UPS sobre los cortes de energía.*

[1] UPS: Sistema de Alimentación Ininterrumpida (*Uninterruptable Power Supply*)

El aire acondicionado con capacidad suficiente para un centro de datos también constituye un elemento crítico. La mayoría de los equipos de comunicaciones de datos son diseñados para operar normalmente a temperaturas de hasta 40ºC (104ºF), pero a temperaturas superiores, las fallas de hardware aumentan en un factor de 1,7 a 2,2 por cada aumento de 10ºC.

III.4.6 EN EL DISEÑO DE RED, SIMPLE SIGNIFICA CONFIABLE

El hecho de reducir la complejidad de la red tal vez, inesperadamente, pueda constituir otra forma para que el proveedor de servicio de redes pueda lograr una mayor disponibilidad de redes. Minimizar el número de los diferentes distribuidores que suministran equipos a la red constituye un enfoque efectivo a todo esto, ya que cuanto más abastecedores existan, el entorno IT se va a tornar más complejo.

Los abastecedores múltiples comprometen la disponibilidad del servicio en dos formas. En primer lugar, cuanto mayor cantidad de diferentes marcas conozca el personal de operaciones del proveedor de servicio de redes, es probable que se cometa una mayor cantidad de errores- es difícil ser un experto en todo. Y en aquellos casos en que ocurre alguna falla, por lo general, lleva más tiempo identificar el problema, repararlo y restaurar el servicio al cliente.

Gracias a las pautas industriales, los componentes de redes de prácticamente todos los distribuidores pueden diseñarse, con un poco de esfuerzo, para que operen de manera conjunta. Pero la ventaja de todo esto, y la posibilidad de mantener una red operando de punta a punta, es una cuestión diferente: Los centros de datos que poseen una multitud de equipos de diferentes distribuidores, por lo general, tienen que enfrentar el dilema conocido como creador de conflictos de personal "*Balkanization of staff*". Por ejemplo: lo que Juan sabe acerca de este equipo, no lo sabe acerca del otro. En cambio, Alfredo es un experto en este otro equipo y María es la única que puede configurar el "nuevo equipo".

Evidentemente, este escenario no resulta nada eficiente pero, peor aún, conduce a errores frecuentes (cuando "Juan tiene que trabajar con el equipo de María") así como también a demoras (debido a que el hecho de resolver los numerosos problemas relacionados con la red requiere como mínimo a dos técnicos, quienes se van a demorar ya que van a necesitar "traducir" la terminología, etc. desde el marco de referencia de un distribuidor hasta el marco de referencia de otro distribuidor).

En una encuesta reciente realizada por los lectores de la revista *Information Week*, se tuvo conocimiento de que más del 90 por ciento de aquellas personas encuestadas creían que esa complejidad de IT y de red conducía a una gestión más

difícil y constituía una pérdida de tiempo, era más costosa y estresante. El mismo porcentaje de encuestados coincidió que el hecho de simplificar cualquier aspecto de IT genera mayores beneficios comerciales. La tabla III.5 muestra las diferentes causas que informaron los encuestados acerca de los problemas de IT y de red como consecuencia de la complejidad.

PROBLEMAS EMERGENTES POR COMPLEJIDAD	PORCENTAJE
Contratación de Personal Adecuado	*84%*
Personal Debidamente Capacitado	*74%*
Comunicaciones Intra-empresariales	*68%*
Mejoras Permanentes	*67%*
Puntualidad del Proyecto	*61%*
Gestión de Costos del Proyecto	*56%*
Seguridad de Red/Datos Adecuada	*55%*
Expansión a Nuevos Mercados	*37%*

Tabla III.5 *Impactos de la complejidad*

III.4.7 VERIFICACIÓN DEL PRODUCTO

La verificación del producto también constituye un elemento importante. A tal fin, se utilizan instalaciones enteras para certificar el cumplimiento de *Telecordia Network Equipment Building Systems* (NEBS) así como también de otras pautas similares, incluyendo las tablas de vibración (para la resistencia de terremotos y de "*fell-off-the-truck*[1]"), cámaras de temperatura y de humedad, pruebas contra incendios y cámaras sordas de gran tamaño (para probar las interferencias y las emisiones electrónicas).

En cuanto al software, alcanzar una mayor confiabilidad genera la prevención de fallas, la retención de fallas, la detección de errores y la recuperación de errores. Llevar a cabo una verificación extensiva constituye el enfoque principal para la prevención de las fallas en software, teniendo en cuenta las situaciones que pueden ocurrir, tales como la escasez de memoria u otras mermas de recursos. La retención de fallas significa retener los efectos de cualquier falla en el menor número posible de componentes. El hecho de evitar el uso de espacio de memoria compartida, de dividir el software complejo en numerosos procesos independientes y de inspeccionar y de restringir cuidadosamente cualquier llamada de interfase de programación de aplicación (API[2]) constituyen técnicas comúnmente usadas.

[1] Fell off the Truck : Vibraciones de camiones
[2] API: Interfase de Programación de Aplicación (*Application Program Interface*): Especificación de convenciones de llamadas de función que define una interfaz a un servicio.

El punto de control permite que un componente de software almacene una copia consistente de su estado interno en una memoria temporal de manera que pueda ser leída al reinicio luego de una caída del proceso de software. Este tipo de función también puede ser utilizado para sincronizar el estado interno entre los procesos de software redundantes principales y de *backup*. El punto de control se puede realizar en modo inmediato (el proceso que requiere el punto de control queda suspendido hasta que se complete la operación de punto de control) o en modo demorado (en aquellos casos donde el proceso subordinado independiente maneja la operación del punto de control sin suspender el proceso de llamada). Los datos del punto de control pueden ser almacenados en la misma tarjeta donde se realiza el proceso de llamada (el enfoque más rápido) o en una tarjeta diferente (lo cual facilita la inserción en línea y la remoción de tarjetas).

III.4.8 RECUPERACIÓN DE ERRORES

Un error debe ser detectado antes del inicio de la recuperación, lo cual puede suceder de varias maneras. Un agente de detección de fallas puede ser utilizado para controlar los valores principales de operación o de desempeño, tal como la memoria libre. Los gerentes del sistema pueden detectar la finalización anormal de un proceso, o los cronómetros vigilantes (*watchdog*) pueden agotarse sin ser reiniciados, haciendo de este modo que el proceso se termine o que se inicie el reiniciado del hardware de la máquina. Los cronómetros vigilantes también tienen la función de proteger los circuitos infinitos, los cierres inactivos de software o los problemas de prioridad que podrían resultar difíciles de detectar utilizando otros medios. Los cronómetros vigilantes pueden ser implementados en hardware, en software o en ambos.

La recuperación de errores incluye las acciones tomadas luego de haber detectado el error a fin de minimizar la interrupción de la operación de todo el sistema. El diseño para minimizar el tiempo requerido para poder cambiar de hardware, reiniciar una tarjeta, reconstruir un nodo o resincronizar dos series de software, resulta una tarea crítica así como lo son los numerosos enfoques para evitar la corrupción de la base de datos. Otro ejemplo sería diseñar un sistema de manera que si una simple tarjeta de líneas comienza a fallar, pueda recargarse únicamente el software para esa línea y no todo el sistema.

El *Hot Standby Router Protocol* (HSRP) constituye otro ejemplo de software con una mayor confiabilidad y opera a un mayor nivel. El protocolo HSRP hace que una serie de routers trabajen en forma conjunta para presentar la apariencia de un router o gateway virtual simple hacia una serie de unidades centrales IP. Al compartir una dirección IP (así como también una dirección de Control de Acceso de Medios [MAC]), dos (o más) routers, actuando como un router virtual simple,

son capaces de continuar en forma ininterrumpida las funciones de ruteo en caso de una falla del router, una interrupción del servicio de energía, un mantenimiento programado u otras razones. Esta situación permite a las unidades centrales de una red continuar emitiendo paquetes IP hacia una dirección MAC e IP consistente, además de causar la conversión de dispositivos haciendo que el ruteo hacia ellos y sus sesiones sea transparente.

III.4.9 INSTALACIÓN Y CONFIGURACIÓN DE UNA RED CONFIABLE

Aún con el equipo bien diseñado e instalado en la red de un proveedor de servicio, pueden aparecer problemas. Por ejemplo, todas las opciones y las variables de software deben instalarse correctamente. La configuración de un equipo de operación en red con tecnología moderna resulta difícil, ya que pueden detectarse errores, especialmente en las redes que operan rápidamente.

III.4.10 SEGURIDAD DE RED

La seguridad de red y la disponibilidad de red se encuentran correlacionadas: una red comprometida puede no estar disponible para sus usuarios habituales. De este modo, la prevención de problemas de seguridad aumentará la confiabilidad total de los servicios de red.

Asimismo, en cuanto al área de seguridad, es necesario implementar herramientas con protocolos que manejen filtraje de dirección IP y el límite de velocidad del tráfico inesperado. El filtraje de dirección IP previene que las direcciones IP, que deberían ser únicamente utilizadas dentro de una empresa, atraviesen la red del proveedor de servicios así como también filtra cualquier tráfico con direcciones fuente inapropiadas (es decir, no parte del rango de direcciones IP asignado de la organización). Ambos tipos de tráficos son sospechosos, y al filtrarlos, desalienta a los "*hackers"* de utilizar la red para producir ataques maliciosos.

El límite de velocidad mediante mecanismos, tal como la velocidad de acceso comprometida (CAR[1]), controla el tráfico en ambos puntos de ingreso y de egreso de la red del proveedor de servicios, de este modo, reduciendo los ataques DOS y DOS distribuidos (DDoS). Los ataques DOS sobrecargan la banda ancha de acceso entre el proveedor de servicios y la empresa o sobrecargan un recurso de red con peticiones de servicios no requeridas, de este modo, despojando los recursos

[1] CAR : Velocidad de Acceso Comprometida *(Comitted Acces Rate).*

disponibles para ser utilizados en el tráfico legitimo. El tráfico de *Internet Control Message Protocol* (ICMP) es una manera común de sobrecargar el ancho de banda debido a que numerosos, si no todos los dispositivos de la red responden a estas peticiones. Las peticiones TCP SYN son una manera común de ocupar y de sobrecargar los servidores accesibles públicamente y costosos con peticiones con apertura de sesión no requeridas. Un ISP debería medir la línea de base de este tipo de tráfico no deseado. Luego de agregar el 50 por ciento para los valores picos, el proveedor de servicios obtendrá los parámetros requeridos para configurar el límite de velocidad que debería configurarse en ambos puntos del perímetro de su red.

Los proveedores de servicio de redes mentalizados en la seguridad contarán con sistemas detectores de ladrones (IDSs[1]) instalados en su red. Estos productos controlan todo el tráfico de la red, en busca de cualquier actividad o tráfico sospechoso que altere automáticamente al personal de operaciones de la red. Incluso la capacidad más simple de un IDS identifica 59 de los ataques de red más comunes y exploraciones con información utilizando análisis de firmas. El tráfico sospechoso puede ser registrado cronológicamente a fin de crear un rastreo de auditoria para un análisis posterior y si se desea, para hacer que los routers desechen automáticamente los paquetes dudosos.

III.4.11 MANTENIMIENTO Y OPERACIONES PROGRESIVAS "EL MAYOR RIESGO DE LA CONFIABILIDAD"

Un equipo sólido y bien diseñado, un excelente diseño de red con atención primordial en la redundancia y en la flexibilidad así como también un gran entorno físico son factores esenciales, pero los errores producidos por el personal de operaciones del proveedor de servicio de redes pueden frustrar todos estos factores. *Gartner Group* ha estudiado este problema e informa que no menos que el 40 por ciento, y tanto como el 80 por ciento, de la no disponibilidad de la red puede atribuirse al error humano.

El hecho de buscar y de contratar a un personal con experiencia no constituye una tarea fácil para un proveedor de servicio de redes como si lo es para una gran empresa. Pero aquellas personas con algunas aptitudes y cierta experiencia pueden ser mas fáciles de encontrar que otras.

El siguiente problema para los gerentes de operaciones es la capacitación del personal. Mantener al personal al día con los cambios en la tecnología y en los requerimientos de las mejores prácticas constituye una tarea desafiante.

[1] IDS : Sistema de Detección de Intrusiones (*Intrusión Detection System*)

Desafortunadamente, siempre habrá problemas de manera ocasional, y los excelentes proveedores de servicio de redes implementarán un programa activo de análisis con causa de raíz.

III.4.12 ERRORES HUMANOS Y PROCESOS DE ADMINISTRACIÓN Y MANTENIMIENTO.

Uno de los conceptos más difíciles para incluir en la preedición de disponibilidad es la contribución del error humano en el tiempo de inactividad de la red. Este concepto no es muy difícil de creer. No es una particular dificultad medir cuando esto pasa. La dificultad se origina cuando nosotros intentamos predecir estos errores por adelantado. Claro que los errores humanos normalmente ocurren cuando se realizan operaciones estándar. Una compañía que minimiza los errores humanos en operaciones estándar es un buen soporte para una alta disponibilidad de la red.

El error humano más que un error cuantitativo es un error cualitativo que contribuye al tiempo inactivo de las redes, hay un gran número de ejemplos donde se muestra la contribución del error humano en simples operaciones normales dentro de la red.

III.4.12.1 III.4.12.1 CREANDO EL MAPA DE TIEMPO INACTIVO CAUSADO POR DIFERENTES PROCESOS

Generalmente un humano que configura algún equipo in apropiadamente genera tiempo inactivo de la red. Esto pasa a menudo cuando las compañías intentan crecer sus redes y rompen una regla que causan que porciones de la red paren de trabajar. Una nota chistosa es que la persona que realiza el error raramente se da cuenta del problema esto no pasa con el nuevo componente, pero preferentemente con que ellos hagan para su red por intentar instalar el nuevo componente in apropiadamente. Por esta razón, nosotros incluiremos varios componentes en nuestra tabla involucrando las cosas que ocurren regularmente como ingenieros de redes cuando intentamos crecer sus redes.

Proceso	Disponibilidad	Tiempo Inactivo Anual
Falta de un plan de restauración para largas actualizaciones	*0.998178*	*16 horas*
Falta de un proceso de control de direcciones IP para nuevos equipos	*0.99932*	*6 horas*
Falta de proceso de prueba de nuevos productos antes de introducirlos a la producción de la red	*0.999*	*8 ¾ hora*
Falta de control de Password de acceso	*0.995*	*44 horas*
Autorizar cambio de routers sin procesos de estimación y prueba	*0.999*	*8 ¾ hora*

Tabla III.6 *Ejemplos de contribuciones de tiempos inactivos debido a errores humanos y procesos.*

Hay un centenar y muchos más de ejemplos de procesos que causan problemas dentro de la red y procesos que suavizan los problemas de la red. Por ahora introduciremos una pequeña cantidad de información en orden para proceder con la siguiente sección donde incluiremos estos tipos de figuras en nuestras predicciones de disponibilidad.

III.4.12.2 INCORPORANDO DESARROLLO DE PROCESOS EN LAS PREDICCIONES DE LA DISPONIBILIDAD DE RED.

Primeramente, nosotros mostramos como uno puede derivar la disponibilidad en un número de ejemplos de errores de procesos, después mostramos como podemos formar una tabla de problemas típicos en los procesos y asociarlos con los tiempos de la inactividad de la red. Ahora, usaremos la tabla generada para realizar un ejemplo de los cálculos de disponibilidad incluyendo los errores humanos y la contribución de los procesos para completar el tiempo inactivo de la red.

La primera cosa que tenemos que hacer, es crear un RBD[1] de nuestro escenario. Hacer esto es asociar el error con el tiempo inactivo. Para juntarlos, debemos de determinar como aplicar el tiempo inactivo. Un pequeño campo generara tiempo inactivo en una sola porción de la red. Un gran campo causara un tiempo inactivo en toda la red.

Para hacer las cosas más simples, usaremos un simple diagrama de red que representa a dos hogares los cuales están conectados a Internet vías un proveedor de servicio (ISP). Para clarificar el ejemplo, nosotros realizaremos los cálculos para un error hecho por un usuario del hogar el cual solo afecta sus propios servicios de red dentro del hogar y después realizaremos los cálculos para un error hace que se suspendan los servicios de red del proveedor de servicio. En la figura III.10 mostraremos el diagrama de red.

La tabla III.7 incluye los datos necesarios para calcular los tiempos inactivos de la red en base a los resultados de errores observados anualmente.

[1] RBD : Diagrama de Bloques de Comfiabilidad (*Reability Block Diagram*)

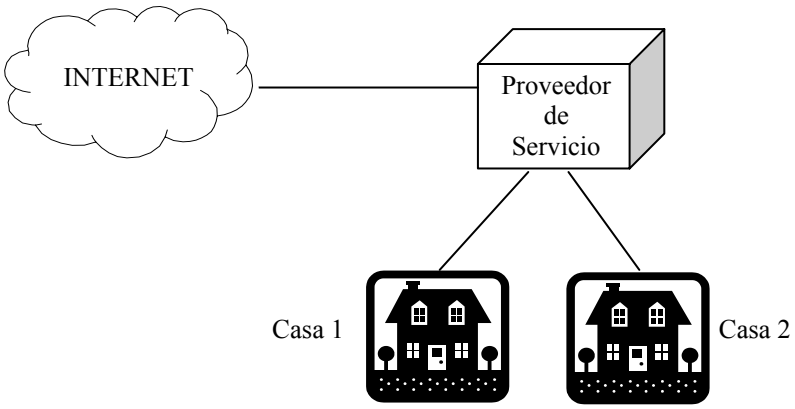


Figura III.10 *Diagrama de red para ejemplificar el error humano*

Componente de red	disponibilidad o frecuencia	Tiempo inactivo anual
La red del proveedor de servicio	.99999	5.2 minutos
Redes de las casa 1 y 2	.9999	52 minutos
El Internet	0.999999	.86 minutos
Error en la red del proveedor de servicio	35,064 horas	60 minutos
Error en la red de la casa 1	12,000 horas	120 minutos

Tabla III.7 *Los números de disponibilidad para ejemplos de errores humanos*

El primer error ocurrirá cuando el usuario en la red del hogar 1 hace algo que hace que su red sea incapaz de conectarse a la red del proveedor de servicio por un par de horas. Porque este error no afecta a la red del otro hogar donde el usuario hizo el error, el impacto para la red del hogar 2 es cero. En nuestro RBD en la figura III.11, podemos ver como dibujamos este concepto.

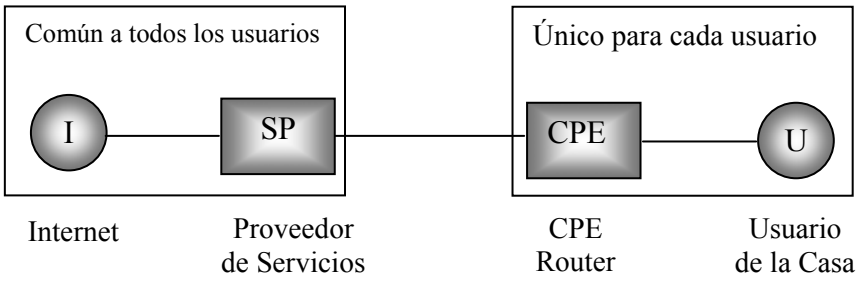


Figura III.11 *El RBD para ejemplos errores humanos*

Para el usuario en la casa 1 dibujado en la figura III.11, esta pausa es significativa. El segundo error será algún error hecho por el proveedor de servicio. El error del proveedor de servicio sacara todos los clientes de servicio por una hora. Este error sucederá una vez cada cuatro años como se muestra en la tabla III.7.

Ahora que sabemos como incluir el error humano dentro de las predicciones, comenzaremos una pequeña discusión acerca del proceso de las operaciones.

III.4.12.3 MITIGANDO EL ERROR HUMANO A TRAVÉS DE LA OPERACIÓN DE PROCESOS

La meta de predecir, cuantificar y generalmente hacer todo este trabajo de disponibilidad es hacer redes altamente disponibles. Porque una gran cantidad de datos en la contribución de errores humanos en los tiempos de inactividad de las redes no existe como tal, es mejor poner estos juntos en un simple proceso con el cual se pueden establecer los tiempos en particular sobre el tiempo.

En esta sección discutiremos un simple proceso por el cual se podrá determinar la contribución del error humano en el tiempo inactivo de la red. Predecir la futura contribución, y después tratar de minimizar esta contribución.

III.4.13 EL ALGORITMO PARA MEJORAR LA DISPONIBILIDAD DE RED.

El algoritmo que se usara constantemente para mejorar la disponibilidad de la red incluye 4 pasas. Cada uno de estos pasos debe ser atómico por naturaleza. Esto quiere decir que cada paso debe realizarse solo. Sin embargo los datos de otros paso pueden utilizarse por un paso subsecuente, pero el mezclar los datos invalidara los resultados y romperá el proceso.

Los cuatro pasos son listados como siguen a continuación:

Paso 1 Predicción
Paso 2 Medición
Paso 3 Análisis del problema o carencia
Paso 4 Cambio/cambio de dirección

III.4.13.1 PREDICCIÓN.

La fase de la predicción es fácil de explicar. En la predicción se debe predecir la disponibilidad de la red como mejor se pueda con la información que se tiene. Como se vera mas adelante “predicción de la disponibilidad punto a punto de la red: El método de Divide y Conquista”, predecir la disponibilidad de la red puede ser calculada desde diferentes perspectivas.

En un alto nivel, establecer las disponibilidades para cualquier porción de la red que se quiera cuantificar debe de ser echa en esta etapa.

Una vez que las disponibilidades se han calculado, se deben archivar hasta que sean nuevamente requeridos en el paso 3 de este proceso, el cual es el análisis del problema o carencia.

Se necesitara utilizar las técnicas avanzadas del método Divide y Conquista para completar este paso completamente. Para la explicación de este proceso, se necesitara simplemente entender que estaremos produciendo el porcentaje de predicción de la disponibilidad para cada red e irlas almacenando para un futuro uso.

III.4.13.2 CUANTIFICACIÓN

La fase de la cuantificación de los procesos difiere un poco de lo que se ha hecho hasta ahora. En lugar de predecir la disponibilidad de la red, estaremos realmente midiendo la disponibilidad de la red. Adicionalmente, en esta fase usaremos el método de fallas por millón de horas operacionales como se uso anteriormente.

Para producir los números requeridos para completar satisfactoriamente el análisis del problema hecho en el paso 3 de nuestro proceso, necesitaremos juntar una variedad de datos sobre nuestro tiempo de actividad de la red. Básicamente, necesitaremos juntar los datos del tiempo total de operación, el número de fallas y el tiempo inactivo de la red.

El tiempo de operación de nuestra red debe ser el número total de horas de operación. Esto incluye tanto el tiempo activo como el tiempo inactivo de la red. Este número debe ser multiplicado por el promedio de usuarios a los cuales les da servicio la red durante ese tiempo. Esto eventualmente llegara a ser nuestro denominador en nuestras ecuaciones de fallas por millos de horas.

Las horas de tiempo inactivo de servicio necesitaran ser guardadas para llevar un perfecto control de cada falla. Para cada falla, hay que guardar los tiempos de respuesta para restaurar la red para trabajar en orden, y con los cuales promediaremos para generar el MTTR. Adicionalmente, otros tiempos serán involucrados con la restauración de la red y que en cada falla deben ser anotados. En la figura III.12 indica los diferentes tiempos que se necesitan ser medidos en orden para ser completar satisfactoriamente la medida exacta de la disponibilidad de la red.

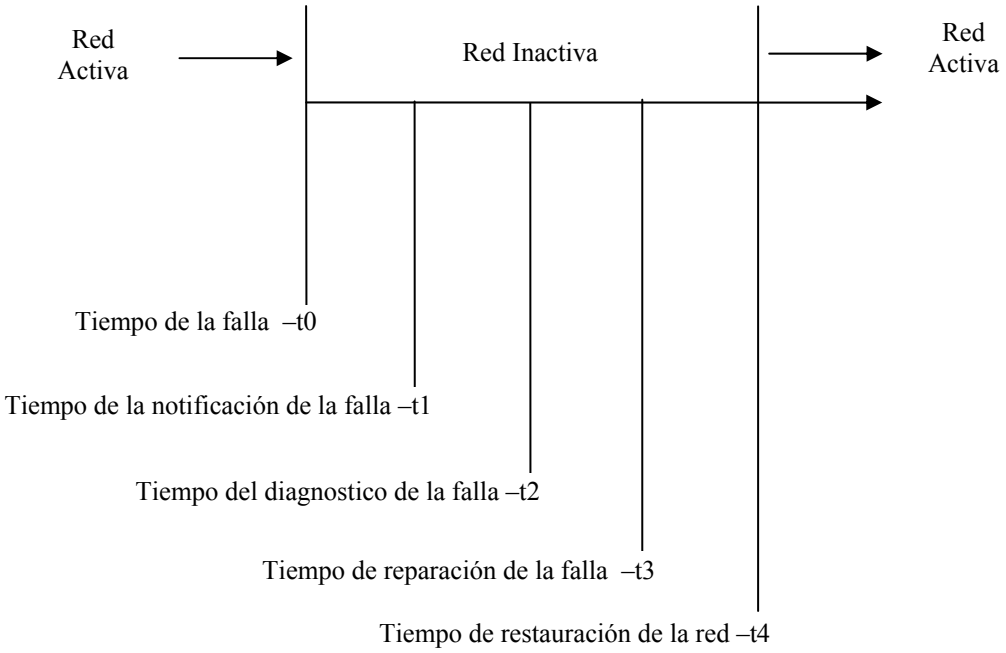


Figura III.12 *Datos que se necesitan colectar de cada falla*

Como se junten los datos como se muestra en la figura III-12, los datos deben ser registrados dentro de una hoja de calculo o una base de datos por que necesitaremos realizar una serie de de cálculos con los datos. Al recolectar toda esta información necesitaremos anotar tanto la fecha como el tiempo para cada ítem en el horario.

En la fase del análisis del problema de operación de la red, realizaremos una variedad de cálculos usando la información capturada durante la fase de cuantificación.

Un punto interesante, es que se puede seleccionar el tiempo de duración de la fase de medición para hacer más sencilla la matemática. Por ejemplo si se tienen 1000 usuarios en la red, se puede acabar la fase de recolección de datos de cada 1000 horas. Unas 1000 horas son aproximadamente seis semanas que podría ser una frecuencia conveniente para evaluar el estado de la red y realizar cualquier cambio.

III.4.13.3 ANÁLISIS DEL PROBLEMA

En esta fase de nuestro proceso de operación, realizaremos todos los cálculos para convertir nuestros datos tomados en la fase de medición reportes significativos. Adicionalmente, convertiremos algunos de los datos en un porcentaje de disponibilidad, y así podremos comparar las mediciones con las predicciones. Si las mediciones no concuerdan con las predicciones, entonces necesitamos realizar una

investigación mas detallada, hacer cambios, o de otra manera decidimos que acción hacer para mejorar las disponibilidad de la red.

Los primeros cálculos que mucha de la gente hace son simplemente calcular el numero de falla por un millón de horas y el tiempo promedio para reparar cada falla. Como veremos, nosotros no tenemos que esperar un millón de horas para observar las fallas en un millón de horas. Nosotros podemos utilizar multiplicadores como por ejemplo numero de usuarios para obtener el millón de horas mucho más rápido que 114 años.

Como aprendimos anteriormente en este capitulo, MTTR es generado tomando el total de horas de tiempo inactivo y dividido por el número de fallas para obtener la cantidad de tiempo promedio por falla.

La siguiente cosa por hacer en nuestro análisis de los datos que medimos, es mirar cualquier oportunidad para mejorarla. Lograr nuestra meta de cinco 9´s puede ser posible con cambios que pueden ser obvios al observar nuestros datos. Se puede observar que el tiempo de notificación del problema fue considerablemente grande si el problema ocurrió a media noche por ejemplo. Ahora queremos mostrar como podemos encontrar este tipo de cosas usando los reportes que pueden ser generados por los datos que recogimos.

En muchos casos si nosotros observamos un incremento en el rango o la desviación estándar, podemos encontrar una oportunidad para mejorar. Y si se encuentra una fase sospechosa, se realiza una post verificaron en cada uno de las fallas y tratamos de descubrir por que la fase es menos consistente que as otras fases.

III.4.13.4 CAMBIO/ CAMBIO DE ADMINISTRACIÓN

La fase de cambio de administración es el tiempo cuando hacemos cambios sobre nuestra red o procedimientos operacionales. Si nosotros hacemos los cambios descritos en la sección anterior, fuera del ciclo, no tendríamos forma de conocer si nuestros cambios fueron hechos para bien o para mal en nuestra red.

En la sección anterior, observamos que localizamos un problema en el proceso al usar las medidas y cálculos hechos en las fases apropiadas. El proceso debe continuar de tal manera que nosotros hacemos cualquier cambio durante la fase de cambio de administración, documentando estos cambios, actualizando nuestras predicciones de disponibilidad si es necesario, y después procedemos con la fase de medición. Este repetitivo proceso hace incrementar muy probablemente nuestra disponibilidad

III.4.13.5 ERROR HUMANO Y RESUMEN DE PROCESOS DE OPERACIÓN

Como con las otras contribuciones para el tiempo inactivo en una red, el error humano y los procesos estándares pueden ser considerados. En la ausencia de una gran cantidad de datos para usarse para la predicción, nosotros tenemos que establecer un proceso para reunir datos que puedan ayudarnos ha determinar el tiempo inactivo relacionado con el error humano y los problemas de proceso.

III.5 PREDICIENDO PUNTO A PUNTO LA DISPONIBILIDAD DE LA RED. EL MÉTODO DE DIVIDE Y VENCERÁS.

Ahora describiremos un proceso con el cual dividiremos una red en razonables escenarios y creamos diagramas e bloque de fiabilidad (RBD) para cada escenario. Una vez que entendimos como predecir la disponibilidad de una red por escenario, podremos tomar decisiones para mejorar el diseño de la red para aumentar la disponibilidad de la misma.

En este capitulo solo consideraremos la disponibilidad de los sistemas y su asociado hardware y software. Omitimos olas otras contribuciones de tiempo inactivo de la red para hacer mas sencillo la explicación del método divide y vencerás.

III.5.1 PASOS DEL MÉTODO DIVIDE Y VENCERÁS.

Cuando comenzamos a estudiar la disponibilidad inherente en una red compleja, nosotros notamos rápidamente que hay varios escenarios diferentes. Redes de Voz sobre IP (VoIP) tienen escenarios que son fáciles de ver. Una persona que hace una llamada telefónica a la casa de la siguiente puerta utiliza una red completamente diferente que una persona que hace una llamada telefónica a través de la ciudad.

El primer paso a usar en el método divide y vencerás es para reconocer que mas de un escenario existe en la red en cuestión. Una vez que tenemos decidido que hay múltiples escenarios, estaremos listos para comenzar a utilizar el algoritmo de divide y vencerás.

El algoritmo divide y vencerás esta representado por los siguientes pasos:

Paso 1 Determinar los escenarios y crear RBDs para cada escenario para ser analizado. Asegurarse de las redundancias.

Paso 2 Realizar cálculos para componente de la red en el RBD

Paso 3 Para cada escenario:

- Realizar cálculos en secciones seriales, contenidas dentro de las secciones paralelas, para determinar una figura de disponibilidad para cada sección.
- Realizar cálculos en secciones paralelas dentro de una figura de disponibilidad para la sección paralela
- Repita como sea requerido hasta que el resultado punto a punto pueda ser archivado vía un simple cálculo serial punto a punto.

Paso 4 Para cada escenario, multiplicamos todas las secciones (incluyendo los resultados del paso 3) para obtener el resultado de disponibilidad punto a punto.

IV

NECESIDADES DE MAYORES TASAS DE TRANSMISIÓN Y LIMITACIONES ACTUALES DE UN SISTEMA DE TELECOMUNICACIONES

Con el avance de la tecnología, miles de personas e innumerables empresas están participando del proceso de globalización, principalmente a través de las comunicaciones y de la red de comunicación de datos.

La comunidad de negocios asigna actualmente un alto valor a determinados atributos, una demanda insaciable de velocidad, la facultad de acceso instantáneo a fuentes de información, y sobre todo la imperiosa necesidad de adaptarse a fluctuantes exigencias de los usuarios.

Estas necesidades se deben al gran desarrollo y demanda de aplicaciones, como son el Internet, simulaciones en tiempo real interactivas, modelado tridimensional, manejo de imágenes, videos, así como el manejo de diferentes tipos de información y la integración de los sistemas de voz.

También el gran avance y crecimiento en las industrias de las telecomunicaciones y computo han hecho que algunas de las redes actuales no soporten el incremento tan importante en el trafico de datos. Además que los sistemas de información cada vez son mas grandes, autónomos y complejos.

Un ejemplo claro es el crecimiento del Internet, desde 1994 la población global de Internet se ha incrementado de forma exponencial (de 13 a 300 millones), y las cifras más recientes muestran el gran crecimiento del Internet en los últimos años

- ***Páginas web:*** más de dos mil millones de páginas de información se encuentran disponibles en la Web.
- ***Volumen de tráfico:*** Cada cien días el volumen de tráfico en Internet aumenta 100%. (U.S. Dept. of Commerce, abr. 2000).
- ***Visitas diarias:*** En EE.UU, las páginas web recibieron en promedio mil millones de impactos por día en octubre de 2001 (eMarketer/Media Metrix, nov. 1999).
- ***Cantidad de e-mails:*** Los cálculos de 1998 indican que durante ese año se envió un promedio de entre 618.000 millones y 4 billones de e-mails. En comparación, el correo estadounidense repartió 101.000 millones de cartas. (U.S. Internet Council, abr. 2002).
- ***Capacidad de backbone:*** La capacidad de transporte de información a través del backbone de Internet se duplica cada 100 días. (U.S. Internet Council, abr. 1999).
- ***Registro de dominios:*** Existen 12.844.877 de "dominios" (Ej.: Cisco.com) registrados en el mundo. Cada semana se inscriben 428.023 dominios. (NetNames Statistics 12/28/2002).

Está claro que si con este gran crecimiento todas las personas intentaran acceder a toda esa información en algún momento al mismo tiempo, se producirá una saturación inmensa. La regla general ha sido siempre que no importa cuán grande sea el tamaño del canal, Internet lo podrá llenar y rebasar sin ninguna duda.

Otros aspectos importantes en considerar es la introducción de aplicaciones las cuales no solo soportan datos sino que estas ya integran, voz, datos, video, imágenes, audio telemetría, etc., y las cuales demandan mejores diseños de red, ancho de banda, herramientas de monitoreo, configurarción y mantenimiento de las redes, las cuales son funciones y responsabilidad de la administración de la red.

Pero aun más importante para el diseño de estas redes es la necesidad de transparencia de interconexión de las mismas, en el software y en el hardware, tanto en las redes de área local como remota.

IV.1 SISTEMAS MULTIMEDIA

Las investigaciones y desarrollos en el área de la multimedia se puede dividir en dos grandes grupos: el primero centrado en el área de estaciones de trabajo independientes con el software y las herramientas relacionadas, tal como composición musical, enseñanza asistida por computador, video interactivo, etc. El segundo grupo centrado en el intercambio de información multimedia entre esas estaciones de trabajo a través de redes, combinando así los sistemas distribuidos con la multimedia. Todo esto ofrece un gran panorama y un enorme potencial para nuevas aplicaciones basadas en los sistemas multimedia distribuidos, los cuales incluyen sistemas de información multimedia, los sistemas de colaboración y conferencia, los servicios multimedia sobre demanda, televisión de alta resolución y la enseñanza a distancia.

Los sistemas distribuidos multimedia requieren transferencia de datos continua sobre periodos de tiempo relativamente altos, sincronización en el manejo de los diferentes tipos de datos (ejemplo: voz y sonido), espacios de almacenamiento extremadamente grandes, manejo de tiempo real y técnicas especiales de indexamiento y recuperación de los datos de tipo multimedia, además de otros problemas que surgen a partir de éstos.

Esa creciente necesidad de incrementar la interconexión de las cada vez más poderosas estaciones de trabajo multimedia da como resultado una evolución de las comunicaciones en búsqueda de las redes (sus características) que soporten la transmisión de este tipo de información multimedia.

Los distintos avances en la tecnología han permitido el desarrollo de aplicaciones multimedia técnica y económicamente realizables. Estos avances incluyen el poder de las estaciones de trabajo, la alta capacidad de los dispositivos de almacenamiento, las altas velocidades de las redes, los avances en tratamiento de imágenes y vídeo, los avances en el manejo del procesamiento del audio, procesos de reconocimiento de voz, los algoritmos de compresión y el avance mismo del audio y el vídeo.

Los sistemas de conferencia permiten que un cierto número de participantes intercambien información multimedia a través de redes de voz y datos. Cada participante cuenta con su estación de trabajo multimedia sobre redes que soportan velocidades altas. Cada uno de dichos participantes puede enviar o recibir vídeo, audio, y datos y puede desempeñar ciertas actividades de colaboración. Estas conferencias multimedia manejan el concepto de “espacios de trabajo virtual compartido” el cual describe las partes del despliegue que son replicadas para todas las estaciones.

IV.1.1 REDES MULTIMEDIA

Muchas aplicaciones, tal como el video mail, video conferencia y los sistemas de trabajo colaborativo requieren redes multimedia, en donde los objetos multimedia son almacenados en un servidor y desplegados en los sitios de los clientes. Tales aplicaciones requieren grandes anchos de banda, hacer transmisiones de los datos multimedia a todas las direcciones (los diversos sitios remotos) de una red o subred y acceder grandes depósitos de recursos multimedia.

En los ambientes tradicionales de redes de área local la información de tipo multimedia se encuentra almacenada en cada uno de los equipos y es manejada de manera independiente por cada uno de ellos. En general no pueden soportar un esquema en el cual cada uno de esos equipos acceda a servidores remotos en los cuales se encuentra toda la información multimedia, debido a varias razones, entre las cuales se tienen:

- Las redes multimedia requieren de altos anchos de banda aún cuando los datos se encuentren comprimidos, por ejemplo los requerimientos de ancho de banda proyectados para el manejo de televisión de alta definición es de 20 Mbps mínimo.

- La mayoría de las comunicaciones de las redes multimedia son multipunto, a diferencia de las redes tradicionales que realizan comunicaciones punto a punto, lo que implica que muchas aplicaciones como las de conferencia utilicen métodos de "*multicasting*" (replica una simple señal de entrada y las transmite a múltiples destinos) y "*bridging*" (combina múltiples señales de entrada dentro de una o más señales de salida, las cuales entonces se transmiten a los participantes).

- Las redes tradicionales son manejadas de tal manera que los datos estén libres de errores, no obstante muchas aplicaciones multimedia pueden tolerar errores en su transmisión, bien sea por errores en los paquetes o perdida de los mismos. En algunos casos, los requerimientos de tiempo real no permiten realizar corrección a los datos o realizar retransmisión de los mismos (ya que se incurriría en demoras inaceptables), lo cual hace pensar que se requieren protocolos más flexibles que los protocolos centrados en la detección y corrección de errores.

Con este tipo de requerimientos las redes tradicionales no soportan el manejo de sistemas multimedia.

IV.1.2 REQUERIMIENTOS EN COMUNICACIONES MULTIMEDIA

Los sistemas distribuidos multimedia requieren transferencia de datos continuos sobre periodos de tiempo relativamente altos, sincronización en el despliegue de los diferentes tipos de datos (ejemplo: voz y sonido), espacios de almacenamiento extremadamente grandes, manejo de tiempo real y técnicas especiales de indexamiento y recuperación de los datos de tipo multimedia, además de otros problemas que surgen a partir de éstos. En general la complejidad de los problemas relacionados con las aplicaciones multimedia tienen que ver con todos los componentes de un sistema de computación.

IV.1.2.1 REQUERIMIENTOS A NIVEL DE RED

Desde el punto de vista de la red, los más importantes requerimientos son:

- Tasa de transferencia sobre demanda: Las redes deben soportar tasas de transferencia de bits constantes y variables por cada conexión establecida, para diferentes y cambiantes necesidades. Por ejemplo unos pocos Kbps son necesarios para llevar a cabo rutinas de reporte o de control pero muchos Mbps son necesarios para poder transmitir imágenes de alta resolución o para comunicaciones de vídeo de alta definición. Este punto es bien importante si se tiene en cuenta que para los nuevos servicios, que van desde la comunicación de vídeo interactivo hasta la distribución del mismo, se requiere de distintas y variables ráfagas de bits.

- Conexiones sobre demanda: Una específica estructura de comunicación, como por ejemplo los sistemas de trabajo colaborativo, puede demandar un manejo dinámico de las distintas conexiones involucradas (adicionando nuevas conexiones para manejar nuevos patrones de comunicación, liberar una conexión cuando no se requiera por mucho tiempo, etc.) lo cual estaría relacionado, además, a sí la conexión es punto a punto, sí es multipunto, si existen relaciones de multicasting, etc. Esto requeriría de un sistema de comunicación que pueda ser configurado y reconfigurado dinámicamente y que sea de alguna manera, como sea posible, independiente de las restricciones físicas para incrementar su flexibilidad.

- Sincronización de diferentes tipos de información sobre demanda: Los nuevos tipos de información multimedia hacen que se tenga que manejar nuevas características de sincronización en la comunicación. Se necesita desde la sincronización de conexiones de comunicación de diferentes tipos de información mutuamente dependientes (vídeo con su correspondiente información de sonido) dentro de un dialogo o un mensaje hasta la sincronización que involucra manejo de tiempo real o, para algunos tipos de

información, la sincronización de objetos que esperan por algunos eventos previamente definidos.

- Calidad del servicio sobre demanda: Para manejar las comunicaciones de los distintos tipos de datos multimedia se deben definir la calidad del servicio. La calidad del servicio es un conjunto de parámetros que incluye las ráfagas de velocidad, la utilización del medio de transmisión, el promedio de las demoras, la rata de errores permitida, la rata de error de los paquetes, etc.

IV.1.3 VOZ IP

La telefonía IP forma parte de una serie de tecnologías, conocidas como tecnologías de convergencia, que están llamadas a jugar un papel muy importante en un futuro próximo. Estas tecnologías hacen desaparecer la diferenciación actual entre voz y datos, de tal manera que ambas compartan una misma infraestructura, y tratan de aportar a las comunicaciones de voz las posibilidades y ventajas que ofrecen las redes basadas en el protocolo Internet.

Las redes de convergencia permiten desplegar aplicaciones de banda ancha de forma más eficiente, asimismo se eliminan muchos costos asociados a la gestión de telefonía conmutada, gracias a los sistemas de directorios, así como a la posibilidad de acceso telefónico a bases de datos y agendas personales.

Dado lo anterior, la telefonía IP está llamada a experimentar un importante crecimiento en los próximos años. Según un informe realizado recientemente por la firma de analistas ***Giga Group***, se pone de manifiesto el relativo buen comportamiento experimentado por el mercado del telefonía IP dentro de mercado de las telecomunicaciones. A pesar de la recesión de este mercado, durante el pasado ejercicio se dobló el número de nuevas líneas IP de voz instaladas en Estados Unidos, suponiendo el 18% del total de nuevas líneas contratadas. En Europa esta cifra alcanza el 10% del total.

Se espera que para el 2003, el porcentaje de nuevas líneas de voz IP implantadas alcance el 25% del total en Estados Unidos, con un crecimiento sostenido de aquí a 2006, fecha en la que se estima que el número de nuevas líneas de voz IP superará al de nuevas líneas conmutadas. En Europa y resto del mundo la tendencia será similar, pero habrá que esperar algunos años más para que la voz IP supere el 50% de nuevas líneas.

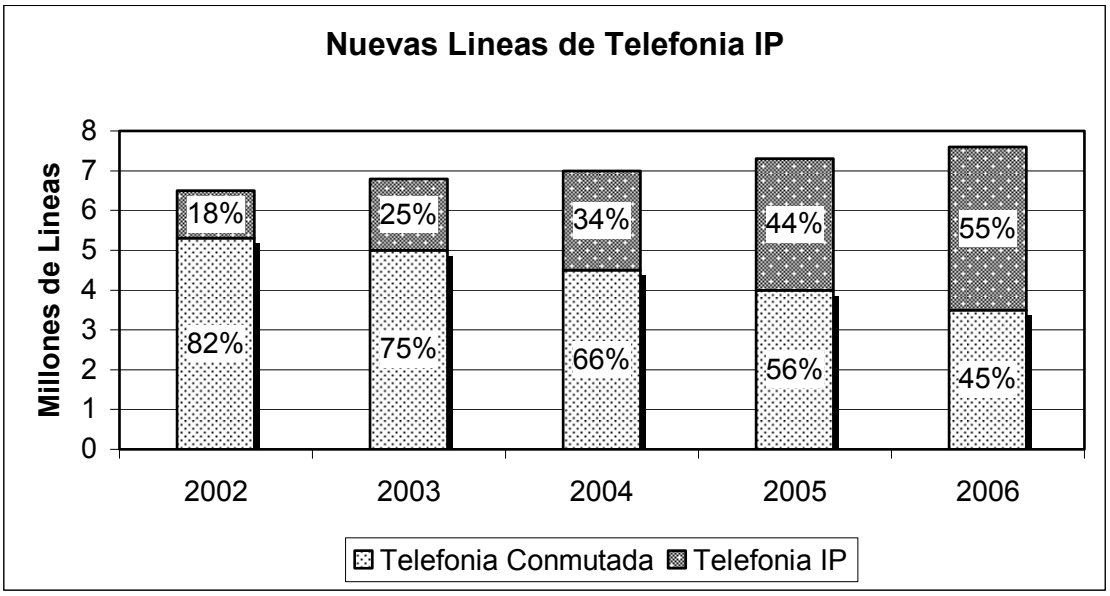


Figura IV.1 *Nuevas líneas de Telefonía*

Se ha observado asimismo que hasta la fecha, los despliegues de redes de voz IP han correspondido en Estados Unidos a empresas de tamaño medio o sucursales. La tendencia sin embargo se va a modificar, aumentando el número de líneas instaladas en grandes compañías, a medida que salgan al mercado equipos capaces de satisfacer las necesidades de estos clientes y éstos amorticen sus anteriores inversiones en equipos de telefonía.

IV.1.3.1 NUEVAS FUNCIONALIDADES EN EL MERCADO DE TELEFONÍA IP

Uno de los factores que van a dinamizar este mercado es el gran número de prestaciones que ofrece la convergencia, ya que permite a las empresas aprovechar las mismas infraestructuras de red de datos para soportar las comunicaciones de voz, eliminando la necesidad de contar con una infraestructura de voz paralela.

Asimismo se eliminan muchos costos asociados a la gestión de telefonía conmutada, gracias a los sistemas de directorios, así como a la posibilidad de acceso telefónico a bases de datos y agendas personales.

IV.1.4 BANDA ANCHA

Al hablar de estas crecientes demandas de redes las multimedia o redes de convergencia necesariamente tenemos que hablar de sistemas de banda ancha. Mucha gente asocia a la banda ancha con determinada velocidad de transmisión o un

conjunto específico de servicios, tales como el bucle de abonado digital (DSL) o las redes inalámbricas de área local (WLAN). Sin embargo, puesto que las tecnologías de banda ancha cambian continuamente, su definición va evolucionando a la par. Hoy en día el término banda ancha normalmente describe a las conexiones Internet recientes que funcionan entre 5 y 2 000 veces más rápido que las anteriores tecnologías de marcación por Internet. Sin embargo, el término banda ancha no se refiere a una velocidad determinada ni a un servicio específico.

El concepto de banda ancha combina la capacidad de conexión (anchura de banda) y la velocidad. En la Recomendación I.113 del Sector de Normalización de la UIT se define la banda ancha como una "capacidad de transmisión más rápida que la velocidad primaria de la red digital de servicios integrados (RDSI) a 1,5 ó 2,0 megabits por segundo (Mbits)".

IV.1.4.1 LA BANDA ANCHA TIENE TRES VENTAJAS PRINCIPALES:

Las velocidades de la banda ancha son apreciablemente más rápidas que las de tecnologías anteriores, por lo cual resulta más rápido y cómodo acceder a la información o efectuar transacciones en línea utilizando Internet. La velocidad del servicio de banda ancha también ha permitido perfeccionar algunos servicios existentes tales como el de juegos en línea, y ha dado lugar a nuevas aplicaciones como la telecarga de música y vídeos.

En función del tipo de tecnología utilizada, la banda ancha puede aportar beneficios económicos. Por ejemplo, gracias a la tecnología DSL, los usuarios pueden utilizar una sola línea telefónica normalizada para servicios de voz y datos.

Esto les permite navegar por Internet y efectuar una llamada simultáneamente utilizando la misma línea telefónica. Anteriormente los usuarios asiduos de Internet tenían que instalar una línea telefónica adicional en su vivienda para acceder a Internet; gracias a la banda ancha, ya no se necesitan dos líneas telefónicas.

La banda ancha permite perfeccionar las actuales aplicaciones de Internet, al tiempo que abona el terreno para nuevas soluciones que antes resultaban demasiado onerosas, ineficaces o lentas. Éstas varían desde los nuevos servicios de administración gubernamental en línea, tales como rellenar electrónicamente los formularios de impuestos, hasta servicios de salud o aprendizaje en línea sin dejar mencionar el aumento del nivel de comercio electrónico.

IV.1.5 LIMITANTES

Pero no solo la necesidad de mayores anchos de banda solucionan las necesidades de las redes actuales, hay otros factores que interesan y que pueden llegar a ser limitantes en el diseño de redes, tales como las tecnologías, protocolos, seguridad, movilidad, calidad de servicio, costos, etc.

En general las tecnologías como tales, tienen algunas limitantes, ya sea en los protocolos que manejan y a su vez diferentes aspectos que en veces no son considerados.

Como por ejemplo el stack de protocolos TCP/IP, el cual fue creado hace mas de 20 años y el cual ha demostrado ser flexible y poderoso, pero con el gran crecimiento exponencial del Internet se ha visto que es la inminente la saturación del espacio de direcciones publicas IP, además que tiene varias ineficiencias como son:

- Requiere de mecanismos de seguridad
- Ruteo ineficiente,
- Difícil de adecuar a las nuevas aplicaciones de videoconferencia y multimedia,
- Necesidad de usar NAT.

Estas y otras características son consecuencia de que IPV4 no fue pensado para ser seguro, fue solo un diseño para ser una red militar, investigación y educación, pero aislada que después se convirtió en una red publica y la gente la vio como un gran negocio comercial. Es por ello que han surgido muchas limitantes de IPV4 para las nuevas aplicaciones que tiene hoy en día, en especial la necesidad de nuevas direcciones públicas de la red que obstaculiza el crecimiento de esta.

IV.1.5.1 SEGURIDAD

La seguridad es otro punto muy importante hoy en día dentro de las redes de comunicaciones con la explosión del uso masivo de Internet, tanto las computadoras personales como las redes de computadoras, pueden ser vulnerables a diversos tipos de ataques. Internet ha pasado a ser sin ningún tipo de dudas la mayor red pública de datos, a través de la cual se facilitan comunicaciones personales y empresariales en todo el mundo.

Conforme va aumentando el uso de la red de redes, aumentan las posibles amenazas sobre las distintas empresas y particulares que hacen uso de Internet. Entre los posibles ataques a los que puede estar sujeta una red corporativa o un

particular se encuentran los virus, vándalos y troyanos; los ataques de *hackers* como podrían ser ataques de reconocimiento, de acceso, de negación de servicios y de interceptación de datos; e incluso una empresa debe ser capaz de estar protegida frente a los ataques desde dentro de la misma empresa, donde los mismos empleados de forma inconsciente, negligente o vengativa pueden causar daños irreparables.

Entre las principales consecuencias de estos ataques se encuentran la pérdida de datos de vital importancia, violación de la privacidad y caída de la red durante varios días.

Es importante, por parte de las empresas el establecer un sistema total de seguridad basado en identificación, privacidad, administración de las políticas y definición de un perímetro de seguridad.

Por otra parte la integración de voz IP en las redes de datos hace que también se tome en cuenta la seguridad sobre los aparatos, ya que los teléfonos también son susceptibles de recibir ataques de *hackers* y son un punto de entrada vulnerable que hay que proteger.

IV.1.5.2 MOVILIDAD

Una de las tecnologías más prometedoras y discutidas en estos tiempos es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante ondas de radio o luz infrarroja. Las redes inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos.

En los últimos años el crecimiento en la demanda de soluciones inalámbricas para las empresas y últimamente también para el hogar, ha crecido de una manera espectacular. Las distintas tecnologías inalámbricas permiten dar una cobertura casi en cualquier rincón del planeta. Cientos de millones de personas en todo el mundo se comunican e intercambian información todos los días usando una u otra tecnología inalámbrica, permitiendo el envío de datos y con una movilidad sin precedentes.

Las tecnologías más usadas y conocidas hoy día son las de los teléfonos celulares, sistemas de navegación, servicios de mensajes, el antiguo radio etcétera. Pero el gran exponente hoy de la revolución digital y como los bits forma parte de nuestro día a día, proviene del intercambio de datos digitales. Estos datos no sólo se quedan limitados al ámbito de las computadoras, sino también en una gran cantidad de aplicaciones, pasando desde los grandes sistemas de tratamiento de datos empresariales y científicas hasta las más pequeñas utilidades personales destinadas a mejorar nuestro día a día.

Ya no estamos atados a redes cableadas sino que podemos acceder y compartir datos llevándolos con nosotros, dondequiera que vayamos.

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una *"red híbrida"* y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina

La disponibilidad de conexiones inalámbricas y redes LAN inalámbricas puede ampliar la libertad de los usuarios de la red a la hora de resolver varios problemas asociados a las redes con cableado fijo y en algunos casos, incluso reducir los gastos de implementación de las redes. Sin embargo, a pesar de esta libertad, las redes LAN inalámbricas traen consigo un nuevo conjunto de desafíos, principalmente la interconexión y nuevamente la seguridad.

La seguridad en las redes alámbricas es una nueva limitante de las redes actuales ya que en un principio se preocuparon solamente por alcanzar mayores tasas de transmisión pero quedaron pendientes varios temas por cubrir, entre ellos la seguridad. Con la tecnología inalámbrica si logramos la movilidad tan deseada pero hay que considerar que ahora el medio de difusión de la red es público y cualquier persona puede acceder a ella y ya no solo se corren los riesgos de una intrusión desde Internet, sino que cualquier persona puede tener acceso directo a la infraestructura de la red LAN.

IV.1.5.3 CALIDAD DE SERVICIO

Se entiende por calidad de servicio la posibilidad de asegurar una tasa de datos en la red (ancho de banda), un retardo y una variación de retardo (*jitter*) acotados a valores contratados con el cliente. En las redes Frame Relay o ATM por ejemplo la calidad de servicio se garantiza mediante un contrato de CIR [1] (*Committed Information Rate*) con el usuario. Para disponer de una calidad de servicio aceptable en redes soportadas en protocolo IP se han diseñado herramientas a medida como son los protocolos de tiempo-real RTP[2] y de reservación RSVP[3]. Por otro lado, un problema evidente es que cuando se soporta un servicio de voz sobre IP (VoIP) por

[1] CIR : Tasa de Información Comprometida, Velocidad a la que una red *Frame Relay* acepta transferir información bajo condiciones normales.
[2] RTP : Protocolo de Transporte en Tiempo Real (*Real Time Protocol*)
[3] RSVP : Protocolo de Reservación de Recursos (*Resource ReserVation Protocol*)

ejemplo, los paquetes son cortos y el encabezado es largo comparativamente. En este caso se requiere un encabezado reducido y un proceso de fragmentación e intercalado LFI[4]. Mediante QoS (*Quality os Service*) se tiende a preservar los datos con estas características. Los servicios tradicionales de la red Internet (SMTP o FTP) disponen de una calidad denominada "*best effort*"; es decir que la red ofrece el mejor esfuerzo posible para satisfacer los retardos mínimos; lo cual no es mucho pero es suficiente para servicios que no requieren tiempo-real como el web. Para servicios del tipo "*real-time*" (voz y vídeo) se requiere una latencia mínima.

Latencia-Jitter. Se denomina latencia a la suma de los retardos en la red. Los retardos están constituidos por el retardo de propagación y el de transmisión (dependiente del tamaño del paquete), el retardo por el procesamiento "*store-and-forward*" (debido a que los switch o router emiten el paquete luego de haber sido recibido completamente en una memoria buffer) y el retardo de procesamiento (necesario para reconocimiento de encabezado, errores, direcciones, etc). Un tiempo de latencia variable se define como *jitter* (fluctuación de retardo) sobre los datos de recepción. La solución al jitter es guardar los datos en memorias buffer, lo cual introduce un retardo aun mayor. Se han implementado diversas formas de buffer garantizados mediante software:

- ***Cola prioritaria:*** donde el administrador de la red define varios niveles (hasta 4) de prioridad de tráfico.
- ***Cola definida:*** donde el administrador reserva un ancho de banda para cada tipo de protocolo específico.
- ***Cola ponderada:*** mediante un algoritmo se identifica cada tipo de tráfico priorizando el de bajo ancho de banda. Esto permite estabilizar la red en los momentos de congestión.

IV.1.5.4 VARIANTES DE SERVICIOS.

Los servicios de datos y multimediales tienen distintos requerimientos de calidad referido a latencia y *jitter*. Para satisfacer los requerimientos de calidad se acude al manejo de las colas de paquetes, la reservación de ancho de banda y la gestión del tráfico. Para obtener estos objetivos en diversos ámbitos se han definido variantes de servicios.

[4] LFI : Indicador de ultimo archivo

V

NUEVAS TECNOLOGÍAS EN SISTEMAS DE TRANSMISIÓN DE INFORMACIÓN

V.1 IPV6

Uno de los nuevos estándares que se están implementando es IPv6. Aunque aun no se ha introducido oficialmente como un estándar, debido a que este se encuentra todavía en observación, por lo cual es muy posible que esta información este sujeta a cambios. Para efecto de la tesis se considerará IPv6[1] como un estándar, pero se debe aclarar que esta información no es definitiva.

Algunos libros se han publicado para describir más a detalle este estándar emergente, así como todos los RFC[2]s disponibles en Internet tienen información detallada de como se esta desarrollando, así como sus avances.

[1] IPv6: Protocolo de Internet Versión 6 (*Internet Protocol V. 6*)
[2] RFC: Petición de Comentarios *(Request for Comments)*

IPv4[1] en la actualidad es el protocolo mas usado, aunque genera preguntas sobre su capacidad de desempeño dentro de la comunidad de Internet, IPv4 fue elaborado en los años setenta y ha empezado a mostrar las debilidades de su edad. El problema principal de IPv4 es la falta de direccionamiento, porque muchos expertos creen que estamos superando las casi cuatro mil millones de direcciones disponibles. Aunque esto parece como un número muy grande de direcciones, múltiples bloques de gran tamaño son dados a las agencias gubernamentales y a las grandes organizaciones. Por lo cual IPv6 podría ser la solución a muchos problemas, pero todavía no se desarrolla ni se estandariza totalmente.

IPv6 fue recomendado por los directores del área de IPng del *Internet Engineering Task Force* en la reunión del IETF de Toronto el 25 de julio de 1994, el RFC 1752, es la recomendación para el protocolo de la generación siguiente del IP, dicha recomendación fue aprobada por el *Internet Engineering Steering Group* e hizo un estándar el 17 de noviembre de 1994.

IPv6 fue hecho un estándar de bosquejo del IETF el 10 de agosto de 1998. La versión 6 del Protocolo de Internet se abrevia IPv6 (donde el "6" refiere es la versión número 6). La versión anterior del Protocolo de Internet es la 4 (designada IPv4).

IPv6 es una nueva versión de IP que fue diseñada para ser un paso evolutivo de IPv4. Puede ser instalado como mejora del software en dispositivos de Internet y es interoperable con el IPv4 actual. IPv6 se diseño para funcionar en redes de alto rendimiento (ej. Gigabit-Ethernet, etc.) y al mismo tiempo que sea eficiente para las redes de bajo ancho de banda. Además, proporciona una plataforma para la nueva funcionalidad de Internet que será requerida en un futuro.

IPv6 incluye un mecanismo de transición que permite que los usuarios adopten y desplieguen IPv6 de una manera altamente difusa y que proporcionen interoperabilidad directa entre los usuarios de IPv4 e IPv6. La transición a una nueva versión del Protocolo de Internet debe ser incremental, con pocos o ningunas interdependencias críticas.

Muchos de los diseñadores más capacitados han estado con IPv6 desde inicios de los 90s, cientos de RFCs han sido escritos y han detallado algunas de las áreas más importantes, incluyendo direccionamiento expandido, formato de encabezado simplificado, etiquetado de flujo, autenticación y privacidad.

El direccionamiento expandido nos mueve desde una dirección de 32-bits a una de 128-bits a través del método de direccionamiento. También proporciona nuevos métodos unicast y de broadcasting, inyecta notación hexadecimal en las direcciones

[1] IPv4: Protocolo de Internet Versión 4 (*Internet Protocol V. 4*)

IP y se mueve de usuario a usuario con delimitadores, la figura V.1 muestra el formato de paquete de encabezado de IPv6.

Figure V.1 *Formato de Paquete de Encabezado de IPv6.*

V.1.1 DESCRIPCIÓN DE PAQUETE DE ENCABEZADO

El encabezado simplificado es de una longitud de 40 bits y el formato consiste en versión, clase, etiqueta de flujo, longitud de la carga útil, siguiente encabezado, límite de salto, dirección de la fuente, dirección de destino, datos, y campos de la carga útil.

V.1.2 HEXADECIMAL "HEX"

Simplificadamente, los números hexadecimales están en base 16. El decimal es base 10, contando de 0 a 9 y agregando una columna para hacer 10. Contando en hexadecimal se va de 0 a F antes de agregar una columna, los caracteres a través de F representan los valores decimales de 10 a través de 15, como se ilustra en la Tabla V.1.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
HEXADECIMAL	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

Tabla V.1. *Caracteres Hexadecimales de A a través de F, representan los números de 10 a través 15.*

Por lo tanto el conteo en Hexadecimal es como sigue: 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 y más, hasta donde se quiera llegar.

V.1.3 LA AUTENTICACIÓN Y CAPACIDADES DE RETIRO

IPng[1] incluye definición de extensiones que apoyan la autenticación, integridad de datos, y confidencialidad. Esto es un elemento básico de IPng y será incluido en todas las aplicaciones.

El protocolo de IPng consiste en dos partes, el título de IPng y la extensión de encabezados de IPng.

V.1.4 LAS CAPACIDADES DE QoS

Una nueva capacidad se agrego para habilitar el etiquetado de paquetes que pertenecen al "tráfico particular", para que el remitente pida un manejo especial, como la calidad del valor predeterminado de servicio o como por ejemplo, servicio de "tiempo-real" como voz.

V.1.5 EXTENSIONES DE IPV6

IPng incluye un mecanismo de mejora por encima de IPv4. Se ponen las opciones de IPng en extenciones de encabezados separados que se localizan entre el encabezado de IPng y el encabezado de la capa de transporte en un paquete. La mayoría de las extensiones de IPng no se examinan o procesan por cualquier router a lo largo del camino, desde la entrega hasta que llegue a su destino. Esto facilita una mayor eficacia en el router para los paquetes que contienen las opciones. En IPv4 la presencia de cualquier opción exigía al router examinar todas las opciones.

Las etiquetas de IPng pueden ser de longitud arbitraria y el importe global de opciones llevadas en un paquete no se limita a 40 bites; este rasgo más la manera en que ellos se procesan, permite usar las opciones de IPng para funciones que no eran prácticas para IPv4. Un ejemplo de esto es la autenticación de IPng y la seguridad en las opciones de encapsulamiento.

Las etiquetas IPng extendidas que están actualmente definidas son:

- La asignación de ruta extendida (como IPv4 la ruta de la fuente libre).
- La fragmentación
- La fragmentación y Reensamblaje.
- La autentificación
- La integridad y Autentificación.

[1] Ipng: Protocolo de Internet de la siguiente Generación (*IP next generation*)

- La Seguridad
- Encapsulación
- La confidencialidad.
- La Opción del brinco-por-brinco
- Opciones especiales que requieren el brinco por el proceso del brinco.
- Las Opciones del destino
- La información optativa a ser examinada por el nodo del destino.

V.1.6 DESCRIPCIÓN DE DIRECIONAMIENTO

Observemos un ejemplo de dirección de IPv6. La dirección es una octava parte de una dirección hexadecimal separada por dos puntos (" : "). Cada parte n puede igualar un número de 16-bits y es ocho partes más largo, proporcionando una longitud de dirección de 128-bits (16*8 = 128).

Las direcciones son los n:n:n:n:n:n:n:n n = 4 dígitos hexadecimales enteros, 16*8 = 128 direcciones.

1080:0:0:0:8:800:200C:417A dirección Unicast
FF01:0:0:0:0:0:0:101 la dirección Multicast

V.1.7 MÉTODOS DE BROADCASTING

Incluidos en IPv6 hay un número de nuevos métodos de broadcasting:

- Unicast
- Multicast
- Anycast

V.1.7.1 UNICAST

Unicast es una comunicación entre un solo host y un solo receptor, los paquetes enviados a una dirección de unicast son supervisados por una interfaz identificada por esa dirección, como se observa en la figura V.2.

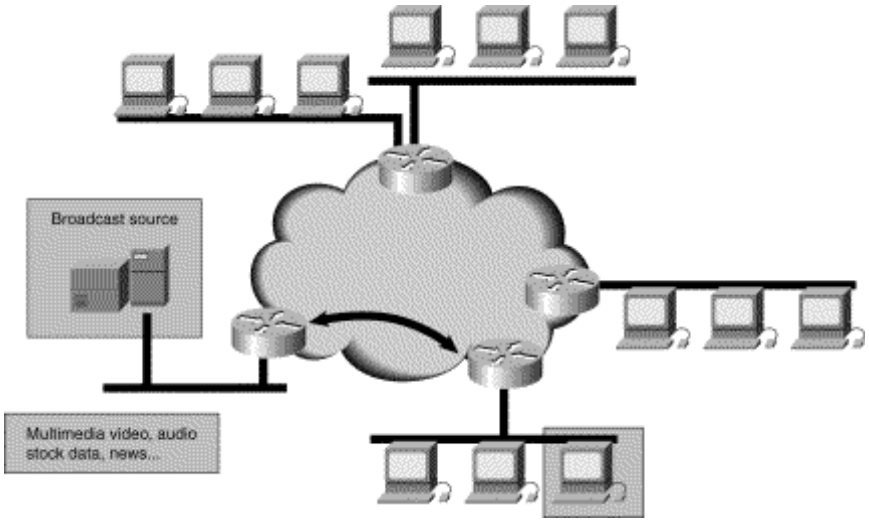


Figure V.2 *Unicast envía paquetes a una Interfaz específica*

V.1.7.2 MULTICAST

Multicast es la comunicación entre un solo host y receptores múltiples. Los paquetes son enviados a todas las interfaces identificadas por esa dirección, como se observa en la figura V.3.

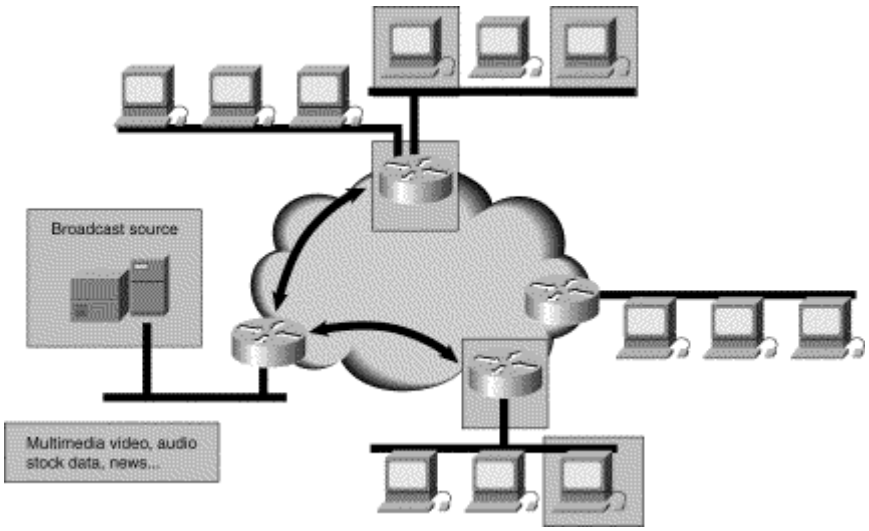


Figure V.3 *Multicast envía paquetes a la Subred,y define dispositivos específicos para los paquetes de multicast.*

V.1.7.3 ANYCAST

Los paquetes son enviados a una dirección de anycast o lista de direcciones a la interfaz más cercana identificada por dicha dirección, anycast es una comunicación

entre un solo remitente y cualquier o toda la lista de direcciones, como se muestra en la figura V.4.

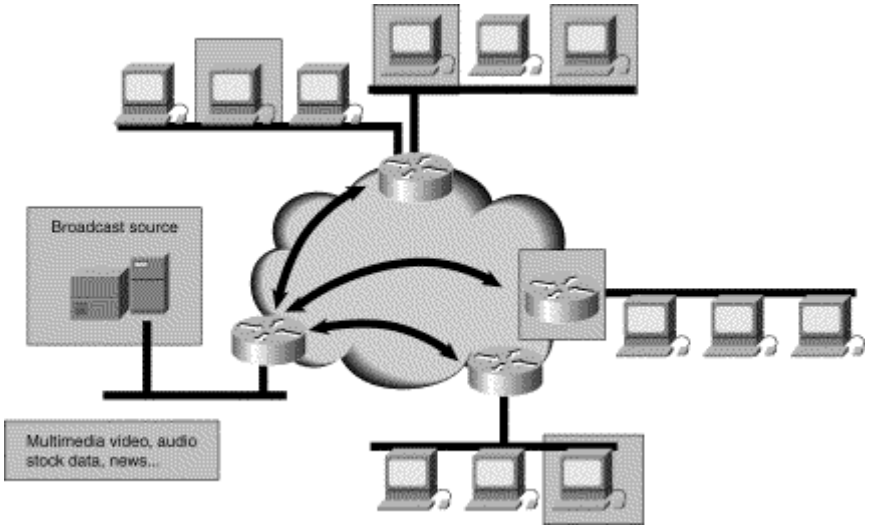


Figure V.4 *Anycast envía paquetes a una interfaz de una lista específica y puede contener nodos terminales y routers*

V.1.8 IPV.6 EN MÉXICO

V.1.8.1 OBJETIVOS

Investigar, probar e instalar IPv6 en redes de telecomunicaciones en México.

- Participar en el desarrollo de proyectos de IPv6 nacionales e internacionales.
- Participar en el fortalecimiento y difusión de IPv6 y sus aplicaciones.
- Proveer servicios de IPv6 en México y Latinoamérica.

El IETF[1] ha producido un conjunto comprensible de especificaciones (RFC 1752, 1883, 1886, 1971, 1993, etc.) que definen la siguiente generación del IP[2] conocido como " IPng " o " IPv6".

IPv6 es la versión nueva del Protocolo de Internet que está diseñada como un paso evolutivo del IPv4. Representa el fruto de muchas propuestas del IETF y de grupos de trabajo centrados en desarrollar un IPng.

[1] IETF: Fuerza de Tareas de Ingenieria de Internet (*Internet Engineering Task Force*)
[2] IP: Protocolo de Internet (*Internet Protocol*)

V.1.8.2 IPV6 EN MÉXICO

La UNAM inició investigaciones en la materia desde el mes de diciembre de 1998, fecha en la que se constituye el proyecto IPv6 en nuestra máxima casa de estudios, y durante el segundo semestre del año 1999 es notable el liderazgo de la UNAM en el ámbito nacional. Dentro del proyecto IPv6 de la UNAM se estableció un amplio programa de pruebas y trabajos con temas como: implementaciones, stacks IPv4/IPv6, túneles, software de conexión, aplicaciones multimedia, servidores para Web y DNS, autoconfiguración, calidad de servicio, IPv6 sobre ATM, conexión con redes internacionales de IPv6 (6Bone, 6REN), IPv6 en Internet2, etc.

Dentro de las primeras pruebas realizadas, destaca la de conexión a 6Bone , la cual es una red mundial experimental utilizada para probar los conceptos y la puesta en operación de IPv6. Actualmente participan en 6Bone en el ámbito mundial 47 países, entre ellos México, donde la UNAM fue el primer nodo en el país, registrándose en junio de 1999.

Posteriormente en septiembre de 1999 la UNAM fue aceptada como uno de los 68 nodos de Backbone que a la fecha operan en 6Bone, obteniendo un rango de direcciones tipo pTLA: 3ffe:8070::/28. Cabe destacar que con este hecho la UNAM es el primer nodo, y hasta el momento el único, de este tipo en México, y el tercero en Latinoamérica. Adicionalmente, la UNAM puede delegar direcciones y configurar túneles a instituciones en México y en el mundo interesadas en realizar pruebas con IPv6.

Para contar con una red de pruebas en una primera etapa, y posteriormente con una red de producción, se instaló la Red IPv6 de la UNAM, la primera red IPv6 instalada en México y que inició operaciones en agosto de 1999. Esta red cuenta con varios túneles hacia otros nodos de Backbone de 6Bone: SPRINT, FIBERTEL, MERIT, BAY NETWORKS, JANET e ISI-LAP, y hacia los hosts que tiene la UNAM corriendo con sistemas operativos como Win NT4, Win 2000, Solaris y Linux.

Actualmente se esta trabajando con instituciones mexicanas y de América Latina para realizar su conexión IPv6 hacia la UNAM.

V.1.8.3 RED UNAM IPV6 PARA PRODUCCIÓN

- Servicios de Internet basados en IPv6.
- Para usuarios en México y Latinoamérica.

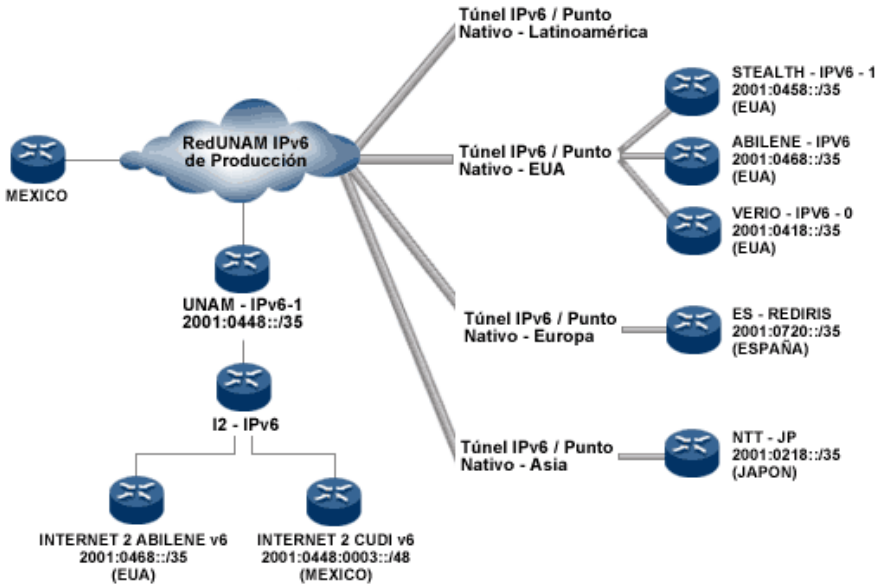


Figura V.5 *Red UNAM IPv6 de Producción.*

V.1.8.4 EN RESUMEN

Algunos de los beneficios de IPv6 parecen obvios: direccionamiento espaciado, construir en QoS, y mejor la asignación de ruteo y servicios. Sin embargo, deben superarse varias barreras antes de la aplicación de IPv6. La pregunta más grande para la mayoría de nosotros será que es lo que necesitan las empresas para mover de la actual IPv4 a IPv6. La aplicación no ha aparecido todavía, pero podría estar terminada en menos de lo que nosotros pensamos. La segunda consideración es que el costo no sería mucho en el reemplazo de hardware. Todos los routers robustos tienen la actualización en sistema operativo (ej. IOS).

Quizá la mayor dificultad sería migrar y dar menor soporte a dispositivos menores de IP como las copiadoras y faxes, pese a que IPv6 tiene los esquemas para soportar equipo viejo y nuevo. El último problema a considerar se está tratando y el cual necesitará ser solucionado pronto ya que necesitamos empezar a pensar en un direccionamiento de 128-bits basado en direcciones MAC en hexadecimal. Esto involucra nuevas formas de direccionamiento y será un cambio incómodo para mucha gente.

V.2 MPLS

V.2.1 UTILIZANDO MULTIPROTOCOLO DE CONMUTACIÓN DE ETIQUETAS PARA ENTREGA DE SERVICIOS IP

Normalmente el ruteo IP esta basado en el intercambio de información sobre una red, por medio de un protocolo de ruteo, tal como OSPF[1] u otros. Los ruteadores examinan la dirección IP destino contenida en el encabezado IP de cada paquete que es recibido, y así es utilizada la información para saber a donde enviar el paquete. Este proceso es también conocido como ***búsqueda de ruta***, el cual es ejecutado salto a salto (por cada salto existe un ruteador), a lo largo del recorrido de un paquete. Dicho proceso tiende a reducir el rendimiento en una red, debido a la intensa demanda de requerimientos de CPU para procesar cada paquete. Sin embargo algunos ruteadores implementan técnicas de conmutación por software y hardware para acelerar el proceso de evaluación y así crear entradas de cache de alta velocidad, estos métodos se basan por encima de protocolos de ruteo de Capa 3 para determinar la ruta al destinatario.

Desafortunadamente los protocolos de ruteo tienen poco, sino es que nada de visibilidad dentro de las características de Capa 2 de la red, particularmente en cuanto a QoS y carga. La gran demanda y los cambios en el tipo y cantidad de tráfico manejado por la Internet y la explosión en el número de usuarios están poniendo en un gran apuro la infraestructura de Internet, esta presión demanda nuevas y mejores soluciones de administración y maneje de tráfico. MPLS esta resolviendo muchos de los retos que envuelven a la Internet y a la comunicación de datos de alta velocidad en general.

Para satisfacer estas nuevas demandas, el *multiprotocolo de conmutación de etiquetas* (MPLS)[2] cambio el paradigma de salto a salto por el de permitir dispositivos para especificar rutas en la red basado sobre QoS y necesidades de ancho de banda para las aplicaciones. En otras palabras, la selección de rutas ahora puede tomar en cuenta los atributos de Capa 2.

[1] OSPF: Abrir la Ruta mas Corta Primero (*Open Shortest Path First*)
[2] MPLS: Multiprotocolo de Conmutación de Etiquetas (*Multiprotocol Label Switching*)

V.2.2 EL CONCEPTO DE UTILZAR ETIQUETAS COMO ENVÍO DE INFORMACIÓN

MPLS ha sido estandarizado dentro de la IETF sobre el paso de algunos años, e introduce un nuevo acercamiento para despliegue de redes IP, este separa el mecanismo de control del mecanismo de envío e introduce la "etiqueta" utilizada para el envío de paquetes.

MPLS puede ser empleado en redes de solo-ruteo o en ambientes ATM para la integración de infraestructuras de Capa 2 y Capa 3, dentro de redes IP + ATM. Una red MPLS consiste de LSRs[1] en el núcleo de la red y LSRs-frontera rodeando la red, como se muestra en la figura V.7.

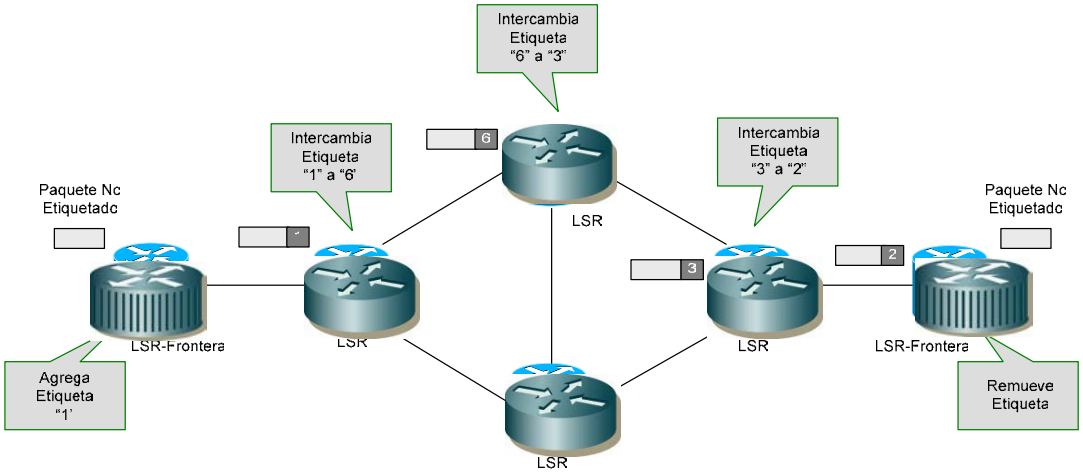


Figura V.6 *El LSR Frontera esta etiquetando en el lado de ingreso para que sea utilizada la etiqueta por el LSR en el núcleo para enviar el tráfico a través del camino deseado y será removida por el LSR Frontera de lado de salida*

Dentro de la red de MPLS, el tráfico es enviado utilizando etiquetas. Los LSRs-Frontera del lado de ingreso de la nube de MPLS son responsables de asignar la etiqueta y enviar el paquete al próximo salto o LSR a lo largo del camino que el tráfico sigue a través de la nube de MPLS. Todos los LSRs a lo largo del camino utilizan la etiqueta como un índice dentro de una tabla que mantiene la información del próximo salto y una nueva etiqueta. La vieja etiqueta es intercambiada con la nueva etiqueta desde la tabla y el paquete es enviado al próximo salto. Utilizar este método implica que el valor de la etiqueta es únicamente de significado local entre dos LSRs. Del lado de salida de la red, la etiqueta es removida y el tráfico es enviado, utilizando mecanismos normales de protocolos de ruteo IP.

[1] LSR: Ruteador Conmuta Etiquetas (*Label Switch Router*)

V.2.3 DEFINICIÓN DE TÉRMINOS UTILIZADOS POR MPLS

A continuación se muestran los conceptos y definiciones básicas que se utilizan por MPLS.

Etiqueta: Un encabezado creado por un LSR-Frontera y utilizado por el LSR de núcleo para el envío de paquetes. El formato del encabezado varía según el tipo de red. Por ejemplo, en una red ATM, la etiqueta tiene colocados campos de VPI/VCI en cada encabezado de celda ATM, en una ambiente LAN, el encabezado es un separador localizado en el encabezado entre Capa 2 y Capa 3.

Base de Información de Reenvío de Etiquetas (LFIB): Es una tabla creada por un dispositivo capas de conmutar etiquetas (LSR) que indica donde y como es enviado un paquete con un valor de etiqueta especifico.

Ruteador Conmuta Etiquetas (LSR): Es un dispositivo tal como un switch o un router que envía entidades etiquetadas basadas sobre valores de etiquetas.

Ruteador Conmuta Etiquetas Frontera (LSR-Frontera): Es el dispositivo que inicia agregando o termina removiendo la etiqueta del paquete.

Etiqueta Conmutada: Cuando un LSR hace una decisión de envío basada sobre la presencia de etiquetas en la trama/celda.

Camino de Etiqueta-Conmutada (LSP): El camino definido por la etiqueta a través de LSRs entre puntos finales.

Etiqueta de Circuito Virtual (LVC): Un LSP a través de un sistema ATM.

Control de Etiqueta Conmutada (LSC): Un LSR que comunica con un switch ATM para proveer y abastecer información de etiquetas dentro del switch.

Protocolo de Distribución de Etiquetas (LDP): Conjunto de mensajes definidos para distribuir información de etiquetas entre LSRs.

XmplsATM: Es la interfaz virtual entre un switch ATM y un LSC.

V.2.4 ARQUITECTURA DE MPLS

MPLS se basa sobre dos componentes principales: reenvío y control. El ***componente de reenvío*** utiliza etiquetas llevadas por los paquetes y la Base de Información de Reenvío de Etiquetas es mantenida por un LSR para ejecutar el

reenvío de paquetes, dicha decisión de reenvío esta basada en un algoritmo de correspondencia-exacta utilizando longitud-fija como un índice. Esto permite simplificar el procedimiento de reenvío, así como incrementar el desempeño de reenvío (muchos paquetes por segundo).

El ***componente de control*** es responsable de mantener la información correcta en la LFIB entre un grupo de LSRs interconectados. El componente de control crea ligas de etiquetas que son distribuidas entre los LSRs utilizando el Protocolo de Distribución de Etiquetas (LDP).

V.2.4.1 PROTOCOLOS DE DISTRIBUCIÓN DE ETIQUETAS

Con el ruteo basado en destino, un ruteador hace decisiones de reenvío basado en direcciones destino de Capa 3, llevadas en un paquete, la información almacenada en la base de información de reenvío (FIB) es mantenida por el ruteador el cual construye esta FIB para usar la información que recibe el ruteador proveniente de los protocolos de ruteo, tales como OSPF y BGP.

Para soportar el ruteo basado en destino con MPLS, un LSR participa con los protocolos de ruteo y construye la LFIB para utilizar la información que es recibida desde los protocolos. En este sentido este opera mas como un ruteador.

Un LSR sin embargo, debe distribuir y utilizar etiquetas localizadas por el LSR par para enviar correctamente la trama a los LSRs distribuyendo etiquetas utilizando un Protocolo de Distribución de Etiquetas (LDP). Una etiqueta mantiene asociado un destino de subred para una etiqueta de significado local (las etiquetas son de significado local por que estas son reemplazadas en cada salto). Siempre que un LSR descubre un LSR vecino, los dos establecen una conexión TCP para mantener la transferencia de etiquetas. LDP intercambia etiquetas/subred utilizando uno o dos métodos: cauce descendiente no solicitado, distribución o cauce descendiente sobre demanda. Ambos LSRs debe acordar que modo utilizar.

V.2.5 APLICACIONES BASADAS EN MPLS

Actualmente el mercado de telecomunicaciones se esta orientando a que los proveedores de servicio traten de crear y vender soluciones con valores agregados para que los clientes puedan hacer uso de los distintos servicios y estar a un paso delante de la cadena de valores. La oportunidad para los proveedores de servicios de ofrecer servicios de VPN basados sobre IP, tal como VPNs BGP/MPLS, hace de esta una tecnología muy atractiva para el mercado. Esto también explica un pequeño

pedazo de "exageración comercial" por MPLS que puede verse en el mercado en los últimos dos años. En nuestro punto de vista, esto no es una visible desaceleración.

La aplicación mas empleada por MPLS es la VPN MPLS. Una típica red VPN MPLS se muestra en la figura V-7. el ruteador de acceso del cliente, también llamado ruteador de ***cliente fronterizo*** (CE[1]), es conectado a los LSRs Frontera, actuando como ruteadores proveedores frontera (PE[2]).

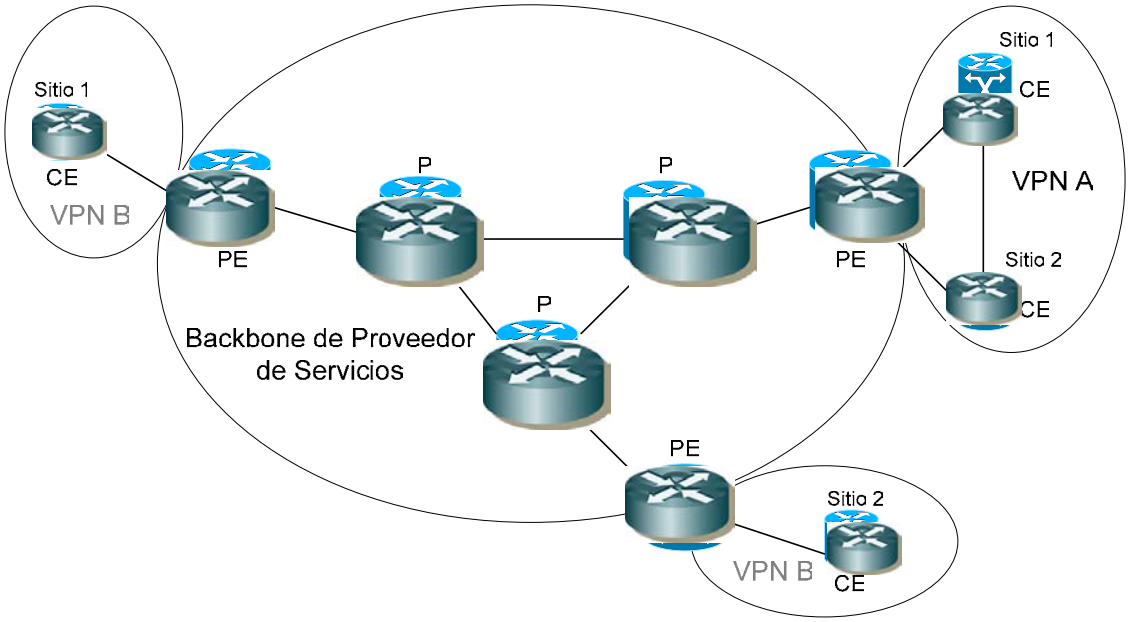


Figura V.7 *VPNs MPLS-Los ruteadores PE utilizan la pila de etiquetas para determinar a cual VPN pertenece la información de ruteo y el tráfico*

Los ruteadores PE asignan dos etiquetas a cada paquete. Una etiqueta representa el identificador de VPN, y la etiqueta superior es utilizada para enviar el paquete a través de la red. Los LSRs en el núcleo de la red son llamados ruteadores proveedores (P) y estos ejecutan conmutación estándar de etiquetas utilizando la etiqueta superior. El ruteador PE en el lado de salida de la red, remueve ambas etiquetas y utiliza la segunda de estas para determinar a cual CE (VPN) el paquete deberá ser enviado.

La segunda aplicación que hace uso del hecho que el componente de control esta completamente separado del componente de reenvío. Los protocolos de ruteo estándar computan el camino opcional desde una fuente a un cierto destino, considerando una métrica de ruteo tal como conteo de saltos, costo, o ancho de banda del enlace. Como resultado, un costo mínimo es elegido. Sin embargo este puede ser un camino alternativo, solo uno es seleccionado por el protocolo de ruteo

[1] CE: Cliente Fronterizo (*Customer Edge*)
[2] PE: Proveedor Fronterizo (*Provider Edge*)

para utilizarse para llevar trafico. Esto conduce a una ineficiente utilización de los recursos de red.

Ingeniería de trafico MPLS (MPLS-TE) introduce el termino ***troncal de trafico***, en el cual un grupo de flujo de trafico con los mismo requerimientos, tal como confiabilidad o prioridad de trafico. MPLS-TE provee manejo de trafico IGP, calculando rutas funcionalmente basado sobre troncal-por-trafico. Otro que al igual que los protocolos estándar de ruteo es manejado por: la topología, utilización de los recursos de la red y atributos de confiabilidad, todo esto es analizado y tomado en cuenta durante la programación del camino. Como se muestra en la figura V.8, múltiples caminos son posibles de un origen a un destino y el mejor es elegido, de acuerdo a la situación actual de la red, asegurando la utilización optima de la red.

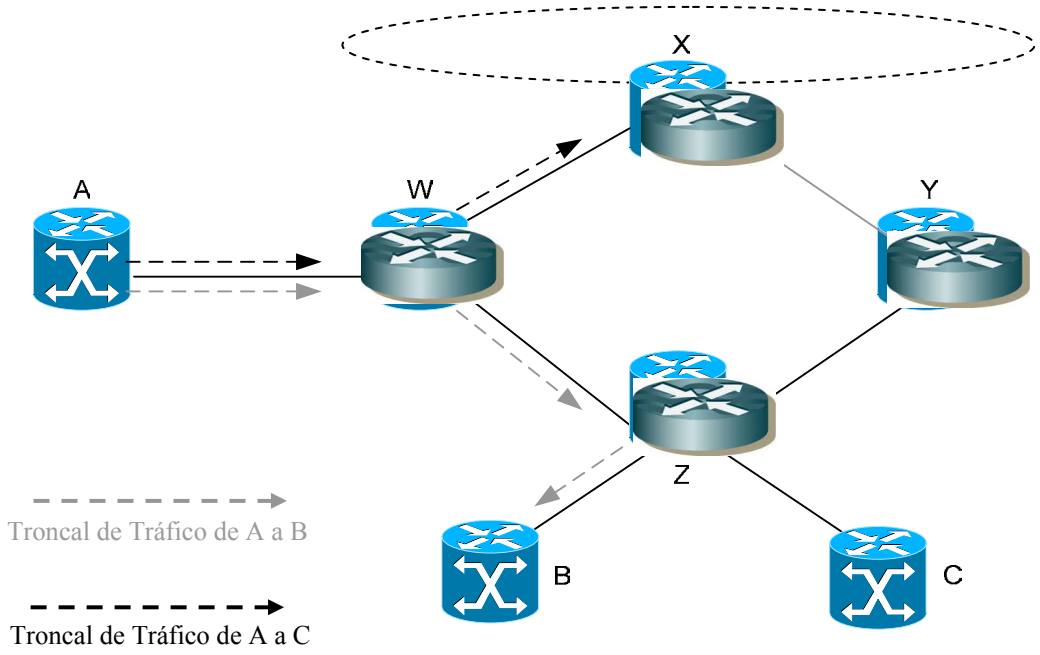


Figura V.8 *Ingeniería de Trafico MPLS provee la habilidad de definir y optimizar el camino que será tomado por el tráfico a través de la red*

V.3 PWE3

PWE3[1] es un mecanismo que emula los atributos esenciales de un servicio como una línea alquilada T1, ATM, Frame Relay o Ethernet sobre una red conmutada de paquetes (PSN[2]). Las funciones requeridas de los PWs[1] incluyen el encapsulado de

[1] PWE3 Emulación de Pseudo Cable punto a punto (*Pseudo Wire Emulation Edge to Edge)*
[2] PSN Red de Paquete Conmutado (*Paquet Switched Network)*

servicios-específicos PDUs[2] que llegan a un puerto de ingreso y son llevados a través de un camino o túnel, administrando su tiempo y orden, y cualquier otra operación requerida para emular el comportamiento y características del servicio tan fielmente como sea posible.

Para la perspectiva de los compradores, el PW es percibido como un enlace no compartido o un circuito del servicio elegido. Sin embargo, hay características que impiden que algunas aplicaciones puedan ser transportadas en un PW. Estas limitantes son y deben ser descritas apropiadamente en cada documento del servicio-especifico.

V.3.1 FUNCIONES ESPECÍFICAS

PWs proveen las siguientes funciones para emular el comportamiento y características de los servicios deseados

- Encapsulacion del servicio especifico PDUs o circuito de datos que llegan al puerto de entrada (lógico o físico)
- Transporte de los datos encapsulados a través de un túnel.
- Administración de la señalización, tiempo, ordenamiento y otros aspectos del servicio en la frontera del PW
- Servicios específicos status de la señalización y administración de alarmas

V.3.2 ARQUITECTURA DE LA RED ACTUAL

Las secciones siguientes se dan algunos antecedentes como son las redes de hoy y por qué estas están cambiando. También hablaremos sobre la motivación para proveer redes que converjan mientras continúan soportando los servicios existentes. Finalmente se discutirá cómo los PWs pueden ser una solución a este dilema.

V.3.2.1 MÚLTIPLES REDES

Para cualquier proveedor de servicios dado que entrega servicios múltiples, su infraestructura actual consiste normalmente de varias redes paralelas o redes

[1] PWs Pseudo Cable *(Pseudo Wire)*
[2] PDUs Unidad Protocolar de Dato (*Protocol Data Unit)*

"*overlay*" (redes revestidas). Cada una de estas redes ofrece un servicio específico, como Frame Relay, acceso a Internet, etc. Esto es bastante costoso, tanto por lo que se refiere al gasto de capital como en gastos de operación. Además, la presencia de redes múltiples complica la planificación. Los proveedores de servicio terminan haciéndose estas preguntas:

¿Cual de mis redes dejare fuera?
¿Cuántas fibras yo necesito para cada red?
¿Cómo manejar eficientemente las múltiples redes?

Una red convergente ayuda a los proveedores de servicio a contestarse estas preguntas en una consistente y económica forma.

V.3.2.2 TRANSICIÓN A UNA RED DE CONVERGENCIA DE PAQUETES-OPTIMIZADOS

Para aumentar al máximo la recuperación de sus capitales, y minimizar los costos de operación, los proveedores de servicio a menudo buscan consolidar la entrega de múltiples tipos de servicio dentro de una simple tecnología de red.

Cuando el tráfico de paquetes es grande y ocupa una gran cantidad de ancho de banda, este llega a ser progresivamente provechoso para optimizar las redes públicas para el Protocolo de Internet. Sin embargo, muchos proveedores de servicio están confrontando grandes obstáculos en la ingeniería de redes de paquetes –optimizados. Aunque el tráfico de Internet es el segmento de tráfico con el mayor crecimiento acelerado, este no genera el mayor capital por bit. Por ejemplo, el tráfico de Frame Relay es el que actualmente genera las mayores rentas por bit a diferencia de lo que hace un servicio nativo de IP. Los servicios de líneas privadas TDM todavía generan aun más réditos por bit que los servicios de Frame Relay. En adición hay una gran cantidad de equipo heredado y desarrollado dentro de las redes públicas que no se comunica utilizando el Protocolo de Internet. Los proveedores de servicios continúan utilizando este equipo no-IP para dar una variedad de servicios, y ven una necesidad de interconectar su este equipo heredado con sus principales redes IP optimizadas.

V.3.3 PWE3 COMO UN CAMINO A LA CONVERGENCIA

Los proveedores de servicio se hacen preguntas de como evaluar cuenta el capital y los beneficios de operación de una nueva infraestructura basada en

paquetes, mientras se hace uso del equipo existente y como proteger la recuperación por flujo de canal asociado con este nuevo equipo ó bien como migrar de las maduras redes ATM y Frame Relay, mientras estas todavía son capaces de proveer lucrativos servicios.

Una posibilidad a todas estas preguntas es la emulación de circuitos o servicios vía PWs.

La emulación sobre ATM y la interconexión de Frame Relay y ATM todavía sigue siendo estandarizado. La emulación permite que los servicios existentes sean transportados a través de la nueva infraestructura, y así sea posible la interconexión de redes distintas. Implementar correctamente, PWE3 puede proveer un medio para soportar los servicios de hoy en día sobre una nueva red.

V.3.4 APLICACIONES ADAPTABLES PARA PWE3

Cuando consideramos ó queremos utilizar a los PWs como una manera para proporcionar una aplicación, las siguientes preguntas deben ser consideradas.

- ¿Es la aplicación es suficientemente desarrollada para garantizar la emulación?
- ¿Hay interés de la parte de los proveedores de servicio en proveer una emulación para la aplicación dada?
- ¿Hay interés de parte de los manufactureros del equipo en proveer productos para la emulación de una aplicación dada?
- ¿Hay complicaciones y limitaciones para proveer una emulación que valga la pena ahorrar capital y ahorrar en gastos de operación?

Si la respuesta a todas las preguntas fue si, entonces la aplicación es muy probable a ser un buen candidato para PWE3. De otra manera, no habrá suficientes coincidencias entre los consumidores, proveedores de servicio, desarrolladores de equipo y tecnología que garantice una emulación.

V.3.5 REFERENCIA DEL MODELO DE PWE3

Un pseudo cable (PW) es una conexión entre las dos puntas del aparato del proveedor los cuales están conectados un circuito adjunto (AC[1]). Un AC puede ser

[1] AC : Circuito Adjunto *(Attachment Circuit)*

un DLCI de Frame Relay, un VPI/VCI de ATM, un puerto Ethernet, una VLAN, un enlace HDLC, una conexión PPP o una interfase física, una sesión PPP por un túnel de L2TP, un LSP de MPLS, etc.

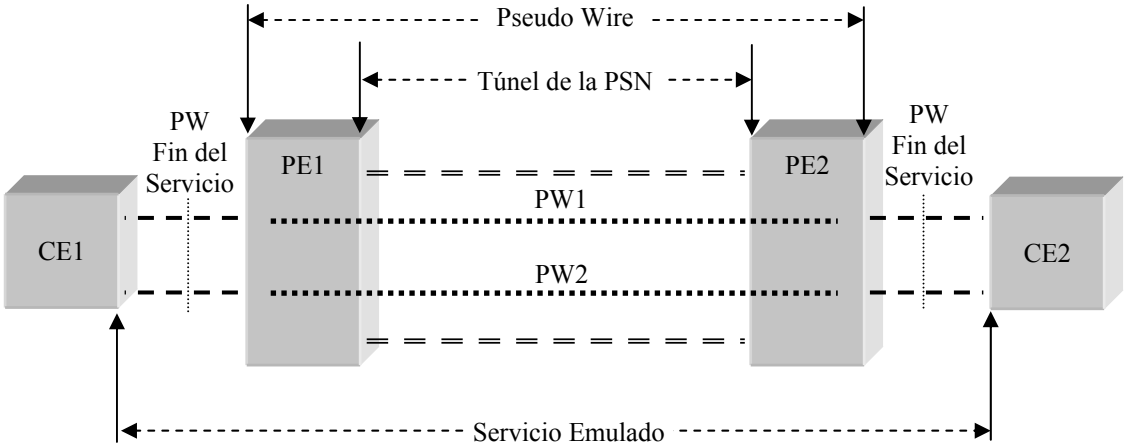


Figura V.9 Modelo de Referencia de PWE3

Durante la configuración de un PW, los 2 PE[1]s pueden ser configurados o serán configurados de manera automática, cambiando información sobre el servicio que será emulado para que después estos sepan procesar los paquetes que vienen del otro lado. Después un PW es configurado entre los dos PEs, los frames recibidos por un PE para un AC serán encapsulados y enviados sobre el PW al PE remoto, donde los frames nativos serán reconstruidos y reenviados al otro CE[2].

V.3.6 PROCESAMIENTO DEL PAQUETE

Esta sección describe brevemente los requisitos de los datos para poder ser considerados dentro de un PWE3.

V.3.6.1 ENCAPSULACIÓN

Todo PE debe proveer un mecanismo de encapsulacion para los PDUs de un AC. Estos deben notarse que los PDUs a encapsular pueden o no contener la información de encabezado L2. Este es el servicio específico. Cada servicio PWE3 debe especificar que PDUs es.

[1] PE : Proveedor Fronterizo (*Provider Edge*)
[2] CE : Cliente Fronterizo (*Customer Edge*)

Un encabezado PW consiste de todos los campos de encabezados en un PW PDU que son usados por el PW salida para determinar como procesar el PDU. La el encabezado del túnel en la PSN no es considerado como parte del encabezado del PW.

TRANSPORTE DE INFORMACIÓN NECESARIA DEL ENCABEZADO L2

La salida de un PW necesita alguna información, por ejemplo, a que servicio nativo pertenecen los PW PDUs, y posiblemente algo de información del encabezado L2, para saber como procesar los PDUs recibidos. Una encapsulacion PWE3 debe proveer algún mecanismo para el transporte con información semejante para el PW de entrada como para el PW de salida. Debe notarse que no toda la información debe ser llevada en el encabezado del PW PDUs

Alguna información (como el tipo de servicio de un PW) puede ser guardado como una información de estado a la salida durante la configuración del PW.

SOPORTE DE PDUS DE LONGITUD VARIABLE

Un PWE3 debe acomodar los PDUs de longitud Variable, si los PDUs de longitud variable son soportados por el servicio nativo. Por ejemplo, un PWE3 para Frame Relay debe acomodar los frames de longitud variable.

SOPORTE DE MULTIPLEXACION Y DEMULTIPLEXACION

Si un servicio en su forma nativa es capaz de agrupar múltiples circuitos en un enlace, por ejemplo múltiples ATM VCCs en un VPC o múltiples interfaces Ethernet 802.1Q en un puerto, algunos mecanismos debe proveer que un simple PW pueda ser usado para conectar dos puntas en el enlace. Desde la perspectiva de encapsulacion, suficiente información debe ser llevada para que la salida del PW pueda demultiplexar los circuitos individuales del PW.

VALIDACIÓN DE PW-PDU

La mayoría de los Frames L2 tienen un campo de detección de errores para asegurar la integridad del frame. Cada servicio PWE3 debe especificar si los *checksum* del frame deben ser preservados a través del PW, o deben ser removidos al ingresar al PE y entonces sean recalculados e insertados a la entrada del PE. Para protocolos como ATM y Frame Relay, el *checksum* solo cubre solo información del enlace local como los identificadores del circuito (por ejemplo DLCI o VPI/VCI). Por consiguiente, el *checksum* puede ser removido por el PE de ingreso y recalculado por el PE de salida.

TRANSMISIÓN DE TIPO DE INFORMACIÓN ÚTIL (PAYLOAD)

Bajo algunas circunstancias es deseable poder distinguir el tráfico PW de otros tipos de trafico como IPv4 o IPv6 o OAM. Por ejemplo, si *Equal Cost Multi-Paht* (ECMP) es ocupado en una PSN, esta adicional capacidad de distinguir puede ser usada para reducir la posibilidad de que los paquetes del PW sean extraviados por el mecanismo de balanceo de cargas. Algunos mecanismos deben proveer la capacidad si es necesario.

V.3.6.2 ORDENAMIENTO DE FRAMES

Cuando los paquetes llevan los PWPDUs atraviesan un PW, estos pueden llegar a la salida fuera de orden, para algunos servicios, los frames deben llegar en orden. Para estos servicios algunos mecanismos deben de asegurar la entrega en orden, proveyendo un número de secuencia en el encabezado del PW para cada paquete o mecanismos de reordenamiento de los frames.

V.3.6.3 DUPLICACIÓN DE FRAMES

En casos raros, los paquetes que atraviesan un PW pueden ser duplicados. Para algunos servicios, la duplicación de frames no esta permitida, Para estos servicios algunos mecanismos deben asegurar que no se entreguen estos frames duplicados. El mecanismo puede o no ser el mismo mecanismo que asegura la entrega en orden de los paquetes.

V.3.6.4 FRAGMENTACIÓN

Si el tamaño combinado de la carga útil del L2, su asociado PWE3 y los encabezados PSN exceden el MTU de la PSN, la carga útil del LS debe ser fragmentada. Con seguridad el servicio nativo, la fragmentación también necesitara mantener el control de la relativa posición de los frames de datos. En general, la fragmentación tiene un impacto en el funcionamiento, es por consiguiente deseable evitar la fragmentación si es posible. Sin embargo, para diferentes servicios, la necesidad de fragmentación debe ser diferente. Cuando hay potencial necesidad de fragmentación, cada servicio especifico PWE3 debe especificar cuando fragmentar el frame en cuestión o dejarlo.

V.3.6.5 CONSIDERACIONES DE SOBRE ENCABEZADO POR PAQUETE DE LA PSN

Cuando el tamaño del L2 PDU es pequeño, para reducir el encabezado del túnel de la PSN múltiples PDUs pueden ser concatenados en un encabezado añadido al túnel de la PSN. Cada PDUs encapsulado puede llevar su propio encabezado PW que el PE de salida el proceso de este. Sin embargo, los beneficios de concatenar múltiples PDUs para eficientar el encabezado debe evaluarse son el incremento del retrato, jitter y sobre todo los riesgos que se corren si se pierde el paquete.

V.3.7 CONSIDERACIONES EXTRAS

En general hay mucho mas consideraciones que son consideradas para proporcionar un PWE3 pero depende de cada servicio que se desea emular, y el cual debe ser especificado en su propio estándar como son la administración, mantenimiento, configuración, verificación, fidelidad, seguridad, calidad de servicio, etc. características que dependen de cada uno de los servicios a ser emulados.

V.3.8 EN RESUMEN

Para maximizar la recuperación de sus gastos y minimizar los gastos de operación, muchos proveedores de servicios están buscando consolidar el desarrollo de múltiples servicios ofrecidos y tipos de tráfico en una simple red IP optimizada.

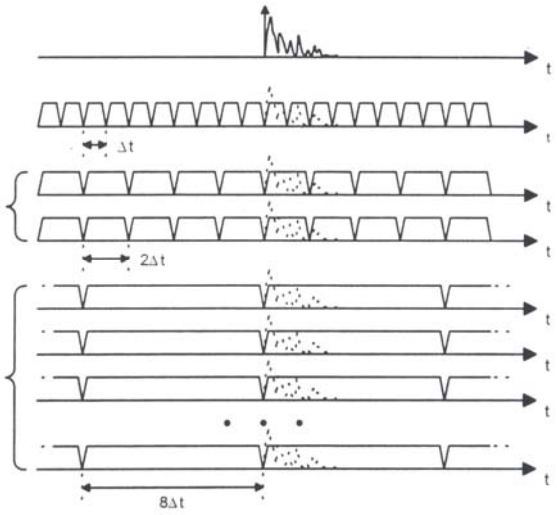
En consecuencia para crear esta nueva generación de redes convergentes, los métodos de estandarización deben ser desarrollados para emular los existentes formatos de telecomunicaciones como Ethernet, Frame Relay y ATM sobre una Red Principal de IP optimizada

V.4 OFDM

El principio básico de OFDM[1] es dividir un flujo de datos de alta velocidad en varios flujos de menor tasa de datos los cuales se transmiten simultáneamente sobre subportadoras a diferentes frecuencias. Como la duración del símbolo se incrementa

[1] OFDM: Multiplexacion Ortogonal por División de Frecuencia (*Orthogonal Frequency Division Multiplexing*)

al tener subportadoras paralelas de más baja velocidad, la cantidad de dispersión relativa en el tiempo causada por el retraso de las multitrayectorias disminuye. La interferencia intersímbolo (ISI, *InterSymbol Interfernece*) se elimina casi completamente mediante la introducción de un intervalo de guarda antes de cada símbolo OFDM. Durante el intervalo de guarda el símbolo se extiende cíclicamente para evitar la interferencia intersímbolo.



FiguraV.10 *El efecto de adoptar un sistema multiportadora*

OFDM en un caso especial de transmisión por multiportadora, donde una sola fuente de datos se transmite sobre un número finito de subportadoras de baja velocidad. Vale la pena mencionar aquí que OFDM puede ser visto tanto como una técnica de modulación como una técnica de multiplexación ya que una sola o varias fuentes de información pueden modular a las subportadoras. Una de las principales razones para utilizar OFDM es su inherente protección contra el desvanecimiento por selectividad de frecuencias o interferencia de banda angosta. En un sistema con una sola portadora, un solo desvanecimiento o interferencia causa el rompimiento completo del enlace, pero en un sistema de multiportadora sólo será afectado un pequeño porcentaje de subportadoras. La codificación para corrección de errores puede ser usada entonces para corregir las portadoras erróneas.

OFDM tiene las siguientes ventajas clave:

- OFDM es una manera eficiente de abatir los efectos de las multitrayectorias. Para una distribución de retardos dada, por ejemplo la de la figura V.11, la complicidad de implementación que significativamente menor comparada con la de un sistema de portadora única con un ecualizador.
- OFDM es un esquema robusto contra la interferencia de banda angosta por dicha interferencia afecta sólo un pequeño porcentaje de las subportadoras.

- OFDM hace posible implementar redes de frecuencia única (SFN, *Single Frecuency Networks*) lo cual especialmente atractivo para aplicaciones de difusión masiva.

Por otro lado. OFDM también tiene algunas desventajas comparado con los esquemas de portadora única

- OFDM es más sensible a las desviaciones de frecuencia y el ruido de fase.
- OFDM tiene una gran relación prepotencia pico bajo precio promedio, lo que tiende a reducir la eficiencia del amplificador de radiofrecuencia.

En un sistema clásico de datos en paralelo la banda total de frecuencias se divide en N subcanales los cuales encuentran sin traslapes. Cada subcanal se modula por separado y luego los N subcanales son multiplexados en frecuencia (FDM). Bajo este esquema es necesario evitar el traslapes espectral de los subcanales para prevenir la interferencia intercanal; sin embargo, esto conlleva aún uso ineficiente del espectro disponible debido a la introducción de banda de guarda. Para contrarrestar estas ineficiencia, las ideas propuestas a mediados de la década de los sesentas fueron utilizar datos en paralelo y FDM con subcanales traslapados, en donde cada portadora un ancho de banda *B* y las portadoras están espaciadas *B/2* en el dominio de la frecuencia para evitar el uso de ecualización de alta velocidad, compartir el ruido impulsivo y la distorsión por un trayectoria, así como incrementar la eficiencia del ancho de banda disponible.

En la figura V.11 se muestra la diferencia entre la técnica convencional de multiportadoras no traslapadas y la técnica de modulación con multiportadoras traslapadas. Sin embargo, para implementar éste técnica es necesario angular de interferencia entre las subportadoras, es decir, que las subportadoras sean ortogonales entre sí.

La palabra ortogonal indica que existe una relación matemática específica entre las frecuencias de las portadoras en el Sistema. En un sistema de multiplexación por división de frecuencias (FDM) normal, las portadoras son espaciadas de tal manera que las señales puedan ser recibidas utilizando filtros y de modula errores convencionales por lo que son introducidas bandas de guarda entre portadoras en el dominio de la frecuencia.

Sin embargo, es posible ordenar las subportadoras en un sistema OFDM de tal manera sus bandas laterales se traslapes y aún así sean recibidas sin interferencia de portadora adyacente. Para llevar a cabo esto las subportadoras deben ser matemáticamente ortogonales.

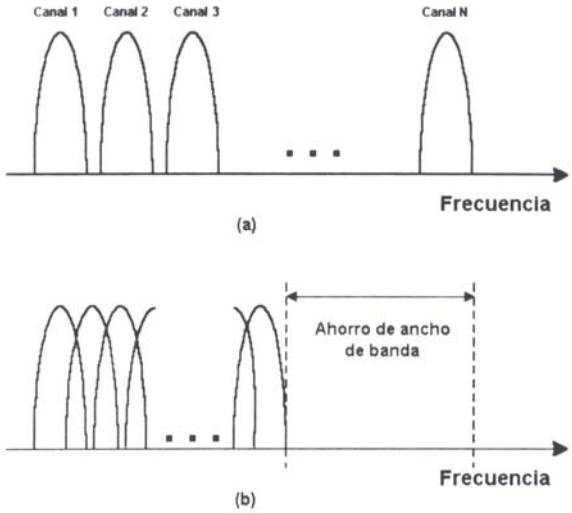


Figura V.11 *Concepto de señal OFDM: (a) Técnica convencional de multiportadora FDM. (b) Técnica de modulación con multiportadoras ortogonales.*

V.4.1 DESCRIPCIÓN OFDM

El estándar IEEE802.11a define la capa física que adopta una modulación OFDM. La capa física de OFDM provee la capacidad para transmitir frames PDU a velocidades superiores a los 54Mbps para redes WLAN donde las transmisiones de contenido multimedia es considerable.

V.4.1.1 SUBCAPA PLCP PARA OFDM

El PPDU es único en la capa física para una modulación OFDM. El PPDU consiste de un preámbulo PLCP y un campo de signal data como se muestra en la figura

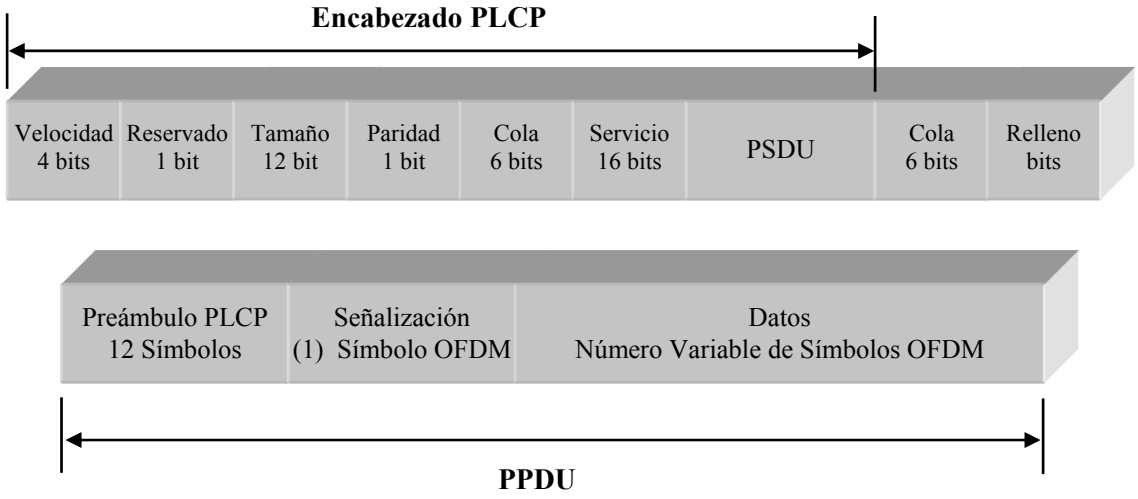


Figura V.12 *Encabezado del PLCP para OFDM*

El receptor usa el preámbulo PLCP para obtener la señal entrante de OFDM y sincronizar el demodulador. EL encabezado PLCP contiene la información acerca del PSDU de la señal enviada de OFDM. El preámbulo PLCP y el campo de *signal* son siempre trasmitidos a 6Mbps, con una modulación BPSK- OFDM modulada usando un código convolucional R=1/2

PLCP preámbulo. Este campo es usado para obtener la señal entrante y el tren de pulsos y sincronizar el receptor. EL preámbulo consiste de 12 símbolos, diez de los cuales son pequeños símbolos, y dos son largos símbolos. Los símbolos cortos son usados para preparar el AGC (*Automatic Gain Control*) y obtener un a aproximación de la frecuencia portadora y el canal. Los símbolos largos son usados para mejorar la sintonización de la frecuencia y la estimación del canal.

Doce subportadoras son usadas para los símbolos cortos y 53 para largos. La preparación del canal OFDM es completado en 16μs. El PLCP preámbulo es modulado por BPSK-OFDM a 6Mbps.

Signal. Es un campo de 24 bits, el cual contiene información acerca de la tasa y longitud del PSDU. EL campo de signal es un código convolucional ½, modulado con BPSK-OFDM. Para cuatro bits (R1 – R4) son usado una codificar la velocidad, 11bits son usados para la longitud, un bit es reservado, un bit de paridad, y seis “0s” son la cola. Los bits que definen la velocidad se muestran en la tabla siguiente

Velocidad	Modulación	Tasa de Codificación	Bits de Señalización (R1 – R4)
6 Mbps	BPSK	R = ½	1101
9 Mbps	BPSK	R = ¾	1111
12 Mbps	QPSK	R = ½	0101
18 Mbps	QPSK	R = ¾	0111
24 Mbps	16QAM	R = ½	1001
36 Mbps	16QAM	R = ¾	1011
48 Mbps	64QAM	R = 2/3	0001
54 Mbps	64QAM	R = ¾	0011

Tabla V.2 *Configuraciones Posibles para los Bits del Campo de Señalización*

La velocidad e transmisión obligatoria para la IEEE 802.11a para los sistemas es de 6Mbps, 12Mbps, y 24 Mbps.

Length Este campo es un número anónimo de 12-bits que indica el número de octetos en el PSDU.

Data. El campo de datos contiene el campo de servicio, PSDU bits de cola y bits de ensamblado. Un total de seis bits de cola contienen "0s" que son adjuntados al PPDU para asegurar que la codificación convolucional vuelva a un estado de cero.

V.4.1.2 MEZCLADOR DE DATOS

Todos los bits transmitidos por la subcapa PDM en una porción de saltos son mezclados usando un frame sincrono 127-bit de una secuencia generadora. La mezcla es usada para aleatorizar el servicio, PSDU, bit de relleno y patrón de datos, los cuales pueden contener largas cadenas de 1s o 0s. Los bits de cola no son mezclados.

V.4.2 MODULACIÓN OFDM

OFDM es un método escogido por la IEEE 802.11a similar a la técnica adoptada en Europa por el ETSI HIPERLAN II en la banda de 5GHz.

El principio básico de operación es dividir las señales binarias de alta velocidad, para ser transmitidas en una tasa menor por diferentes subportadoras. Hay 48 subportadoras de datos y 4 subportadoras piloto para tener un total de 52. Cada stream es modulado por separado en una diferente subportadora de los diferentes canales en la banda de 5GHz.

La interferencia intersimbolo no se presenta generalmente en portadoras de baja velocidad, pero desvanecimiento por interferencia entre canales, es por eso que la interpolación de los bits y un código convolucional son usados para mejorar el funcionamiento del canal.

Para esto se utilice la técnica de OFDM en la cual cada subportadora es ortogonal a la otra. Ahora cada PPDU primeramente es codificado usando un código convolucional r=1/2, y los bits son reordenados. Cada bit es mapeado a un número complejo de acuerdo al tipo de modulación y subdividido en 48 subportadoras de datos y 4 pilot subportadoras. Las subportadoras son combinadas usando una inversa transformada rápida de Fourier y transmitidos. En el receptor, la portadora es convertida nuevamente a multiportadoras de baja velocidad para usar la FFT. Las subportadoras de baja velocidad son combinadas para obtener nuevamente una PPDU de alta velocidad.

Un ejemplo de un sistema IEEE802.11a es ilustrado en la siguiente figura.

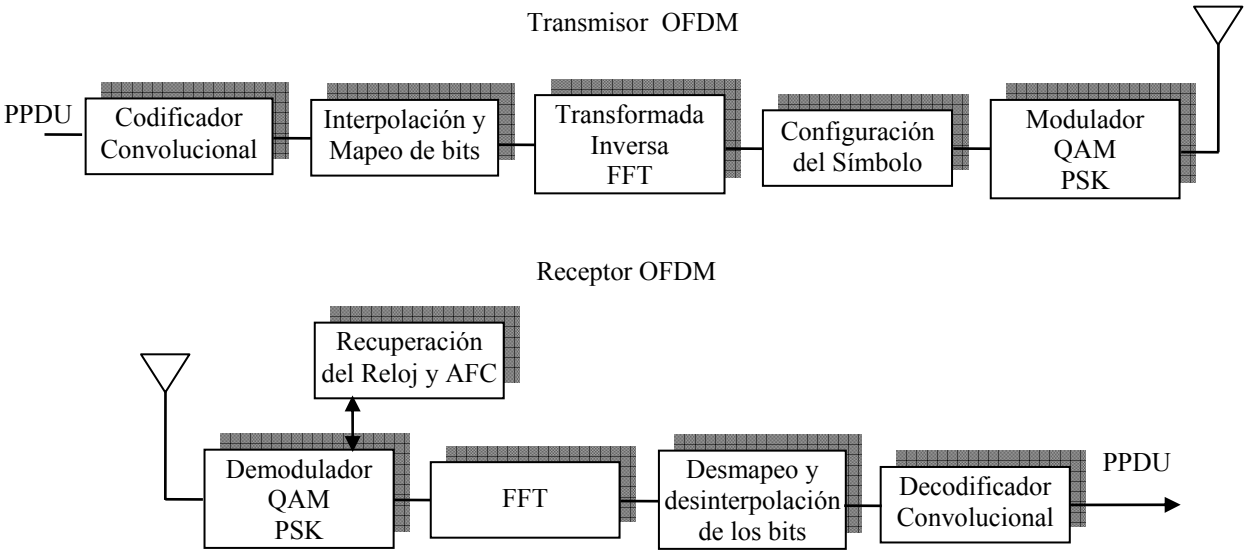


Figura V.13 *Transmisor y Receptor para OFDM*

V.4.3 OPERACIÓN DE CANAL PARA OFDM

La banda de 5GHz es dividida en 3 bandas de 100MHz que van de los 5.15-5.25 Ghz, de los 5.25-5.35GHZ y de los 5.725-5.825 GHZ. Las potencias también son especificadas y son de 40 mW, 200 mW, y 800mW.

V.5 VPN (REDES PRIVADAS VIRTUALES)

V.5.1 INTRODUCCIÓN

En los últimos años las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital, por tanto dichas redes cumplen con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Como ya se ha visto en la actualidad, las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones, sobre todo las que cuentan con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia, es por eso que escuchamos hablar tanto de los famosos firewalls y las VPNs[1]

V.5.2 POR QUÉ UTILIZAR UNA VPN

Cuando se desea enlazar oficinas centrales con alguna sucursal u oficina remota se tienen tres opciones:

1. Modem: Las desventajas es el costo de la llamada, ya que el costo de esta llamada sería por minuto conectado, además sería una llamada de larga distancia, a parte de que no contaría con la calidad, velocidad y seguridad adecuadas.
2. Línea Privada: Tendría que tender mi cable ya sea de cobre o fibra óptica de un punto a otro, en esta opción el costo es muy elevado porque si por ejemplo necesito enlazar mi oficina central con una sucursal que se encuentra a 200

[1] VPN: Red Privada Virtual (*Virtual Private Network*)

Kilómetros de distancia el costo sería por la renta mensual por Kilómetro. Sin importar el uso.

3. VPN: Los costos son bajos porque solo realizo llamadas locales, además de tener la posibilidad de que mis datos viajen encriptados y seguros, con una buena calidad y velocidad.

V.5.3 ¿QUE ES UNA VPN?

Una VPN es una red privada que se extiende mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos, a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte de datos.

Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública. (ver figura V.15)

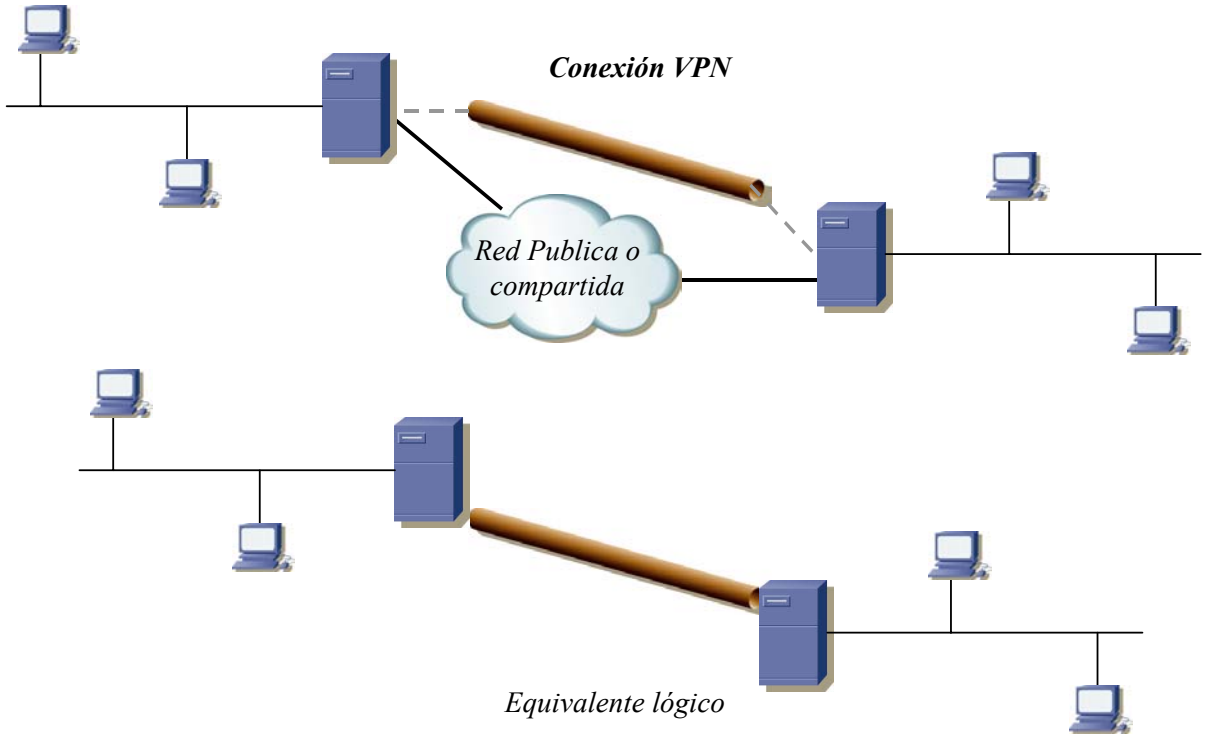


Figura V.14 Conexión de una VPN

En la figura V.14 se muestra como viajan los datos a través de una VPN ya que el servidor dedicado es del cual parten los datos, llegando a un firewall que hace la función de una pared para engañar a los intrusos a la red, después los datos llegan a la nube de Internet donde se genera un túnel dedicado únicamente para nuestros

datos donde se garantiza la velocidad y ancho de banda para así lleguen a su vez al firewall remoto y terminen en el servidor remoto.

Figura V.15 *Como funciona una VPN*

Las VPN pueden enlazar por ejemplo, oficinas corporativas con socios, con usuarios móviles, con oficinas remotas, mediante los protocolos como Internet, IP, Ipsec, Frame Relay, ATM, etc. como lo muestra la figura V.16.

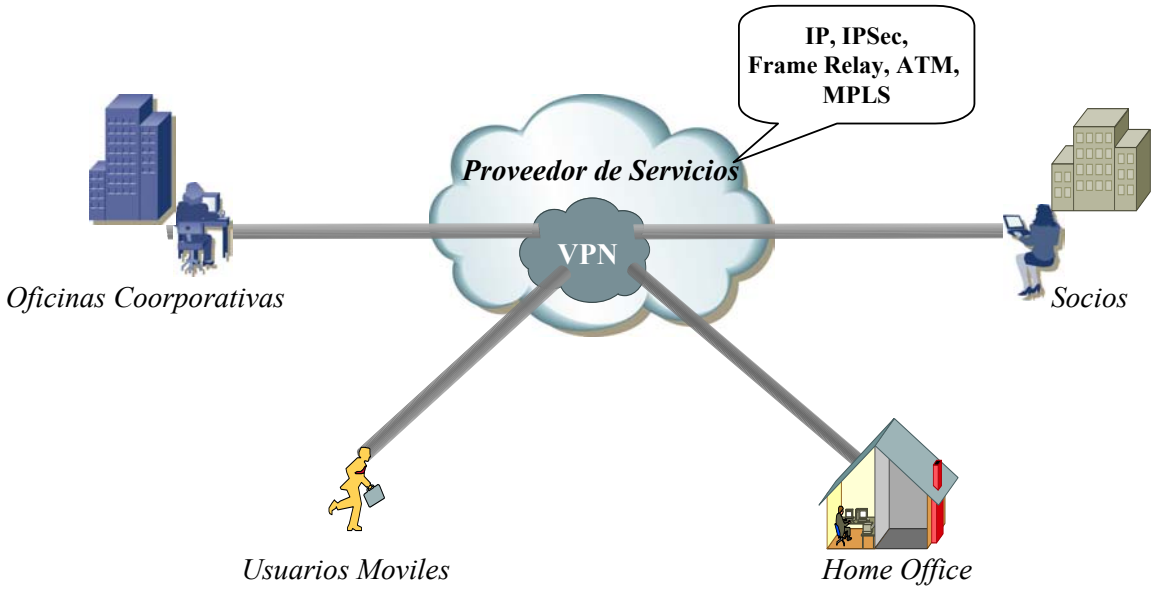


Figura V.16 *Ejemplos de enlaces con VPNs*

V.5.4 TECNOLOGÍA DE TÚNEL

Las redes privadas virtuales crean un túnel o conducto de un sitio a otro para transferir datos a esto se le conoce como encapsulación además los paquetes van encriptados de forma que los datos son ilegibles para los extraños que intentan

interceptarlos. El servidor busca mediante un ruteador la dirección IP del cliente VPN en la red de transito a donde se envían los datos sin problemas.

V.5.5 REQUERIMIENTOS BÁSICOS DE UNA VPN

Por lo general cuando se desea implementar una VPN hay que asegurarse que esta posea:

- Identificación de usuario
- Administración de direcciones
- Codificación de datos
- Administración de claves
- Soporte a protocolos múltiples

V.5.5.1 IDENTIFICACIÓN DE USUARIO

La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien acceso, cuando y que información manejo.

V.5.5.2 ADMINISTRACIÓN DE DIRECCIONES

La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

V.5.5.3 CODIFICACIÓN DE DATOS

Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

V.5.5.4 ADMINISTRACIÓN DE CLAVES

La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

V.5.5.5 SOPORTE A PROTOCOLOS MÚLTIPLES

La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de Internet "IP", el Intercambio de paquete de Internet "IPX", entre otros.

V.5.6 COMPONENTES DE UNA VPN

Los dispositivos que generalmente conforman un entorno con VPNs son los siguientes:

- VPN gateway
- Software
- Firewall
- Router
- Dispositivos con un software y hardware especial para proveer de capacidad a la VPN
- Software

V.5.7 VENTAJAS DE UNA VPN

Dentro de las ventajas más significativas podemos mencionar:

- La integridad, confidencialidad y seguridad de los datos.
- Reducción de costos.
- Sencilla de usar.
- Sencilla instalación del cliente en cualquier PC Windows, Unix, Linux, etc.
- Control de acceso basado en políticas de la organización
- Herramientas de diagnostico remoto.
- Los algoritmos de compresión optimizan el tráfico del cliente.
- Evita el alto costo de las actualizaciones y mantenimiento a las PC´s remotas.

V.5.8 CONCLUSIÓN

Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se han vuelto

un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro, el único inconveniente que pudieran tener las VPN es que primero se deben establecer correctamente las políticas de seguridad y de acceso porque si esto no esta bien definido pueden existir consecuencias serias.

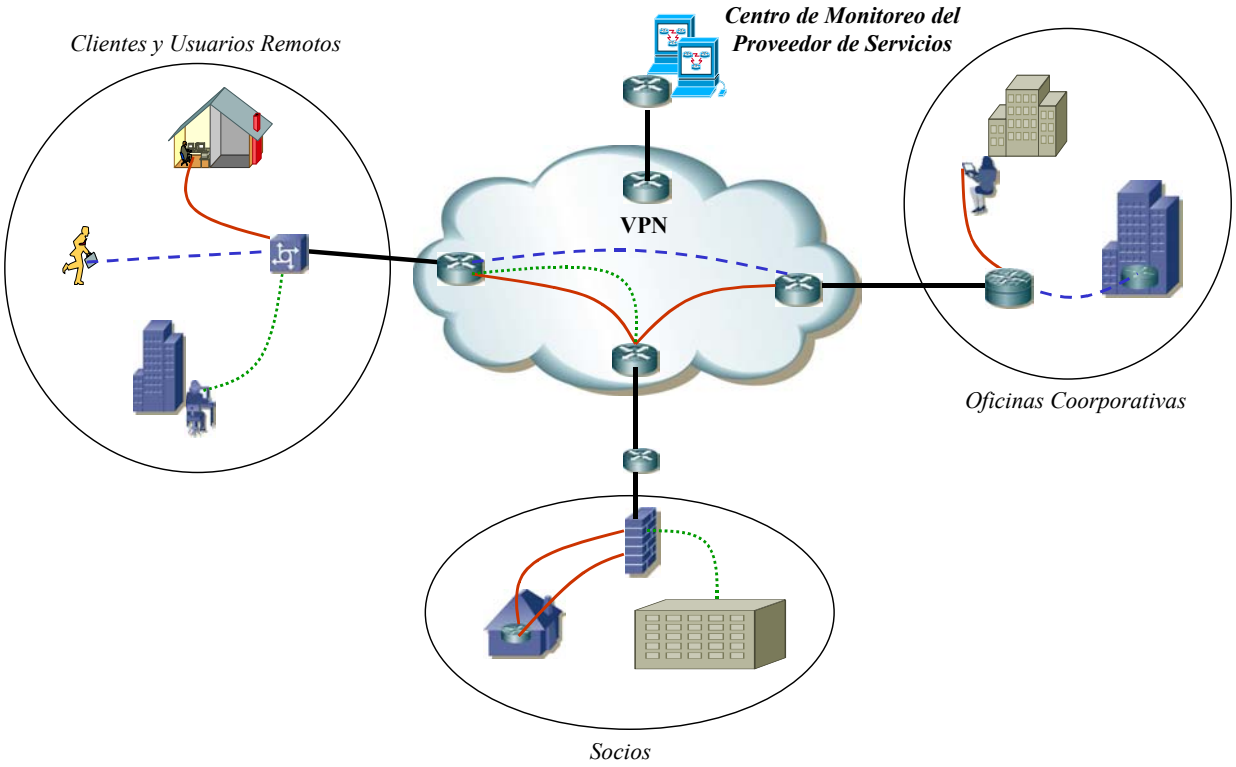


Figura V.17 *Ejemplo de una red implementando VPNs*

V

NUEVAS TECNOLOGÍAS EN SISTEMAS DE TRANSMISIÓN DE INFORMACIÓN

V.1 IPV6

Uno de los nuevos estándares que se están implementando es IPv6. Aunque aun no se ha introducido oficialmente como un estándar, debido a que este se encuentra todavía en observación, por lo cual es muy posible que esta información este sujeta a cambios. Para efecto de la tesis se considerará IPv6[1] como un estándar, pero se debe aclarar que esta información no es definitiva.

Algunos libros se han publicado para describir más a detalle este estándar emergente, así como todos los RFC[2]s disponibles en Internet tienen información detallada de como se esta desarrollando, así como sus avances.

[1] IPv6: Protocolo de Internet Versión 6 (*Internet Protocol V. 6*)
[2] RFC: Petición de Comentarios *(Request for Comments)*

IPv4[1] en la actualidad es el protocolo mas usado, aunque genera preguntas sobre su capacidad de desempeño dentro de la comunidad de Internet, IPv4 fue elaborado en los años setenta y ha empezado a mostrar las debilidades de su edad. El problema principal de IPv4 es la falta de direccionamiento, porque muchos expertos creen que estamos superando las casi cuatro mil millones de direcciones disponibles. Aunque esto parece como un número muy grande de direcciones, múltiples bloques de gran tamaño son dados a las agencias gubernamentales y a las grandes organizaciones. Por lo cual IPv6 podría ser la solución a muchos problemas, pero todavía no se desarrolla ni se estandariza totalmente.

IPv6 fue recomendado por los directores del área de IPng del *Internet Engineering Task Force* en la reunión del IETF de Toronto el 25 de julio de 1994, el RFC 1752, es la recomendación para el protocolo de la generación siguiente del IP, dicha recomendación fue aprobada por el *Internet Engineering Steering Group* e hizo un estándar el 17 de noviembre de 1994.

IPv6 fue hecho un estándar de bosquejo del IETF el 10 de agosto de 1998. La versión 6 del Protocolo de Internet se abrevia IPv6 (donde el "6" refiere es la versión número 6). La versión anterior del Protocolo de Internet es la 4 (designada IPv4).

IPv6 es una nueva versión de IP que fue diseñada para ser un paso evolutivo de IPv4. Puede ser instalado como mejora del software en dispositivos de Internet y es interoperable con el IPv4 actual. IPv6 se diseño para funcionar en redes de alto rendimiento (ej. Gigabit-Ethernet, etc.) y al mismo tiempo que sea eficiente para las redes de bajo ancho de banda. Además, proporciona una plataforma para la nueva funcionalidad de Internet que será requerida en un futuro.

IPv6 incluye un mecanismo de transición que permite que los usuarios adopten y desplieguen IPv6 de una manera altamente difusa y que proporcionen interoperabilidad directa entre los usuarios de IPv4 e IPv6. La transición a una nueva versión del Protocolo de Internet debe ser incremental, con pocos o ningunas interdependencias críticas.

Muchos de los diseñadores más capacitados han estado con IPv6 desde inicios de los 90s, cientos de RFCs han sido escritos y han detallado algunas de las áreas más importantes, incluyendo direccionamiento expandido, formato de encabezado simplificado, etiquetado de flujo, autenticación y privacidad.

El direccionamiento expandido nos mueve desde una dirección de 32-bits a una de 128-bits a través del método de direccionamiento. También proporciona nuevos métodos unicast y de broadcasting, inyecta notación hexadecimal en las direcciones

[1] IPv4: Protocolo de Internet Versión 4 (*Internet Protocol V. 4*)

IP y se mueve de usuario a usuario con delimitadores, la figura V.1 muestra el formato de paquete de encabezado de IPv6.

Figure V.1 *Formato de Paquete de Encabezado de IPv6.*

V.1.1 DESCRIPCIÓN DE PAQUETE DE ENCABEZADO

El encabezado simplificado es de una longitud de 40 bits y el formato consiste en versión, clase, etiqueta de flujo, longitud de la carga útil, siguiente encabezado, límite de salto, dirección de la fuente, dirección de destino, datos, y campos de la carga útil.

V.1.2 HEXADECIMAL "HEX"

Simplificadamente, los números hexadecimales están en base 16. El decimal es base 10, contando de 0 a 9 y agregando una columna para hacer 10. Contando en hexadecimal se va de 0 a F antes de agregar una columna, los caracteres a través de F representan los valores decimales de 10 a través de 15, como se ilustra en la Tabla V.1.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
HEXADECIMAL	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

Tabla V.1. *Caracteres Hexadecimales de A a través de F, representan los números de 10 a través 15.*

Por lo tanto el conteo en Hexadecimal es como sigue: 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 y más, hasta donde se quiera llegar.

V.1.3 LA AUTENTICACIÓN Y CAPACIDADES DE RETIRO

IPng[1] incluye definición de extensiones que apoyan la autenticación, integridad de datos, y confidencialidad. Esto es un elemento básico de IPng y será incluido en todas las aplicaciones.

El protocolo de IPng consiste en dos partes, el título de IPng y la extensión de encabezados de IPng.

V.1.4 LAS CAPACIDADES DE QoS

Una nueva capacidad se agrego para habilitar el etiquetado de paquetes que pertenecen al "tráfico particular", para que el remitente pida un manejo especial, como la calidad del valor predeterminado de servicio o como por ejemplo, servicio de "tiempo-real" como voz.

V.1.5 EXTENSIONES DE IPV6

IPng incluye un mecanismo de mejora por encima de IPv4. Se ponen las opciones de IPng en extenciones de encabezados separados que se localizan entre el encabezado de IPng y el encabezado de la capa de transporte en un paquete. La mayoría de las extensiones de IPng no se examinan o procesan por cualquier router a lo largo del camino, desde la entrega hasta que llegue a su destino. Esto facilita una mayor eficacia en el router para los paquetes que contienen las opciones. En IPv4 la presencia de cualquier opción exigía al router examinar todas las opciones.

Las etiquetas de IPng pueden ser de longitud arbitraria y el importe global de opciones llevadas en un paquete no se limita a 40 bites; este rasgo más la manera en que ellos se procesan, permite usar las opciones de IPng para funciones que no eran prácticas para IPv4. Un ejemplo de esto es la autenticación de IPng y la seguridad en las opciones de encapsulamiento.

Las etiquetas IPng extendidas que están actualmente definidas son:

- La asignación de ruta extendida (como IPv4 la ruta de la fuente libre).
- La fragmentación
- La fragmentación y Reensamblaje.
- La autentificación
- La integridad y Autentificación.

[1] Ipng: Protocolo de Internet de la siguiente Generación (*IP next generation*)

- La Seguridad
- Encapsulación
- La confidencialidad.
- La Opción del brinco-por-brinco
- Opciones especiales que requieren el brinco por el proceso del brinco.
- Las Opciones del destino
- La información optativa a ser examinada por el nodo del destino.

V.1.6 DESCRIPCIÓN DE DIRECIONAMIENTO

Observemos un ejemplo de dirección de IPv6. La dirección es una octava parte de una dirección hexadecimal separada por dos puntos (" : "). Cada parte n puede igualar un número de 16-bits y es ocho partes más largo, proporcionando una longitud de dirección de 128-bits (16*8 = 128).

Las direcciones son los n:n:n:n:n:n:n:n n = 4 dígitos hexadecimales enteros, 16*8 = 128 direcciones.

1080:0:0:0:8:800:200C:417A dirección Unicast
FF01:0:0:0:0:0:0:101 la dirección Multicast

V.1.7 MÉTODOS DE BROADCASTING

Incluidos en IPv6 hay un número de nuevos métodos de broadcasting:

- Unicast
- Multicast
- Anycast

V.1.7.1 UNICAST

Unicast es una comunicación entre un solo host y un solo receptor, los paquetes enviados a una dirección de unicast son supervisados por una interfaz identificada por esa dirección, como se observa en la figura V.2.

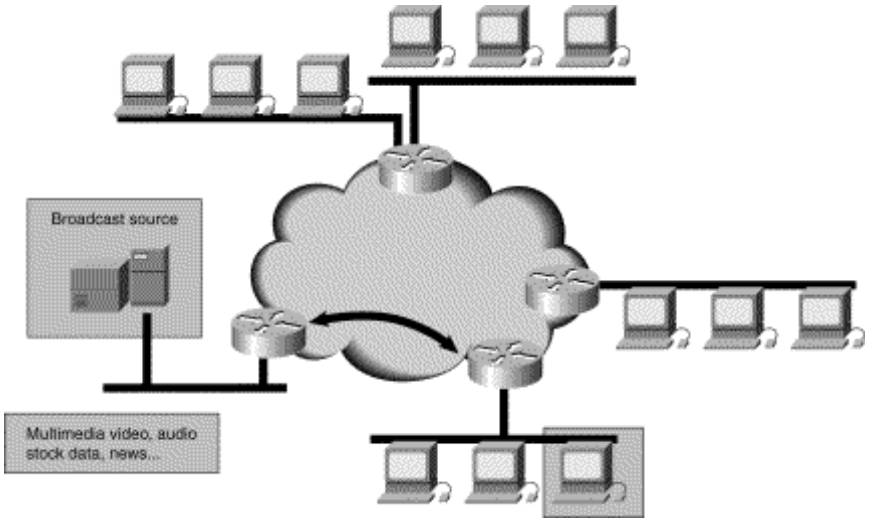


Figure V.2 *Unicast envía paquetes a una Interfaz específica*

V.1.7.2 MULTICAST

Multicast es la comunicación entre un solo host y receptores múltiples. Los paquetes son enviados a todas las interfaces identificadas por esa dirección, como se observa en la figura V.3.

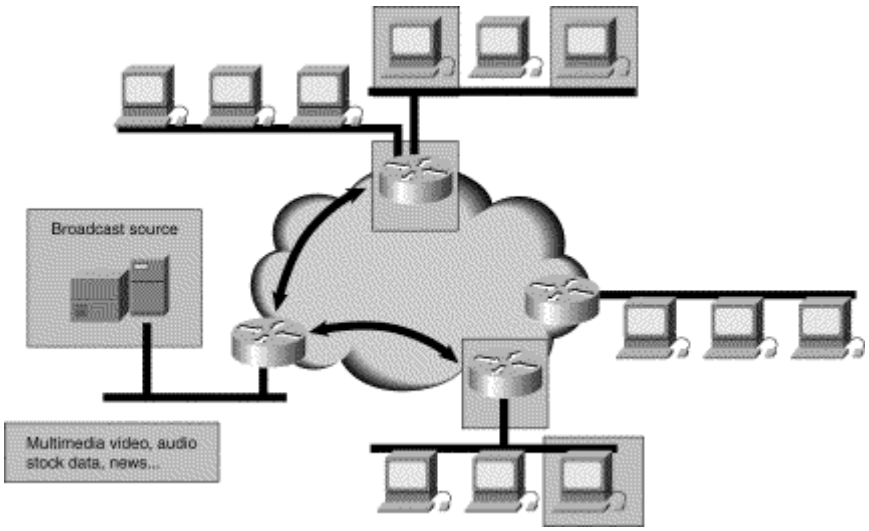


Figure V.3 *Multicast envía paquetes a la Subred,y define dispositivos específicos para los paquetes de multicast.*

V.1.7.3 ANYCAST

Los paquetes son enviados a una dirección de anycast o lista de direcciones a la interfaz más cercana identificada por dicha dirección, anycast es una comunicación

entre un solo remitente y cualquier o toda la lista de direcciones, como se muestra en la figura V.4.

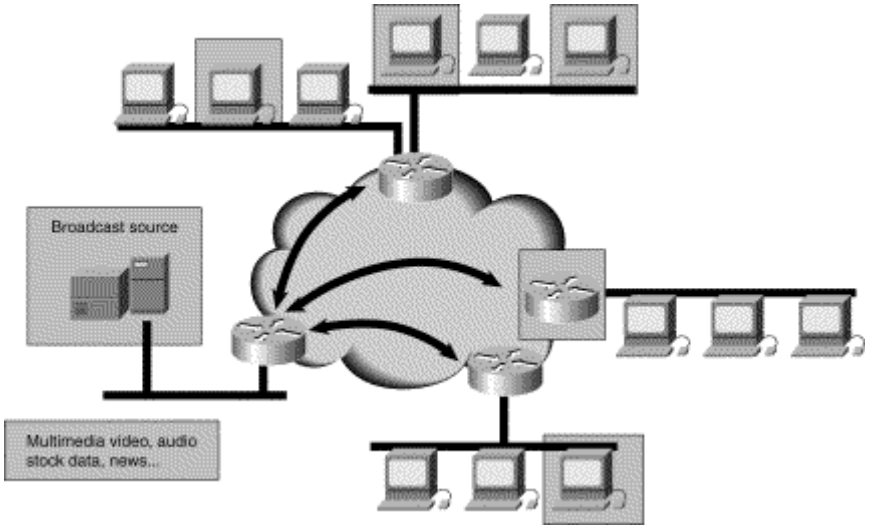


Figure V.4 *Anycast envía paquetes a una interfaz de una lista específica y puede contener nodos terminales y routers*

V.1.8 IPV.6 EN MÉXICO

V.1.8.1 OBJETIVOS

Investigar, probar e instalar IPv6 en redes de telecomunicaciones en México.

- Participar en el desarrollo de proyectos de IPv6 nacionales e internacionales.
- Participar en el fortalecimiento y difusión de IPv6 y sus aplicaciones.
- Proveer servicios de IPv6 en México y Latinoamérica.

El IETF[1] ha producido un conjunto comprensible de especificaciones (RFC 1752, 1883, 1886, 1971, 1993, etc.) que definen la siguiente generación del IP[2] conocido como " IPng " o " IPv6".

IPv6 es la versión nueva del Protocolo de Internet que está diseñada como un paso evolutivo del IPv4. Representa el fruto de muchas propuestas del IETF y de grupos de trabajo centrados en desarrollar un IPng.

[1] IETF: Fuerza de Tareas de Ingenieria de Internet (*Internet Engineering Task Force*)
[2] IP: Protocolo de Internet (*Internet Protocol*)

V.1.8.2 IPV6 EN MÉXICO

La UNAM inició investigaciones en la materia desde el mes de diciembre de 1998, fecha en la que se constituye el proyecto IPv6 en nuestra máxima casa de estudios, y durante el segundo semestre del año 1999 es notable el liderazgo de la UNAM en el ámbito nacional. Dentro del proyecto IPv6 de la UNAM se estableció un amplio programa de pruebas y trabajos con temas como: implementaciones, stacks IPv4/IPv6, túneles, software de conexión, aplicaciones multimedia, servidores para Web y DNS, autoconfiguración, calidad de servicio, IPv6 sobre ATM, conexión con redes internacionales de IPv6 (6Bone, 6REN), IPv6 en Internet2, etc.

Dentro de las primeras pruebas realizadas, destaca la de conexión a 6Bone , la cual es una red mundial experimental utilizada para probar los conceptos y la puesta en operación de IPv6. Actualmente participan en 6Bone en el ámbito mundial 47 países, entre ellos México, donde la UNAM fue el primer nodo en el país, registrándose en junio de 1999.

Posteriormente en septiembre de 1999 la UNAM fue aceptada como uno de los 68 nodos de Backbone que a la fecha operan en 6Bone, obteniendo un rango de direcciones tipo pTLA: 3ffe:8070::/28. Cabe destacar que con este hecho la UNAM es el primer nodo, y hasta el momento el único, de este tipo en México, y el tercero en Latinoamérica. Adicionalmente, la UNAM puede delegar direcciones y configurar túneles a instituciones en México y en el mundo interesadas en realizar pruebas con IPv6.

Para contar con una red de pruebas en una primera etapa, y posteriormente con una red de producción, se instaló la Red IPv6 de la UNAM, la primera red IPv6 instalada en México y que inició operaciones en agosto de 1999. Esta red cuenta con varios túneles hacia otros nodos de Backbone de 6Bone: SPRINT, FIBERTEL, MERIT, BAY NETWORKS, JANET e ISI-LAP, y hacia los hosts que tiene la UNAM corriendo con sistemas operativos como Win NT4, Win 2000, Solaris y Linux.

Actualmente se esta trabajando con instituciones mexicanas y de América Latina para realizar su conexión IPv6 hacia la UNAM.

V.1.8.3 RED UNAM IPV6 PARA PRODUCCIÓN

- Servicios de Internet basados en IPv6.
- Para usuarios en México y Latinoamérica.

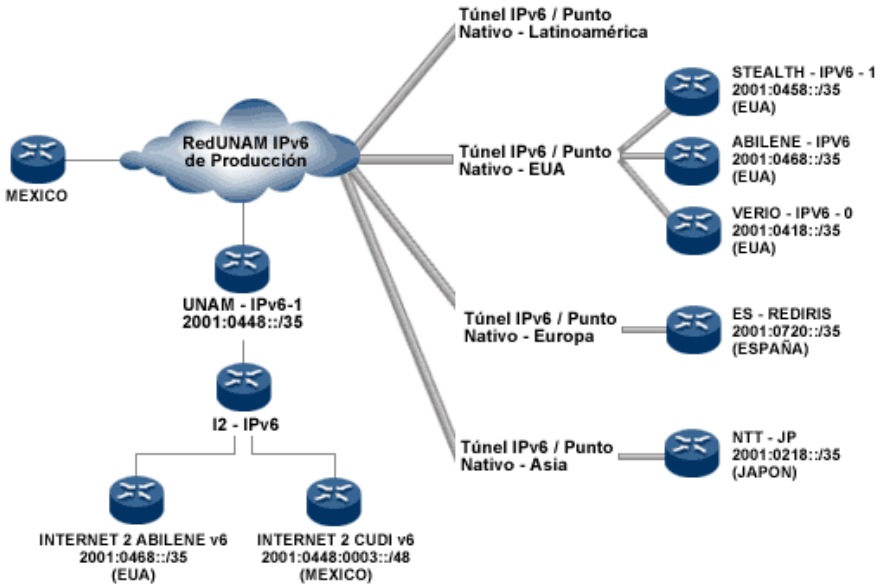


Figura V.5 *Red UNAM IPv6 de Producción.*

V.1.8.4 EN RESUMEN

Algunos de los beneficios de IPv6 parecen obvios: direccionamiento espaciado, construir en QoS, y mejor la asignación de ruteo y servicios. Sin embargo, deben superarse varias barreras antes de la aplicación de IPv6. La pregunta más grande para la mayoría de nosotros será que es lo que necesitan las empresas para mover de la actual IPv4 a IPv6. La aplicación no ha aparecido todavía, pero podría estar terminada en menos de lo que nosotros pensamos. La segunda consideración es que el costo no sería mucho en el reemplazo de hardware. Todos los routers robustos tienen la actualización en sistema operativo (ej. IOS).

Quizá la mayor dificultad sería migrar y dar menor soporte a dispositivos menores de IP como las copiadoras y faxes, pese a que IPv6 tiene los esquemas para soportar equipo viejo y nuevo. El último problema a considerar se está tratando y el cual necesitará ser solucionado pronto ya que necesitamos empezar a pensar en un direccionamiento de 128-bits basado en direcciones MAC en hexadecimal. Esto involucra nuevas formas de direccionamiento y será un cambio incómodo para mucha gente.

V.2 MPLS

V.2.1 UTILIZANDO MULTIPROTOCOLO DE CONMUTACIÓN DE ETIQUETAS PARA ENTREGA DE SERVICIOS IP

Normalmente el ruteo IP esta basado en el intercambio de información sobre una red, por medio de un protocolo de ruteo, tal como OSPF[1] u otros. Los ruteadores examinan la dirección IP destino contenida en el encabezado IP de cada paquete que es recibido, y así es utilizada la información para saber a donde enviar el paquete. Este proceso es también conocido como ***búsqueda de ruta***, el cual es ejecutado salto a salto (por cada salto existe un ruteador), a lo largo del recorrido de un paquete. Dicho proceso tiende a reducir el rendimiento en una red, debido a la intensa demanda de requerimientos de CPU para procesar cada paquete. Sin embargo algunos ruteadores implementan técnicas de conmutación por software y hardware para acelerar el proceso de evaluación y así crear entradas de cache de alta velocidad, estos métodos se basan por encima de protocolos de ruteo de Capa 3 para determinar la ruta al destinatario.

Desafortunadamente los protocolos de ruteo tienen poco, sino es que nada de visibilidad dentro de las características de Capa 2 de la red, particularmente en cuanto a QoS y carga. La gran demanda y los cambios en el tipo y cantidad de tráfico manejado por la Internet y la explosión en el número de usuarios están poniendo en un gran apuro la infraestructura de Internet, esta presión demanda nuevas y mejores soluciones de administración y maneje de tráfico. MPLS esta resolviendo muchos de los retos que envuelven a la Internet y a la comunicación de datos de alta velocidad en general.

Para satisfacer estas nuevas demandas, el *multiprotocolo de conmutación de etiquetas* (MPLS)[2] cambio el paradigma de salto a salto por el de permitir dispositivos para especificar rutas en la red basado sobre QoS y necesidades de ancho de banda para las aplicaciones. En otras palabras, la selección de rutas ahora puede tomar en cuenta los atributos de Capa 2.

[1] OSPF: Abrir la Ruta mas Corta Primero (*Open Shortest Path First*)
[2] MPLS: Multiprotocolo de Conmutación de Etiquetas (*Multiprotocol Label Switching*)

V.2.2 EL CONCEPTO DE UTILZAR ETIQUETAS COMO ENVÍO DE INFORMACIÓN

MPLS ha sido estandarizado dentro de la IETF sobre el paso de algunos años, e introduce un nuevo acercamiento para despliegue de redes IP, este separa el mecanismo de control del mecanismo de envío e introduce la "etiqueta" utilizada para el envío de paquetes.

MPLS puede ser empleado en redes de solo-ruteo o en ambientes ATM para la integración de infraestructuras de Capa 2 y Capa 3, dentro de redes IP + ATM. Una red MPLS consiste de LSRs[1] en el núcleo de la red y LSRs-frontera rodeando la red, como se muestra en la figura V.7.

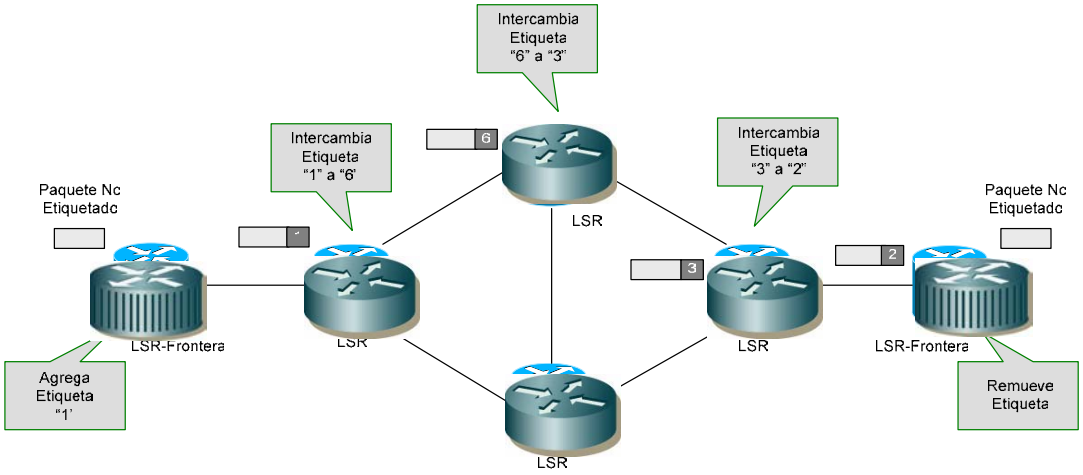


Figura V.6 *El LSR Frontera esta etiquetando en el lado de ingreso para que sea utilizada la etiqueta por el LSR en el núcleo para enviar el tráfico a través del camino deseado y será removida por el LSR Frontera de lado de salida*

Dentro de la red de MPLS, el tráfico es enviado utilizando etiquetas. Los LSRs-Frontera del lado de ingreso de la nube de MPLS son responsables de asignar la etiqueta y enviar el paquete al próximo salto o LSR a lo largo del camino que el tráfico sigue a través de la nube de MPLS. Todos los LSRs a lo largo del camino utilizan la etiqueta como un índice dentro de una tabla que mantiene la información del próximo salto y una nueva etiqueta. La vieja etiqueta es intercambiada con la nueva etiqueta desde la tabla y el paquete es enviado al próximo salto. Utilizar este método implica que el valor de la etiqueta es únicamente de significado local entre dos LSRs. Del lado de salida de la red, la etiqueta es removida y el tráfico es enviado, utilizando mecanismos normales de protocolos de ruteo IP.

[1] LSR: Ruteador Conmuta Etiquetas (*Label Switch Router*)

V.2.3 DEFINICIÓN DE TÉRMINOS UTILIZADOS POR MPLS

A continuación se muestran los conceptos y definiciones básicas que se utilizan por MPLS.

Etiqueta: Un encabezado creado por un LSR-Frontera y utilizado por el LSR de núcleo para el envío de paquetes. El formato del encabezado varía según el tipo de red. Por ejemplo, en una red ATM, la etiqueta tiene colocados campos de VPI/VCI en cada encabezado de celda ATM, en una ambiente LAN, el encabezado es un separador localizado en el encabezado entre Capa 2 y Capa 3.

Base de Información de Reenvío de Etiquetas (LFIB): Es una tabla creada por un dispositivo capas de conmutar etiquetas (LSR) que indica donde y como es enviado un paquete con un valor de etiqueta especifico.

Ruteador Conmuta Etiquetas (LSR): Es un dispositivo tal como un switch o un router que envía entidades etiquetadas basadas sobre valores de etiquetas.

Ruteador Conmuta Etiquetas Frontera (LSR-Frontera): Es el dispositivo que inicia agregando o termina removiendo la etiqueta del paquete.

Etiqueta Conmutada: Cuando un LSR hace una decisión de envío basada sobre la presencia de etiquetas en la trama/celda.

Camino de Etiqueta-Conmutada (LSP): El camino definido por la etiqueta a través de LSRs entre puntos finales.

Etiqueta de Circuito Virtual (LVC): Un LSP a través de un sistema ATM.

Control de Etiqueta Conmutada (LSC): Un LSR que comunica con un switch ATM para proveer y abastecer información de etiquetas dentro del switch.

Protocolo de Distribución de Etiquetas (LDP): Conjunto de mensajes definidos para distribuir información de etiquetas entre LSRs.

XmplsATM: Es la interfaz virtual entre un switch ATM y un LSC.

V.2.4 ARQUITECTURA DE MPLS

MPLS se basa sobre dos componentes principales: reenvío y control. El ***componente de reenvío*** utiliza etiquetas llevadas por los paquetes y la Base de Información de Reenvío de Etiquetas es mantenida por un LSR para ejecutar el

reenvío de paquetes, dicha decisión de reenvío esta basada en un algoritmo de correspondencia-exacta utilizando longitud-fija como un índice. Esto permite simplificar el procedimiento de reenvío, así como incrementar el desempeño de reenvío (muchos paquetes por segundo).

El ***componente de control*** es responsable de mantener la información correcta en la LFIB entre un grupo de LSRs interconectados. El componente de control crea ligas de etiquetas que son distribuidas entre los LSRs utilizando el Protocolo de Distribución de Etiquetas (LDP).

V.2.4.1 PROTOCOLOS DE DISTRIBUCIÓN DE ETIQUETAS

Con el ruteo basado en destino, un ruteador hace decisiones de reenvío basado en direcciones destino de Capa 3, llevadas en un paquete, la información almacenada en la base de información de reenvío (FIB) es mantenida por el ruteador el cual construye esta FIB para usar la información que recibe el ruteador proveniente de los protocolos de ruteo, tales como OSPF y BGP.

Para soportar el ruteo basado en destino con MPLS, un LSR participa con los protocolos de ruteo y construye la LFIB para utilizar la información que es recibida desde los protocolos. En este sentido este opera mas como un ruteador.

Un LSR sin embargo, debe distribuir y utilizar etiquetas localizadas por el LSR par para enviar correctamente la trama a los LSRs distribuyendo etiquetas utilizando un Protocolo de Distribución de Etiquetas (LDP). Una etiqueta mantiene asociado un destino de subred para una etiqueta de significado local (las etiquetas son de significado local por que estas son reemplazadas en cada salto). Siempre que un LSR descubre un LSR vecino, los dos establecen una conexión TCP para mantener la transferencia de etiquetas. LDP intercambia etiquetas/subred utilizando uno o dos métodos: cauce descendiente no solicitado, distribución o cauce descendiente sobre demanda. Ambos LSRs debe acordar que modo utilizar.

V.2.5 APLICACIONES BASADAS EN MPLS

Actualmente el mercado de telecomunicaciones se esta orientando a que los proveedores de servicio traten de crear y vender soluciones con valores agregados para que los clientes puedan hacer uso de los distintos servicios y estar a un paso delante de la cadena de valores. La oportunidad para los proveedores de servicios de ofrecer servicios de VPN basados sobre IP, tal como VPNs BGP/MPLS, hace de esta una tecnología muy atractiva para el mercado. Esto también explica un pequeño

pedazo de "exageración comercial" por MPLS que puede verse en el mercado en los últimos dos años. En nuestro punto de vista, esto no es una visible desaceleración.

La aplicación mas empleada por MPLS es la VPN MPLS. Una típica red VPN MPLS se muestra en la figura V-7. el ruteador de acceso del cliente, también llamado ruteador de ***cliente fronterizo*** (CE[1]), es conectado a los LSRs Frontera, actuando como ruteadores proveedores frontera (PE[2]).

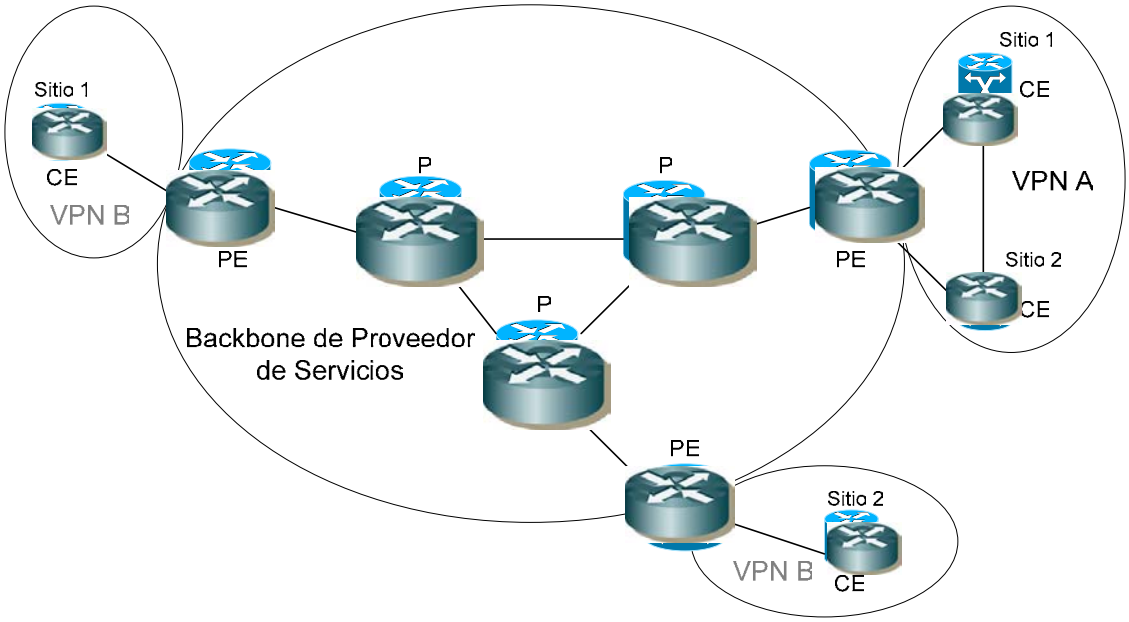


Figura V.7 *VPNs MPLS-Los ruteadores PE utilizan la pila de etiquetas para determinar a cual VPN pertenece la información de ruteo y el tráfico*

Los ruteadores PE asignan dos etiquetas a cada paquete. Una etiqueta representa el identificador de VPN, y la etiqueta superior es utilizada para enviar el paquete a través de la red. Los LSRs en el núcleo de la red son llamados ruteadores proveedores (P) y estos ejecutan conmutación estándar de etiquetas utilizando la etiqueta superior. El ruteador PE en el lado de salida de la red, remueve ambas etiquetas y utiliza la segunda de estas para determinar a cual CE (VPN) el paquete deberá ser enviado.

La segunda aplicación que hace uso del hecho que el componente de control esta completamente separado del componente de reenvío. Los protocolos de ruteo estándar computan el camino opcional desde una fuente a un cierto destino, considerando una métrica de ruteo tal como conteo de saltos, costo, o ancho de banda del enlace. Como resultado, un costo mínimo es elegido. Sin embargo este puede ser un camino alternativo, solo uno es seleccionado por el protocolo de ruteo

[1] CE: Cliente Fronterizo (*Customer Edge*)
[2] PE: Proveedor Fronterizo (*Provider Edge*)

para utilizarse para llevar trafico. Esto conduce a una ineficiente utilización de los recursos de red.

Ingeniería de trafico MPLS (MPLS-TE) introduce el termino ***troncal de trafico***, en el cual un grupo de flujo de trafico con los mismo requerimientos, tal como confiabilidad o prioridad de trafico. MPLS-TE provee manejo de trafico IGP, calculando rutas funcionalmente basado sobre troncal-por-trafico. Otro que al igual que los protocolos estándar de ruteo es manejado por: la topología, utilización de los recursos de la red y atributos de confiabilidad, todo esto es analizado y tomado en cuenta durante la programación del camino. Como se muestra en la figura V.8, múltiples caminos son posibles de un origen a un destino y el mejor es elegido, de acuerdo a la situación actual de la red, asegurando la utilización optima de la red.

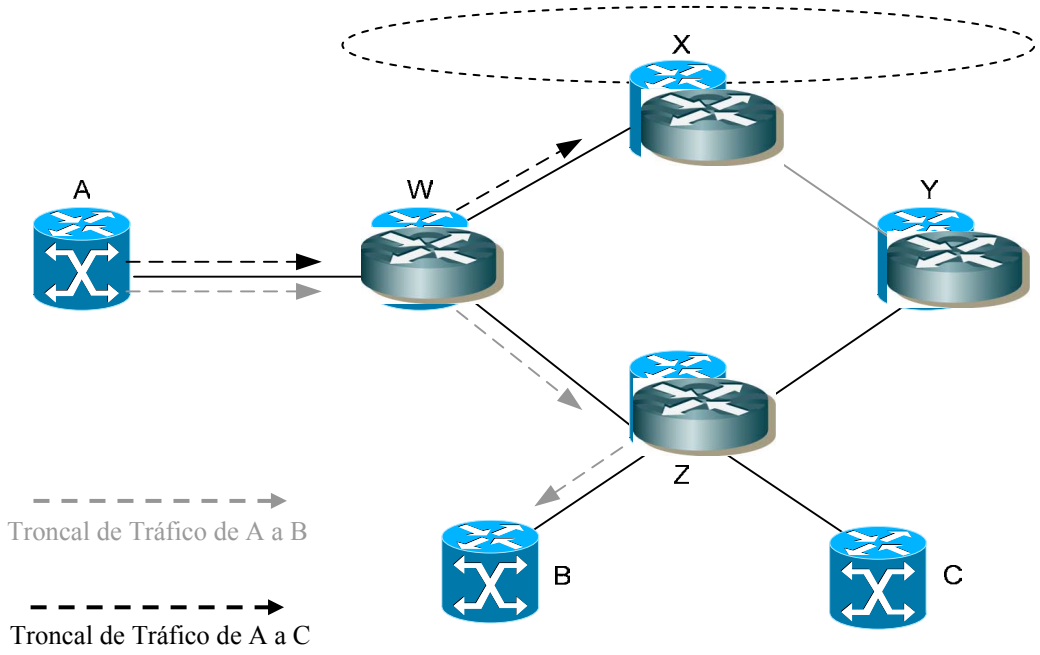


Figura V.8 *Ingeniería de Trafico MPLS provee la habilidad de definir y optimizar el camino que será tomado por el tráfico a través de la red*

V.3 PWE3

PWE3[1] es un mecanismo que emula los atributos esenciales de un servicio como una línea alquilada T1, ATM, Frame Relay o Ethernet sobre una red conmutada de paquetes (PSN[2]). Las funciones requeridas de los PWs[1] incluyen el encapsulado de

[1] PWE3 Emulación de Pseudo Cable punto a punto (*Pseudo Wire Emulation Edge to Edge)*
[2] PSN Red de Paquete Conmutado (*Paquet Switched Network)*

servicios-específicos PDUs[2] que llegan a un puerto de ingreso y son llevados a través de un camino o túnel, administrando su tiempo y orden, y cualquier otra operación requerida para emular el comportamiento y características del servicio tan fielmente como sea posible.

Para la perspectiva de los compradores, el PW es percibido como un enlace no compartido o un circuito del servicio elegido. Sin embargo, hay características que impiden que algunas aplicaciones puedan ser transportadas en un PW. Estas limitantes son y deben ser descritas apropiadamente en cada documento del servicio-especifico.

V.3.1 FUNCIONES ESPECÍFICAS

PWs proveen las siguientes funciones para emular el comportamiento y características de los servicios deseados

- Encapsulacion del servicio especifico PDUs o circuito de datos que llegan al puerto de entrada (lógico o físico)
- Transporte de los datos encapsulados a través de un túnel.
- Administración de la señalización, tiempo, ordenamiento y otros aspectos del servicio en la frontera del PW
- Servicios específicos status de la señalización y administración de alarmas

V.3.2 ARQUITECTURA DE LA RED ACTUAL

Las secciones siguientes se dan algunos antecedentes como son las redes de hoy y por qué estas están cambiando. También hablaremos sobre la motivación para proveer redes que converjan mientras continúan soportando los servicios existentes. Finalmente se discutirá cómo los PWs pueden ser una solución a este dilema.

V.3.2.1 MÚLTIPLES REDES

Para cualquier proveedor de servicios dado que entrega servicios múltiples, su infraestructura actual consiste normalmente de varias redes paralelas o redes

[1] PWs Pseudo Cable *(Pseudo Wire)*
[2] PDUs Unidad Protocolar de Dato (*Protocol Data Unit)*

"*overlay*" (redes revestidas). Cada una de estas redes ofrece un servicio específico, como Frame Relay, acceso a Internet, etc. Esto es bastante costoso, tanto por lo que se refiere al gasto de capital como en gastos de operación. Además, la presencia de redes múltiples complica la planificación. Los proveedores de servicio terminan haciéndose estas preguntas:

¿Cual de mis redes dejare fuera?
¿Cuántas fibras yo necesito para cada red?
¿Cómo manejar eficientemente las múltiples redes?

Una red convergente ayuda a los proveedores de servicio a contestarse estas preguntas en una consistente y económica forma.

V.3.2.2 TRANSICIÓN A UNA RED DE CONVERGENCIA DE PAQUETES-OPTIMIZADOS

Para aumentar al máximo la recuperación de sus capitales, y minimizar los costos de operación, los proveedores de servicio a menudo buscan consolidar la entrega de múltiples tipos de servicio dentro de una simple tecnología de red.

Cuando el tráfico de paquetes es grande y ocupa una gran cantidad de ancho de banda, este llega a ser progresivamente provechoso para optimizar las redes públicas para el Protocolo de Internet. Sin embargo, muchos proveedores de servicio están confrontando grandes obstáculos en la ingeniería de redes de paquetes –optimizados. Aunque el tráfico de Internet es el segmento de tráfico con el mayor crecimiento acelerado, este no genera el mayor capital por bit. Por ejemplo, el tráfico de Frame Relay es el que actualmente genera las mayores rentas por bit a diferencia de lo que hace un servicio nativo de IP. Los servicios de líneas privadas TDM todavía generan aun más réditos por bit que los servicios de Frame Relay. En adición hay una gran cantidad de equipo heredado y desarrollado dentro de las redes públicas que no se comunica utilizando el Protocolo de Internet. Los proveedores de servicios continúan utilizando este equipo no-IP para dar una variedad de servicios, y ven una necesidad de interconectar su este equipo heredado con sus principales redes IP optimizadas.

V.3.3 PWE3 COMO UN CAMINO A LA CONVERGENCIA

Los proveedores de servicio se hacen preguntas de como evaluar cuenta el capital y los beneficios de operación de una nueva infraestructura basada en

paquetes, mientras se hace uso del equipo existente y como proteger la recuperación por flujo de canal asociado con este nuevo equipo ó bien como migrar de las maduras redes ATM y Frame Relay, mientras estas todavía son capaces de proveer lucrativos servicios.

Una posibilidad a todas estas preguntas es la emulación de circuitos o servicios vía PWs.

La emulación sobre ATM y la interconexión de Frame Relay y ATM todavía sigue siendo estandarizado. La emulación permite que los servicios existentes sean transportados a través de la nueva infraestructura, y así sea posible la interconexión de redes distintas. Implementar correctamente, PWE3 puede proveer un medio para soportar los servicios de hoy en día sobre una nueva red.

V.3.4 APLICACIONES ADAPTABLES PARA PWE3

Cuando consideramos ó queremos utilizar a los PWs como una manera para proporcionar una aplicación, las siguientes preguntas deben ser consideradas.

- ¿Es la aplicación es suficientemente desarrollada para garantizar la emulación?
- ¿Hay interés de la parte de los proveedores de servicio en proveer una emulación para la aplicación dada?
- ¿Hay interés de parte de los manufactureros del equipo en proveer productos para la emulación de una aplicación dada?
- ¿Hay complicaciones y limitaciones para proveer una emulación que valga la pena ahorrar capital y ahorrar en gastos de operación?

Si la respuesta a todas las preguntas fue si, entonces la aplicación es muy probable a ser un buen candidato para PWE3. De otra manera, no habrá suficientes coincidencias entre los consumidores, proveedores de servicio, desarrolladores de equipo y tecnología que garantice una emulación.

V.3.5 REFERENCIA DEL MODELO DE PWE3

Un pseudo cable (PW) es una conexión entre las dos puntas del aparato del proveedor los cuales están conectados un circuito adjunto (AC[1]). Un AC puede ser

[1] AC : Circuito Adjunto *(Attachment Circuit)*

un DLCI de Frame Relay, un VPI/VCI de ATM, un puerto Ethernet, una VLAN, un enlace HDLC, una conexión PPP o una interfase física, una sesión PPP por un túnel de L2TP, un LSP de MPLS, etc.

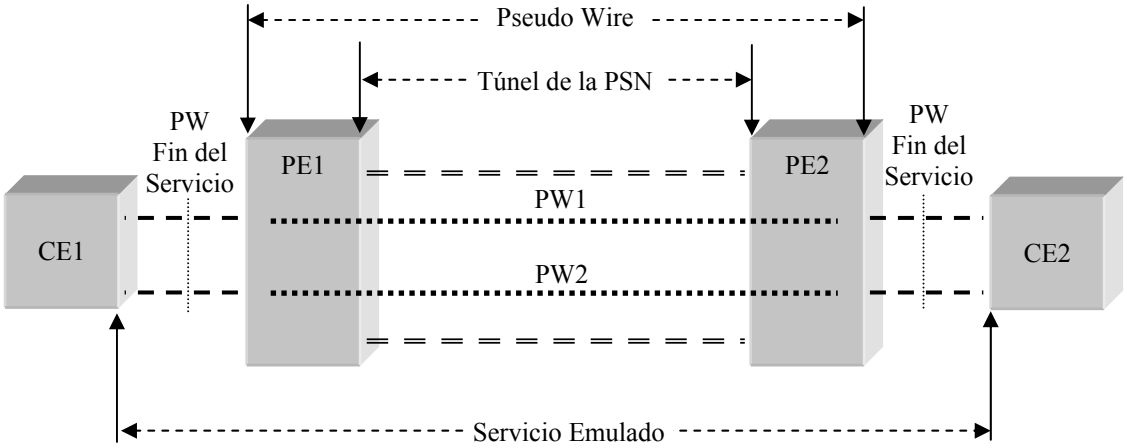


Figura V.9 Modelo de Referencia de PWE3

Durante la configuración de un PW, los 2 PE[1]s pueden ser configurados o serán configurados de manera automática, cambiando información sobre el servicio que será emulado para que después estos sepan procesar los paquetes que vienen del otro lado. Después un PW es configurado entre los dos PEs, los frames recibidos por un PE para un AC serán encapsulados y enviados sobre el PW al PE remoto, donde los frames nativos serán reconstruidos y reenviados al otro CE[2].

V.3.6 PROCESAMIENTO DEL PAQUETE

Esta sección describe brevemente los requisitos de los datos para poder ser considerados dentro de un PWE3.

V.3.6.1 ENCAPSULACIÓN

Todo PE debe proveer un mecanismo de encapsulacion para los PDUs de un AC. Estos deben notarse que los PDUs a encapsular pueden o no contener la información de encabezado L2. Este es el servicio específico. Cada servicio PWE3 debe especificar que PDUs es.

[1] PE : Proveedor Fronterizo (*Provider Edge*)
[2] CE : Cliente Fronterizo (*Customer Edge*)

Un encabezado PW consiste de todos los campos de encabezados en un PW PDU que son usados por el PW salida para determinar como procesar el PDU. La el encabezado del túnel en la PSN no es considerado como parte del encabezado del PW.

TRANSPORTE DE INFORMACIÓN NECESARIA DEL ENCABEZADO L2

La salida de un PW necesita alguna información, por ejemplo, a que servicio nativo pertenecen los PW PDUs, y posiblemente algo de información del encabezado L2, para saber como procesar los PDUs recibidos. Una encapsulacion PWE3 debe proveer algún mecanismo para el transporte con información semejante para el PW de entrada como para el PW de salida. Debe notarse que no toda la información debe ser llevada en el encabezado del PW PDUs

Alguna información (como el tipo de servicio de un PW) puede ser guardado como una información de estado a la salida durante la configuración del PW.

SOPORTE DE PDUS DE LONGITUD VARIABLE

Un PWE3 debe acomodar los PDUs de longitud Variable, si los PDUs de longitud variable son soportados por el servicio nativo. Por ejemplo, un PWE3 para Frame Relay debe acomodar los frames de longitud variable.

SOPORTE DE MULTIPLEXACION Y DEMULTIPLEXACION

Si un servicio en su forma nativa es capaz de agrupar múltiples circuitos en un enlace, por ejemplo múltiples ATM VCCs en un VPC o múltiples interfaces Ethernet 802.1Q en un puerto, algunos mecanismos debe proveer que un simple PW pueda ser usado para conectar dos puntas en el enlace. Desde la perspectiva de encapsulacion, suficiente información debe ser llevada para que la salida del PW pueda demultiplexar los circuitos individuales del PW.

VALIDACIÓN DE PW-PDU

La mayoría de los Frames L2 tienen un campo de detección de errores para asegurar la integridad del frame. Cada servicio PWE3 debe especificar si los *checksum* del frame deben ser preservados a través del PW, o deben ser removidos al ingresar al PE y entonces sean recalculados e insertados a la entrada del PE. Para protocolos como ATM y Frame Relay, el *checksum* solo cubre solo información del enlace local como los identificadores del circuito (por ejemplo DLCI o VPI/VCI). Por consiguiente, el *checksum* puede ser removido por el PE de ingreso y recalculado por el PE de salida.

TRANSMISIÓN DE TIPO DE INFORMACIÓN ÚTIL (PAYLOAD)

Bajo algunas circunstancias es deseable poder distinguir el tráfico PW de otros tipos de trafico como IPv4 o IPv6 o OAM. Por ejemplo, si *Equal Cost Multi-Paht* (ECMP) es ocupado en una PSN, esta adicional capacidad de distinguir puede ser usada para reducir la posibilidad de que los paquetes del PW sean extraviados por el mecanismo de balanceo de cargas. Algunos mecanismos deben proveer la capacidad si es necesario.

V.3.6.2 ORDENAMIENTO DE FRAMES

Cuando los paquetes llevan los PWPDUs atraviesan un PW, estos pueden llegar a la salida fuera de orden, para algunos servicios, los frames deben llegar en orden. Para estos servicios algunos mecanismos deben de asegurar la entrega en orden, proveyendo un número de secuencia en el encabezado del PW para cada paquete o mecanismos de reordenamiento de los frames.

V.3.6.3 DUPLICACIÓN DE FRAMES

En casos raros, los paquetes que atraviesan un PW pueden ser duplicados. Para algunos servicios, la duplicación de frames no esta permitida, Para estos servicios algunos mecanismos deben asegurar que no se entreguen estos frames duplicados. El mecanismo puede o no ser el mismo mecanismo que asegura la entrega en orden de los paquetes.

V.3.6.4 FRAGMENTACIÓN

Si el tamaño combinado de la carga útil del L2, su asociado PWE3 y los encabezados PSN exceden el MTU de la PSN, la carga útil del LS debe ser fragmentada. Con seguridad el servicio nativo, la fragmentación también necesitara mantener el control de la relativa posición de los frames de datos. En general, la fragmentación tiene un impacto en el funcionamiento, es por consiguiente deseable evitar la fragmentación si es posible. Sin embargo, para diferentes servicios, la necesidad de fragmentación debe ser diferente. Cuando hay potencial necesidad de fragmentación, cada servicio especifico PWE3 debe especificar cuando fragmentar el frame en cuestión o dejarlo.

V.3.6.5 CONSIDERACIONES DE SOBRE ENCABEZADO POR PAQUETE DE LA PSN

Cuando el tamaño del L2 PDU es pequeño, para reducir el encabezado del túnel de la PSN múltiples PDUs pueden ser concatenados en un encabezado añadido al túnel de la PSN. Cada PDUs encapsulado puede llevar su propio encabezado PW que el PE de salida el proceso de este. Sin embargo, los beneficios de concatenar múltiples PDUs para eficientar el encabezado debe evaluarse son el incremento del retrato, jitter y sobre todo los riesgos que se corren si se pierde el paquete.

V.3.7 CONSIDERACIONES EXTRAS

En general hay mucho mas consideraciones que son consideradas para proporcionar un PWE3 pero depende de cada servicio que se desea emular, y el cual debe ser especificado en su propio estándar como son la administración, mantenimiento, configuración, verificación, fidelidad, seguridad, calidad de servicio, etc. características que dependen de cada uno de los servicios a ser emulados.

V.3.8 EN RESUMEN

Para maximizar la recuperación de sus gastos y minimizar los gastos de operación, muchos proveedores de servicios están buscando consolidar el desarrollo de múltiples servicios ofrecidos y tipos de tráfico en una simple red IP optimizada.

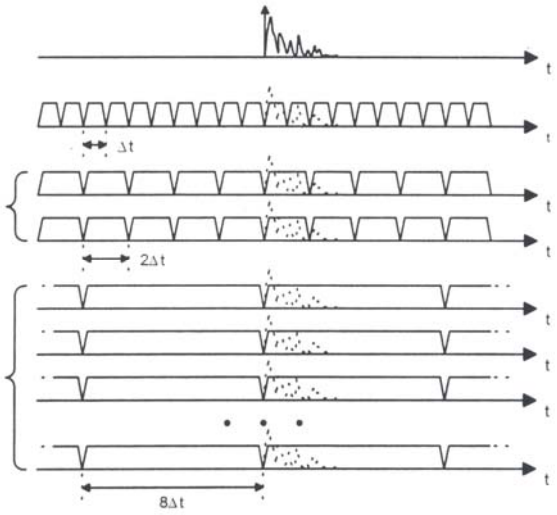
En consecuencia para crear esta nueva generación de redes convergentes, los métodos de estandarización deben ser desarrollados para emular los existentes formatos de telecomunicaciones como Ethernet, Frame Relay y ATM sobre una Red Principal de IP optimizada

V.4 OFDM

El principio básico de OFDM[1] es dividir un flujo de datos de alta velocidad en varios flujos de menor tasa de datos los cuales se transmiten simultáneamente sobre subportadoras a diferentes frecuencias. Como la duración del símbolo se incrementa

[1] OFDM: Multiplexacion Ortogonal por División de Frecuencia (*Orthogonal Frequency Division Multiplexing*)

al tener subportadoras paralelas de más baja velocidad, la cantidad de dispersión relativa en el tiempo causada por el retraso de las multitrayectorias disminuye. La interferencia intersímbolo (ISI, *InterSymbol Interfernece*) se elimina casi completamente mediante la introducción de un intervalo de guarda antes de cada símbolo OFDM. Durante el intervalo de guarda el símbolo se extiende cíclicamente para evitar la interferencia intersímbolo.



FiguraV.10 *El efecto de adoptar un sistema multiportadora*

OFDM en un caso especial de transmisión por multiportadora, donde una sola fuente de datos se transmite sobre un número finito de subportadoras de baja velocidad. Vale la pena mencionar aquí que OFDM puede ser visto tanto como una técnica de modulación como una técnica de multiplexación ya que una sola o varias fuentes de información pueden modular a las subportadoras. Una de las principales razones para utilizar OFDM es su inherente protección contra el desvanecimiento por selectividad de frecuencias o interferencia de banda angosta. En un sistema con una sola portadora, un solo desvanecimiento o interferencia causa el rompimiento completo del enlace, pero en un sistema de multiportadora sólo será afectado un pequeño porcentaje de subportadoras. La codificación para corrección de errores puede ser usada entonces para corregir las portadoras erróneas.

OFDM tiene las siguientes ventajas clave:

- OFDM es una manera eficiente de abatir los efectos de las multitrayectorias. Para una distribución de retardos dada, por ejemplo la de la figura V.11, la complicidad de implementación que significativamente menor comparada con la de un sistema de portadora única con un ecualizador.
- OFDM es un esquema robusto contra la interferencia de banda angosta por dicha interferencia afecta sólo un pequeño porcentaje de las subportadoras.

- OFDM hace posible implementar redes de frecuencia única (SFN, *Single Frecuency Networks*) lo cual especialmente atractivo para aplicaciones de difusión masiva.

Por otro lado. OFDM también tiene algunas desventajas comparado con los esquemas de portadora única

- OFDM es más sensible a las desviaciones de frecuencia y el ruido de fase.
- OFDM tiene una gran relación prepotencia pico bajo precio promedio, lo que tiende a reducir la eficiencia del amplificador de radiofrecuencia.

En un sistema clásico de datos en paralelo la banda total de frecuencias se divide en N subcanales los cuales encuentran sin traslapes. Cada subcanal se modula por separado y luego los N subcanales son multiplexados en frecuencia (FDM). Bajo este esquema es necesario evitar el traslapes espectral de los subcanales para prevenir la interferencia intercanal; sin embargo, esto conlleva aún uso ineficiente del espectro disponible debido a la introducción de banda de guarda. Para contrarrestar estas ineficiencia, las ideas propuestas a mediados de la década de los sesentas fueron utilizar datos en paralelo y FDM con subcanales traslapados, en donde cada portadora un ancho de banda *B* y las portadoras están espaciadas *B/2* en el dominio de la frecuencia para evitar el uso de ecualización de alta velocidad, compartir el ruido impulsivo y la distorsión por un trayectoria, así como incrementar la eficiencia del ancho de banda disponible.

En la figura V.11 se muestra la diferencia entre la técnica convencional de multiportadoras no traslapadas y la técnica de modulación con multiportadoras traslapadas. Sin embargo, para implementar éste técnica es necesario angular de interferencia entre las subportadoras, es decir, que las subportadoras sean ortogonales entre sí.

La palabra ortogonal indica que existe una relación matemática específica entre las frecuencias de las portadoras en el Sistema. En un sistema de multiplexación por división de frecuencias (FDM) normal, las portadoras son espaciadas de tal manera que las señales puedan ser recibidas utilizando filtros y de modula errores convencionales por lo que son introducidas bandas de guarda entre portadoras en el dominio de la frecuencia.

Sin embargo, es posible ordenar las subportadoras en un sistema OFDM de tal manera sus bandas laterales se traslapes y aún así sean recibidas sin interferencia de portadora adyacente. Para llevar a cabo esto las subportadoras deben ser matemáticamente ortogonales.

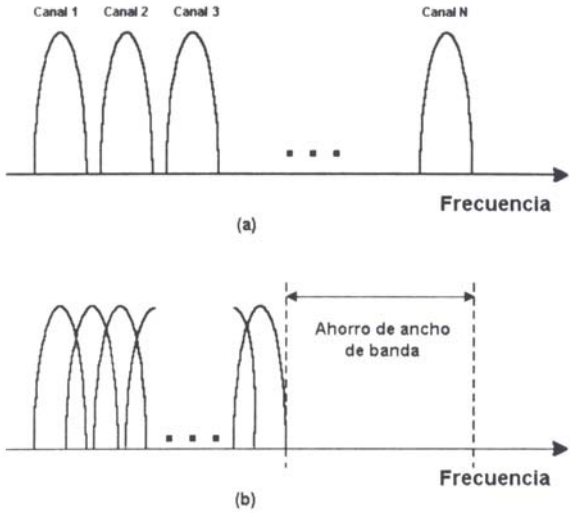


Figura V.11 *Concepto de señal OFDM: (a) Técnica convencional de multiportadora FDM. (b) Técnica de modulación con multiportadoras ortogonales.*

V.4.1 DESCRIPCIÓN OFDM

El estándar IEEE802.11a define la capa física que adopta una modulación OFDM. La capa física de OFDM provee la capacidad para transmitir frames PDU a velocidades superiores a los 54Mbps para redes WLAN donde las transmisiones de contenido multimedia es considerable.

V.4.1.1 SUBCAPA PLCP PARA OFDM

El PPDU es único en la capa física para una modulación OFDM. El PPDU consiste de un preámbulo PLCP y un campo de signal data como se muestra en la figura

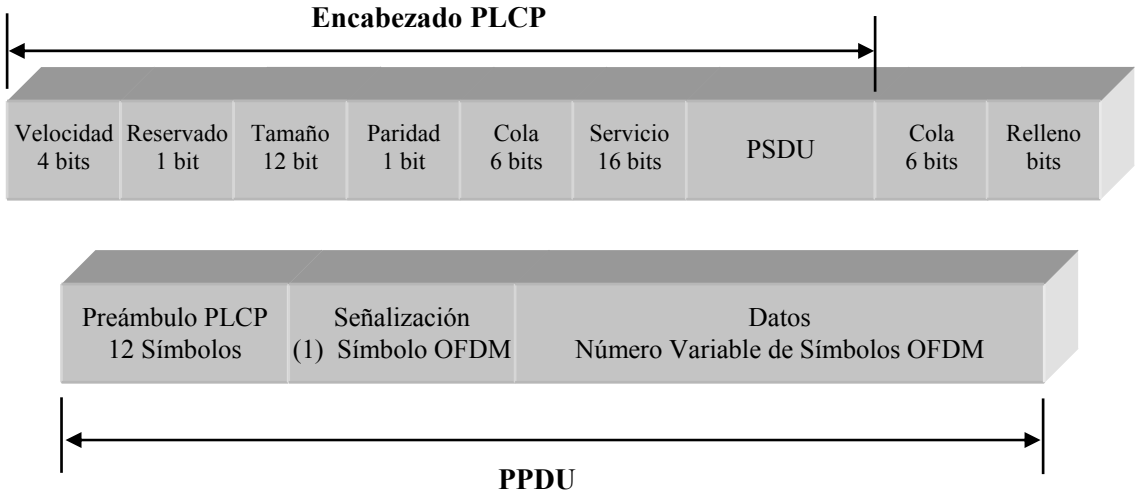


Figura V.12 *Encabezado del PLCP para OFDM*

El receptor usa el preámbulo PLCP para obtener la señal entrante de OFDM y sincronizar el demodulador. EL encabezado PLCP contiene la información acerca del PSDU de la señal enviada de OFDM. El preámbulo PLCP y el campo de *signal* son siempre trasmitidos a 6Mbps, con una modulación BPSK- OFDM modulada usando un código convolucional R=1/2

PLCP preámbulo. Este campo es usado para obtener la señal entrante y el tren de pulsos y sincronizar el receptor. EL preámbulo consiste de 12 símbolos, diez de los cuales son pequeños símbolos, y dos son largos símbolos. Los símbolos cortos son usados para preparar el AGC (*Automatic Gain Control*) y obtener un a aproximación de la frecuencia portadora y el canal. Los símbolos largos son usados para mejorar la sintonización de la frecuencia y la estimación del canal.

Doce subportadoras son usadas para los símbolos cortos y 53 para largos. La preparación del canal OFDM es completado en 16μs. El PLCP preámbulo es modulado por BPSK-OFDM a 6Mbps.

Signal. Es un campo de 24 bits, el cual contiene información acerca de la tasa y longitud del PSDU. EL campo de signal es un código convolucional ½, modulado con BPSK-OFDM. Para cuatro bits (R1 – R4) son usado una codificar la velocidad, 11bits son usados para la longitud, un bit es reservado, un bit de paridad, y seis “0s” son la cola. Los bits que definen la velocidad se muestran en la tabla siguiente

Velocidad	Modulación	Tasa de Codificación	Bits de Señalización (R1 – R4)
6 Mbps	BPSK	R = ½	1101
9 Mbps	BPSK	R = ¾	1111
12 Mbps	QPSK	R = ½	0101
18 Mbps	QPSK	R = ¾	0111
24 Mbps	16QAM	R = ½	1001
36 Mbps	16QAM	R = ¾	1011
48 Mbps	64QAM	R = 2/3	0001
54 Mbps	64QAM	R = ¾	0011

Tabla V.2 *Configuraciones Posibles para los Bits del Campo de Señalización*

La velocidad e transmisión obligatoria para la IEEE 802.11a para los sistemas es de 6Mbps, 12Mbps, y 24 Mbps.

Length Este campo es un número anónimo de 12-bits que indica el número de octetos en el PSDU.

Data. El campo de datos contiene el campo de servicio, PSDU bits de cola y bits de ensamblado. Un total de seis bits de cola contienen "0s" que son adjuntados al PPDU para asegurar que la codificación convolucional vuelva a un estado de cero.

V.4.1.2 MEZCLADOR DE DATOS

Todos los bits transmitidos por la subcapa PDM en una porción de saltos son mezclados usando un frame sincrono 127-bit de una secuencia generadora. La mezcla es usada para aleatorizar el servicio, PSDU, bit de relleno y patrón de datos, los cuales pueden contener largas cadenas de 1s o 0s. Los bits de cola no son mezclados.

V.4.2 MODULACIÓN OFDM

OFDM es un método escogido por la IEEE 802.11a similar a la técnica adoptada en Europa por el ETSI HIPERLAN II en la banda de 5GHz.

El principio básico de operación es dividir las señales binarias de alta velocidad, para ser transmitidas en una tasa menor por diferentes subportadoras. Hay 48 subportadoras de datos y 4 subportadoras piloto para tener un total de 52. Cada stream es modulado por separado en una diferente subportadora de los diferentes canales en la banda de 5GHz.

La interferencia intersimbolo no se presenta generalmente en portadoras de baja velocidad, pero desvanecimiento por interferencia entre canales, es por eso que la interpolación de los bits y un código convolucional son usados para mejorar el funcionamiento del canal.

Para esto se utilice la técnica de OFDM en la cual cada subportadora es ortogonal a la otra. Ahora cada PPDU primeramente es codificado usando un código convolucional r=1/2, y los bits son reordenados. Cada bit es mapeado a un número complejo de acuerdo al tipo de modulación y subdividido en 48 subportadoras de datos y 4 pilot subportadoras. Las subportadoras son combinadas usando una inversa transformada rápida de Fourier y transmitidos. En el receptor, la portadora es convertida nuevamente a multiportadoras de baja velocidad para usar la FFT. Las subportadoras de baja velocidad son combinadas para obtener nuevamente una PPDU de alta velocidad.

Un ejemplo de un sistema IEEE802.11a es ilustrado en la siguiente figura.

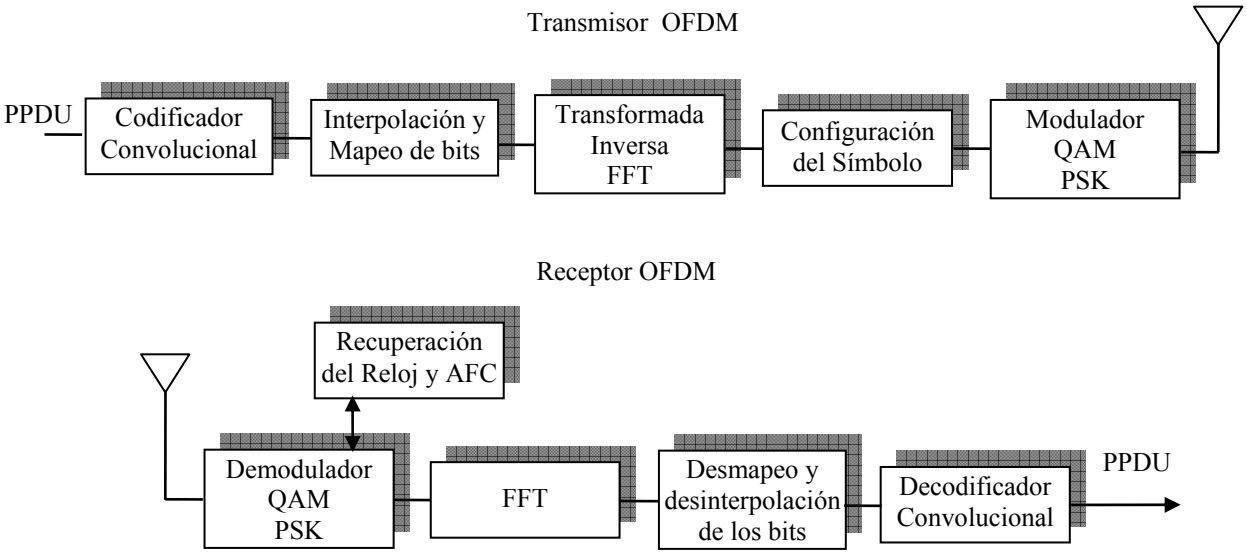


Figura V.13 *Transmisor y Receptor para OFDM*

V.4.3 OPERACIÓN DE CANAL PARA OFDM

La banda de 5GHz es dividida en 3 bandas de 100MHz que van de los 5.15-5.25 Ghz, de los 5.25-5.35GHZ y de los 5.725-5.825 GHZ. Las potencias también son especificadas y son de 40 mW, 200 mW, y 800mW.

V.5 VPN (REDES PRIVADAS VIRTUALES)

V.5.1 INTRODUCCIÓN

En los últimos años las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital, por tanto dichas redes cumplen con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Como ya se ha visto en la actualidad, las redes reducen en tiempo y dinero los gastos de las empresas, eso ha significado una gran ventaja para las organizaciones, sobre todo las que cuentan con oficinas remotas a varios kilómetros de distancia, pero también es cierto que estas redes remotas han despertado la curiosidad de algunas personas que se dedican a atacar los servidores y las redes para obtener información confidencial. Por tal motivo la seguridad de las redes es de suma importancia, es por eso que escuchamos hablar tanto de los famosos firewalls y las VPNs[1]

V.5.2 POR QUÉ UTILIZAR UNA VPN

Cuando se desea enlazar oficinas centrales con alguna sucursal u oficina remota se tienen tres opciones:

1. Modem: Las desventajas es el costo de la llamada, ya que el costo de esta llamada sería por minuto conectado, además sería una llamada de larga distancia, a parte de que no contaría con la calidad, velocidad y seguridad adecuadas.
2. Línea Privada: Tendría que tender mi cable ya sea de cobre o fibra óptica de un punto a otro, en esta opción el costo es muy elevado porque si por ejemplo necesito enlazar mi oficina central con una sucursal que se encuentra a 200

[1] VPN: Red Privada Virtual (*Virtual Private Network*)

Kilómetros de distancia el costo sería por la renta mensual por Kilómetro. Sin importar el uso.

3. VPN: Los costos son bajos porque solo realizo llamadas locales, además de tener la posibilidad de que mis datos viajen encriptados y seguros, con una buena calidad y velocidad.

V.5.3 ¿QUE ES UNA VPN?

Una VPN es una red privada que se extiende mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos, a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte de datos.

Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública. (ver figura V.15)

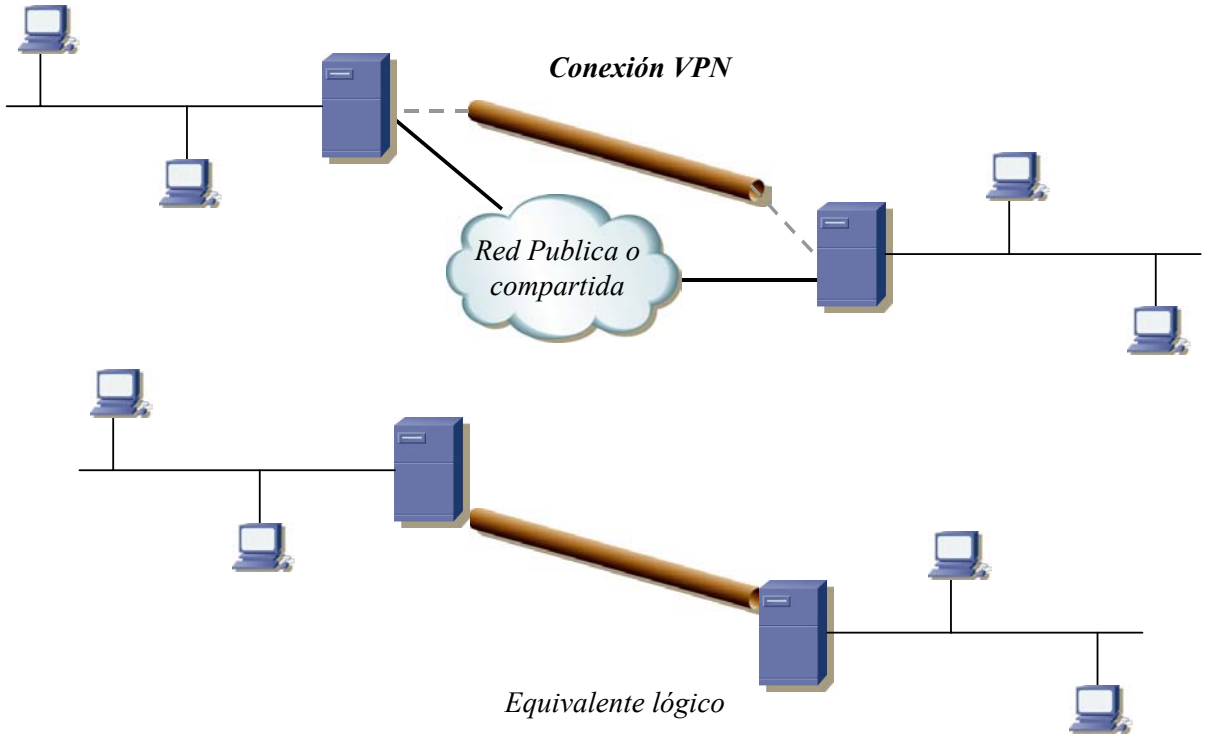


Figura V.14 Conexión de una VPN

En la figura V.14 se muestra como viajan los datos a través de una VPN ya que el servidor dedicado es del cual parten los datos, llegando a un firewall que hace la función de una pared para engañar a los intrusos a la red, después los datos llegan a la nube de Internet donde se genera un túnel dedicado únicamente para nuestros

datos donde se garantiza la velocidad y ancho de banda para así lleguen a su vez al firewall remoto y terminen en el servidor remoto.

Figura V.15 *Como funciona una VPN*

Las VPN pueden enlazar por ejemplo, oficinas corporativas con socios, con usuarios móviles, con oficinas remotas, mediante los protocolos como Internet, IP, Ipsec, Frame Relay, ATM, etc. como lo muestra la figura V.16.

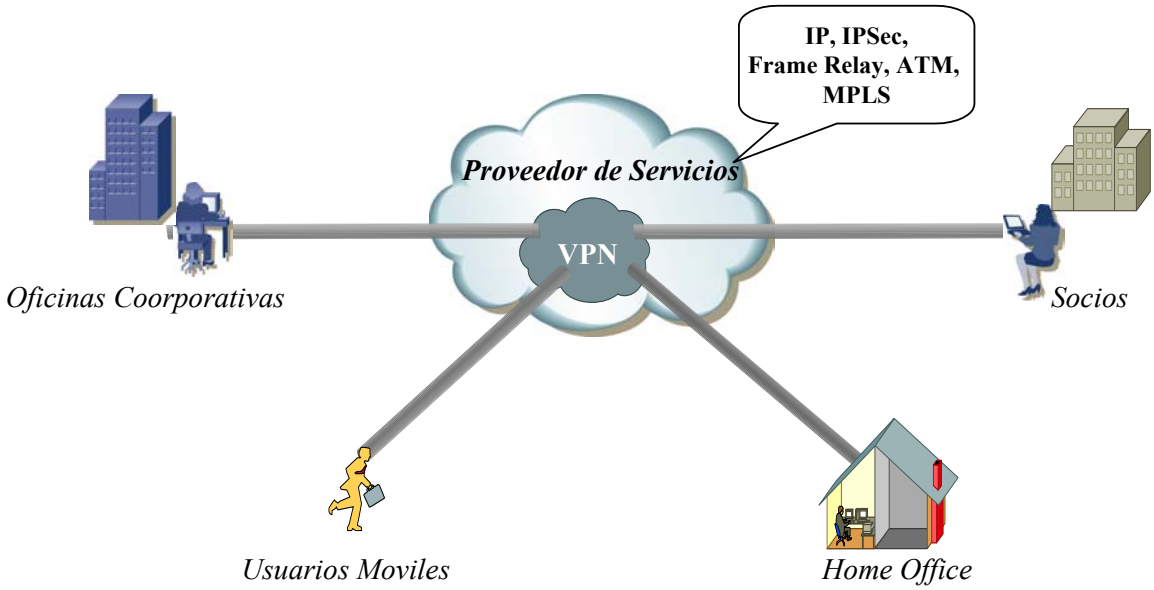


Figura V.16 *Ejemplos de enlaces con VPNs*

V.5.4 TECNOLOGÍA DE TÚNEL

Las redes privadas virtuales crean un túnel o conducto de un sitio a otro para transferir datos a esto se le conoce como encapsulación además los paquetes van encriptados de forma que los datos son ilegibles para los extraños que intentan

interceptarlos. El servidor busca mediante un ruteador la dirección IP del cliente VPN en la red de transito a donde se envían los datos sin problemas.

V.5.5 REQUERIMIENTOS BÁSICOS DE UNA VPN

Por lo general cuando se desea implementar una VPN hay que asegurarse que esta posea:

- Identificación de usuario
- Administración de direcciones
- Codificación de datos
- Administración de claves
- Soporte a protocolos múltiples

V.5.5.1 IDENTIFICACIÓN DE USUARIO

La VPN debe ser capaz de verificar la identidad de los usuarios y restringir el acceso a la VPN a aquellos usuarios que no estén autorizados. Así mismo, debe proporcionar registros estadísticos que muestren quien acceso, cuando y que información manejo.

V.5.5.2 ADMINISTRACIÓN DE DIRECCIONES

La VPN debe establecer una dirección del cliente en la red privada y debe cerciorarse que las direcciones privadas se conserven así.

V.5.5.3 CODIFICACIÓN DE DATOS

Los datos que se van a transmitir a través de la red pública deben ser previamente encriptados para que no puedan ser leídos por clientes no autorizados de la red.

V.5.5.4 ADMINISTRACIÓN DE CLAVES

La VPN debe generar y renovar las claves de codificación para el cliente y el servidor.

V.5.5.5 SOPORTE A PROTOCOLOS MÚLTIPLES

La VPN debe ser capaz de manejar los protocolos comunes que se utilizan en la red pública. Estos incluyen el protocolo de Internet "IP", el Intercambio de paquete de Internet "IPX", entre otros.

V.5.6 COMPONENTES DE UNA VPN

Los dispositivos que generalmente conforman un entorno con VPNs son los siguientes:

- VPN gateway
- Software
- Firewall
- Router
- Dispositivos con un software y hardware especial para proveer de capacidad a la VPN
- Software

V.5.7 VENTAJAS DE UNA VPN

Dentro de las ventajas más significativas podemos mencionar:

- La integridad, confidencialidad y seguridad de los datos.
- Reducción de costos.
- Sencilla de usar.
- Sencilla instalación del cliente en cualquier PC Windows, Unix, Linux, etc.
- Control de acceso basado en políticas de la organización
- Herramientas de diagnostico remoto.
- Los algoritmos de compresión optimizan el tráfico del cliente.
- Evita el alto costo de las actualizaciones y mantenimiento a las PC´s remotas.

V.5.8 CONCLUSIÓN

Las VPN representan una gran solución para las empresas en cuanto a seguridad, confidencialidad e integridad de los datos y prácticamente se han vuelto

un tema importante en las organizaciones, debido a que reduce significativamente el costo de la transferencia de datos de un lugar a otro, el único inconveniente que pudieran tener las VPN es que primero se deben establecer correctamente las políticas de seguridad y de acceso porque si esto no esta bien definido pueden existir consecuencias serias.

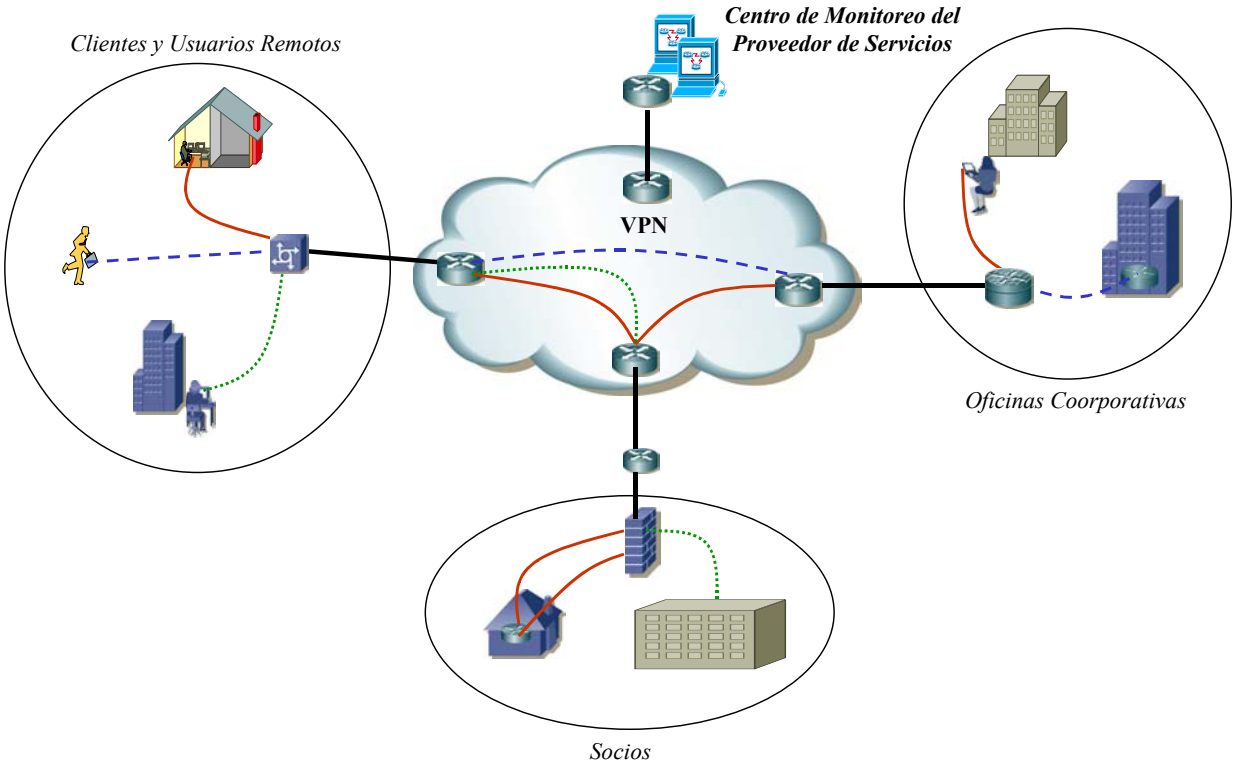


Figura V.17 *Ejemplo de una red implementando VPNs*

VI

DISEÑO Y PROPUESTA DE IMPLANTACIÓN DE UNA RED DE TELECOMUNICACIONES MODERNA

En la actualidad y desde hace algunos años, el diseño de redes se basa en el uso de unas cuantas tecnologías conocidas, enfocándose principalmente a procesos de transmisión de datos entre computadoras sin tomar en cuenta los beneficios que puede traer la implantación de un diseño de red de alta disponibilidad con las características extras que ofrecen las nuevas tecnologías.

En términos generales, los diseños sencillos no toman en cuenta la disponibilidad de la red y particularmente sólo se enfocan en los costos de éstas, lo cual hace que se diseñen redes económicas, dejando en segundo término consideraciones tales como desempeño y confiabilidad.

Por otro lado, hoy en día las demandas de comunicación han aumentado ya que ahora no sólo se requiere de comunicación entre sus computadoras y grandes anchos de banda, sino que también se requiere que tengan una alta disponibilidad, confiabilidad,

seguridad, movilidad y velocidad, lo cual implica que en cualquier época del año los usuarios puedan hacer uso de los recursos de ésta sin temor a fallas o que su información sea usurpada.

Estas nuevas demandas nos llevan a diseñar redes con nuevas tecnologías las cuales cumplan con todas las necesidades que los usuarios requieren.

VI.1 ANÁLISIS DE RED CONVENCIONAL

Un claro ejemplo del diseño típico de redes se muestra en la figura VI.1 en el cual se observa una red convencional de Frame-Relay, donde se considera una organización que cuenta con dos sitios remotos.

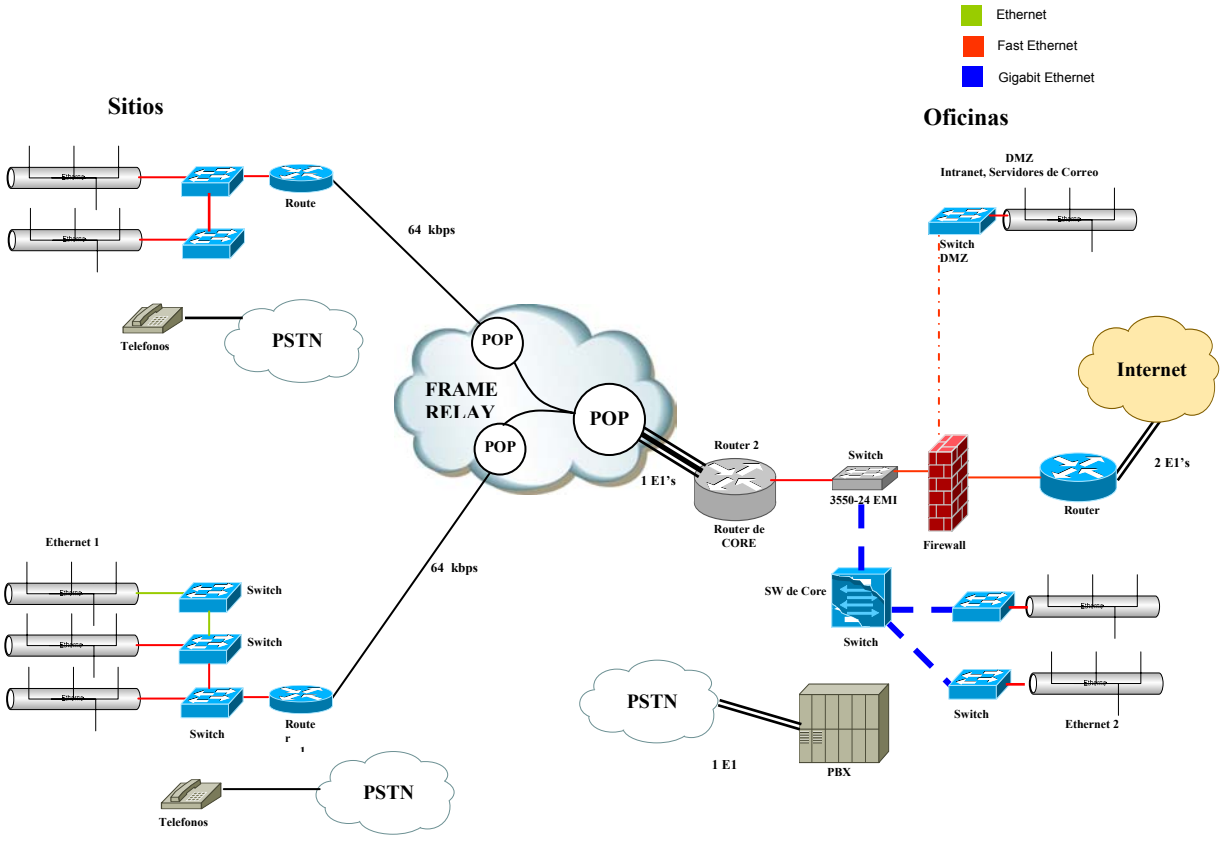


Figura VI.1 Diagrama de Red Frame-Relay.

Si se analiza el diagrama de red, se encuentra que hay varios puntos críticos de falla, tanto en la parte LAN como en la parte WAN, los cuales hacen que la red presente una baja disponibilidad. A continuación se explica el estudio de cada uno de los sitios que conforman la red.

VI.1.1 SITIO LOCAL (OFICINAS GENERALES)

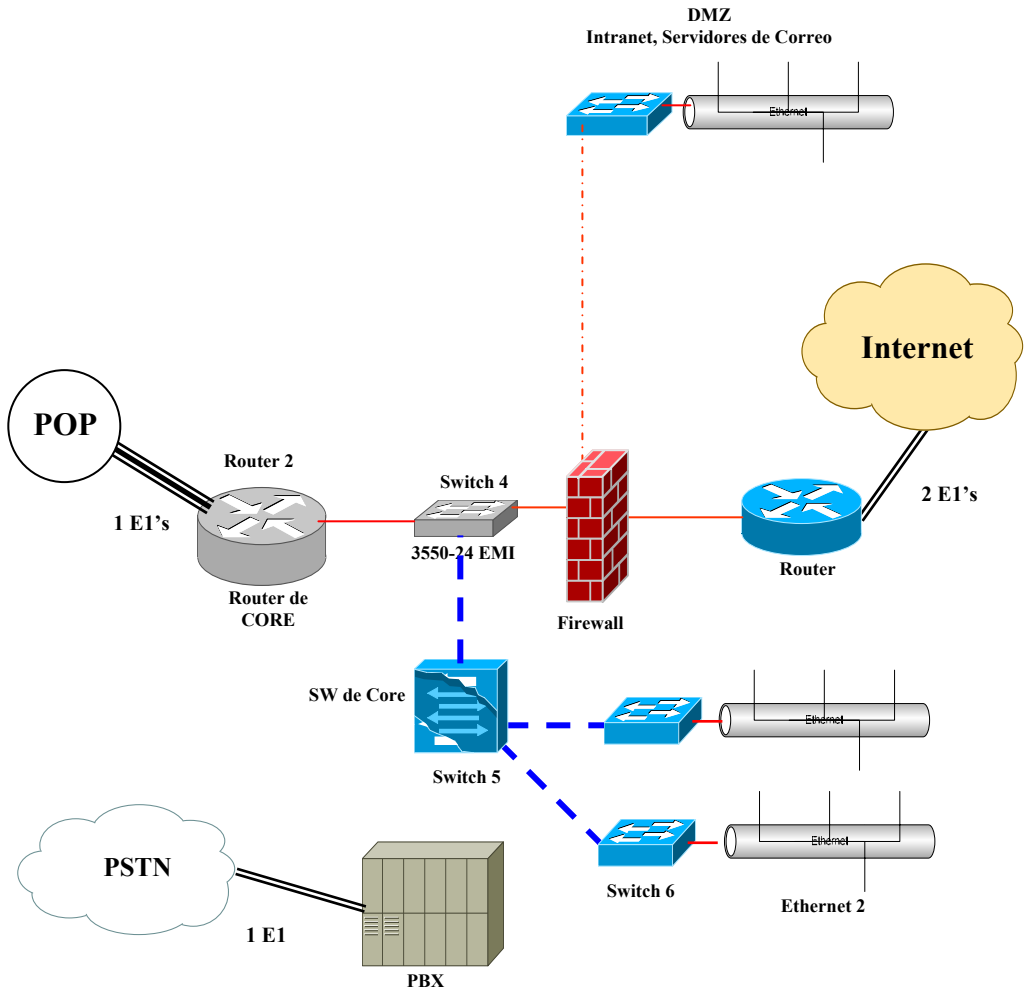


Figura VI.2 Diagrama de Red Sitio Local.

En el diagrama de red del sitio local (figura VI.2) se observa que hay dos routers, un *firewall* y un *switch* conectando la parte WAN. El primero de los routers (el router de CORE) es con el cual se tiene acceso a la red de Frame-Relay y por medio del cual existe comunicación desde los sitios remotos a la granja de servidores dentro de la DMZ y los posibles recursos compartidos de la red local. Este router solo cuenta con un enlace E1 hacia la red Frame Relay lo cual hace que se considere como punto de falla, dado que si en algún momento el router o el enlace dejan de funcionar o fallan, los sitios remotos quedan aislados y sin conexión alguna hacia los servidores o recursos de la red local.

El segundo de los routers es por el cual se tiene acceso al Internet tanto la red local como los sitios remotos. Este cuenta con dos enlaces E1 hacia Internet pero al igual que el router de CORE también es considerado como punto de falla por que, si bien se cuenta con un enlace redundante hacia Internet, ambos enlaces están conectados al mismo router y se confía la disponibilidad de toda la red hacia Internet solo en este elemento.

VI.1.1.1 ELEMENTOS DE CORE

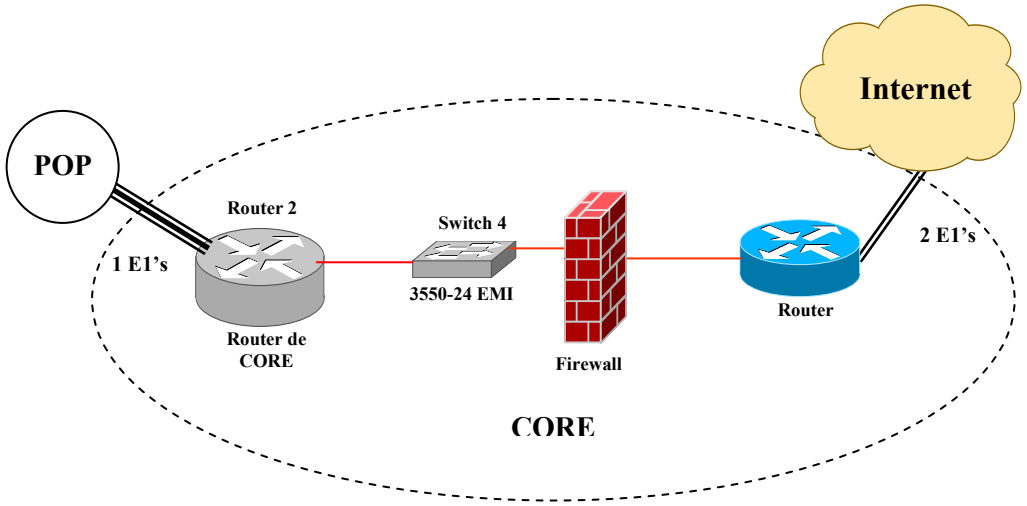


Figura VI.3 Elementos de Core.

Cabe resaltar que todos los elementos de la parte de CORE (figura VI.3), cuentan con enlaces simples y sin redundancia entre ellos (entre el switch, router y firewall), lo cual hace que la disponibilidad baje considerablemente ya que todos los elementos en serie pueden ser considerados como puntos de falla, además de que anchos de banda de dichos enlaces sean insuficientes pisara aplicaciones multimedia.

VI.1.1.2 DISTRIBUCIÓN

En la parte de distribución (figura VI.4), la red cuenta con un switch multicapas por medio del cual da servicio a los demás switches de la parte de acceso, en este punto no tenemos mas problemas que la falta de enlaces redundantes hacia la parte de CORE si consideramos que el equipo tiene un buen desempeño.

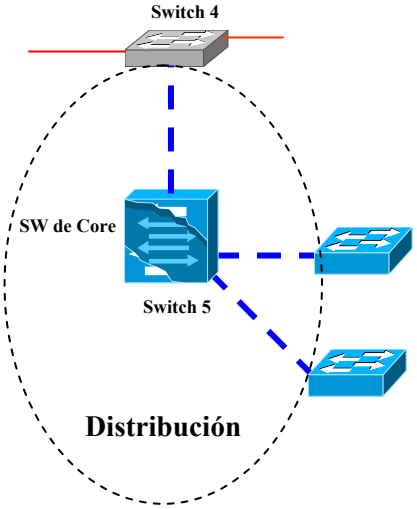


Figura VI.4 Elementos de Distribución.

VI.1.1.3 ACCESO

En la parte de acceso (figura VI.5), tenemos una topología estrella de los diferentes switches hacia el switch de distribución en los cuales se conectan los diferentes equipos de la red LAN del sitio local. En esta parte de la red LAN no tenemos mas problemas que la falta de puntos de acceso por medio de los cuales podamos acceder a nuestra de red de forma inalámbrica y poder utilizar las bondades que nos brinda esta tecnología, sobre todo en el aspecto de crecimiento, movilidad y cableado.

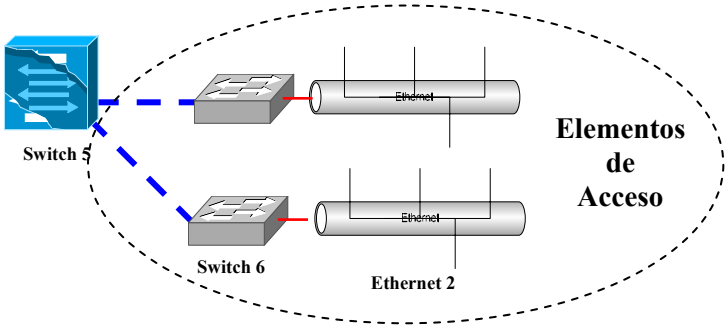


Figura VI.5 Elementos de Acceso.

VI.1.2 SITIO REMOTO 1

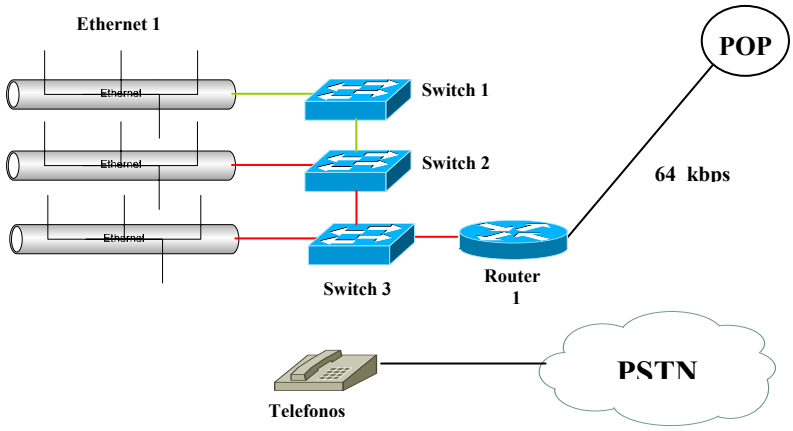


Figura VI.6 Sitio Remoto 1.

En el sitio remoto 1(figura VI.6), se tiene sólo un router en la parte de CORE que ofrece conexión hacia la red Frame-Relay y por el cual se tiene acceso a la información de los servidores en el sitio local e Internet; sólo hay un enlace de 64 Kbps el cual es de baja capacidad y puede llegar a ver retardos considerables de la información requerida, lo cual es un grave problema si se toma en cuenta consideraciones como el posible crecimiento de la red o la posible integración de servicios de voz y video, a parte de que el enlace y el router son considerados otros puntos de fallas, dado que no se cuenta con equipo ni enlaces redundantes hacia la red Frame Relay.

La topología de la red LAN, es una topología jerárquica, en la cual los switches están cascadeados lo cual hace que todos los switches y la mayoría de los usuarios dependan del primer switch o switch raíz, el cual se convierte en un gran punto de falla, ya que si este o su enlace hacia el router deja de funcionar, todos los usuarios de la red no tendrán acceso a la información.

Los enlaces de cascadeo dentro de la red LAN son bajo ancho de banda e incluso hay elementos como el switch 1 que todavía son elementos Ethernet 10baseT.

VI.1.3 SITIO REMOTO 2

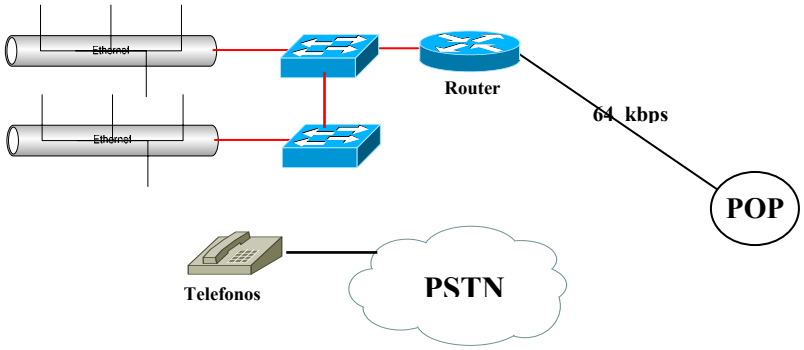


Figura VI.7 Sitio Remoto 2.

Al igual que en el sitio remoto 1, el sitio remoto 2 (figura VI.7), tiene características y problemas semejantes: solo cuenta con un router de acceso a la red WAN, una topología jerárquica en la red LAN, un sólo un enlace de 64kbps, no cuenta con redes híbridas para posibles elementos de la red móviles, etc.

Dentro de este ejemplo de red Frame-Relay, también se observa que sólo se realiza la transmisión de datos y por lo tanto no se aprovecha la infraestructura de dicha red para ofrecer los servicios de voz, los cuales forzosamente deben de ser realizados a través de de la PSTN. Esto generalmente ocasiona un gasto extra, si se considera que en la mayor parte de las organizaciones el tráfico de llamadas es interno, ya sea para resolver problemas de procedimientos de la organización o simplemente llamadas de asistencia técnica. Y aun es mayor el gasto si tomamos en cuenta que dichos sitios remotos pueden estar fuera del área de una llamada local.

Otro inconveniente que se tiene, son los enlaces de bajo ancho de banda sin redundancia, lo cual primeramente hace lento el acceso a los servidores o recursos en la red, lo cual es un factor importante a considerar si se planea en un futuro un crecimiento de las redes LAN en cada uno de los sitios remotos.

Ahora considerando que la red WAN son enlaces de Frame-Relay se sabe que los retardos en el procesamiento de los switches de conmutación y servicios de QoS (calidad de servicio) son muy rudimentarios, lo cual hace que se tengan serios inconvenientes en aplicaciones multimedia a través de la red.

Finalmente dentro de este tipo de redes no se pueden continuar con trabajos pendientes, ya que no es posible acceder a la información a través de la Internet, o bien en muchos casos no se cuenta con la completa seguridad de acceder a dicha información de manera privada y confidencial tanto por Internet como por la misma red Frame-Relay.

VI.2 ANÁLISIS DE RED PROPUESTA

Ahora bien al tomar en cuenta una red de telecomunicaciones con tecnologías modernas se tienen varias diferencias, por ejemplo en la figura VI.8 se observa una propuesta de red con base a las nuevas tecnologías ofrecidas.

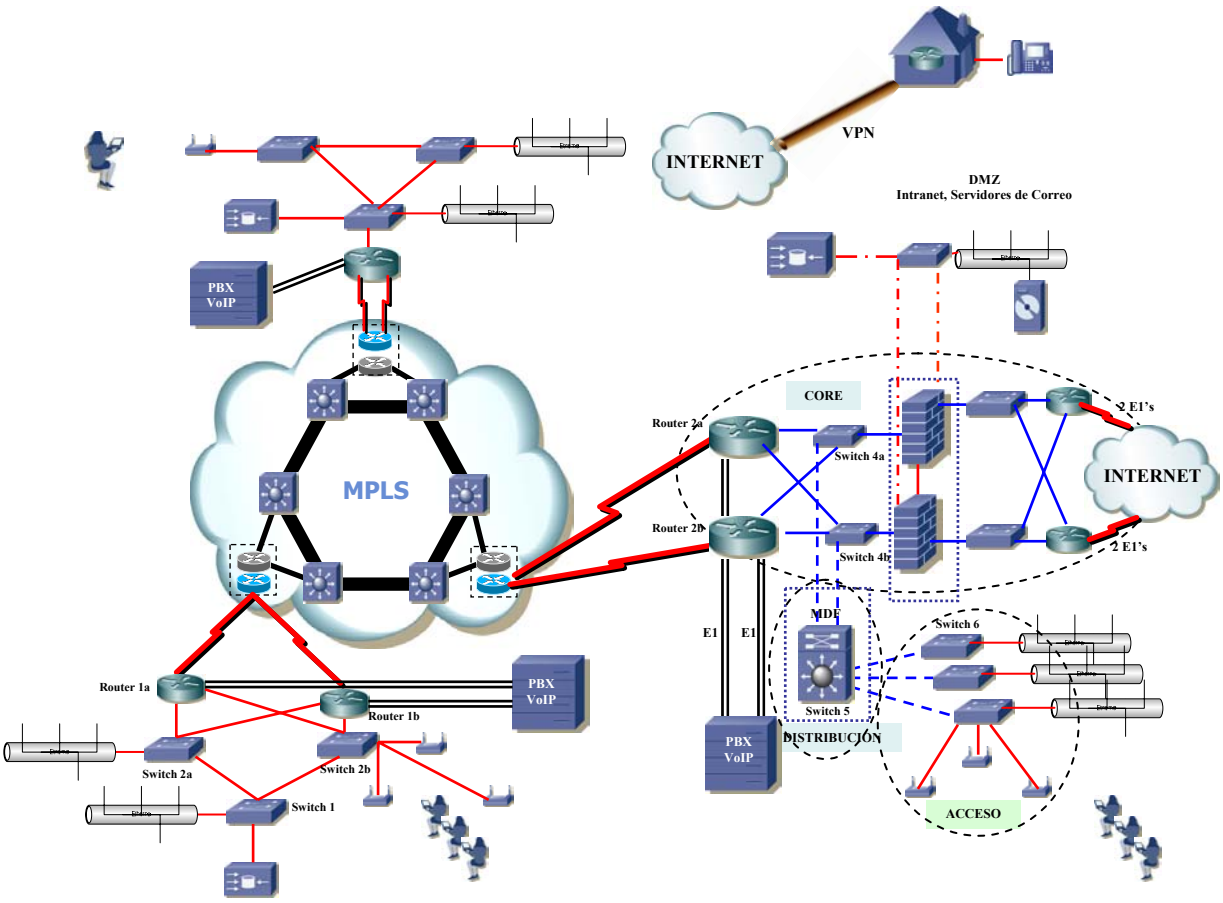


Figura VI.8 Diagrama de Red MPLS.

En el diagrama de red de la figura VI.8 se tiene un diseño de red MPLS, en éste se observan varias diferencias respecto al diagrama de red mostrado en la figura VI.1, dentro de las principales destacan los enlaces y equipos redundantes, así como beneficios que brinda la arquitectura MPLS, ya que el paradigma de sólo alcanzar el destino salto a salto que actualmente supone un freno para el avance de varios enfoques innovadores en el diseño de redes y la optimización del flujo de tráfico, se ve minimizado debido al uso de envío y control independiente de los paquetes utilizando etiquetas, lo cual conlleva a una rápida convergencia en el enrutamiento, ya que ahora la necesidad de publicar la nueva tabla de enrutamiento en todos los dispositivos de ruteo en tránsito y el consumo de recursos en ruteadores, tales como memoria y procesamiento de los ruteadores principales en caso de falla de cualquier enlace WAN, se ve favorecido con el uso de mecanismos que permiten a los dispositivos de ruteo interno, conmutar los paquetes a través de la red desde un router de entrada hacia un router de salida sin tener que analizar la dirección de destino esto se logra combinando los beneficios del envío de paquetes basados en la conmutación de Capa 2 con los beneficios de enrutamiento de Capa 3.

VI.2.1 SITIO LOCAL (OFICINAS GENERALES)

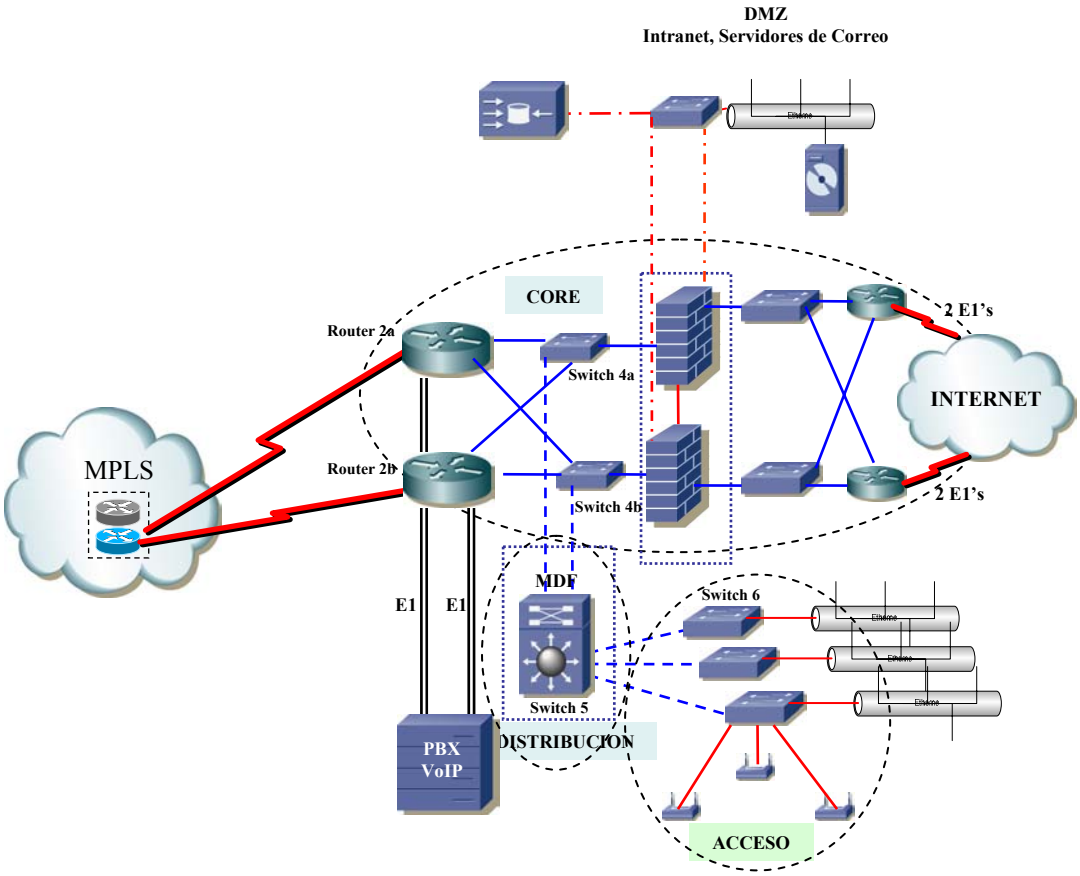


Figura VI.9 Diagrama de Red Sitio Local red MPLS.

En nuestra propuesta de red en el sitio central (figura VI.9), se tienen dos equipos redundantes con sus respectivos enlaces a la red MPLS a los cuales está conectada la red LAN, donde generalmente se encuentran los servidores que proveen servicio primordial de aplicaciones para la operación, con esta configuración se tiene la opción de que los dos equipos se configuren para balancear cargas o en stanby para prevenir la falla de alguno de los equipos o enlaces, la diferencia entre ambas opciones, es que en el balanceo de cargas se utilizan ambos equipos y enlaces de forma activa lo cual beneficia en la repartición de tráfico y procesamiento de paquetes de enrutamiento, en cuanto a la configuración en stanby tanto el equipo como el enlace se tienen en forma pasiva y solo es usado hasta que algún elemento del primer esquema de equipo-enlace falle.

VI.2.1.1 ELEMENTOS DE CORE

En nuestro caso todos los elementos de CORE (figura VI.10), tienen enlaces redundantes y de gran ancho de banda, esto con el fin de aumentar la disponibilidad y evitar posibles cuellos de botella del tráfico pasante.

Los switches hacia la nube de Internet están seguidos de dos *firewalls*. Por medio de la implementación de estos dos *firewalls* en arreglo redundante en el sitio central se garantiza una alta seguridad en la red tanto de ataques internos por medio de una DMZ, donde es posible colocar la granja de servidores de aplicaciones criticas y de ataques externos, así mismo al tener el arreglo redundante se reduce la posibilidad de puntos de falla.

En la zona DMZ se tienen los servidores de correo, servidores de páginas Web y contamos con soluciones de *contenido* que minorizaran el impacto en el tráfico de peticiones que residan en páginas, servidores o servicios de Internet que son acezadas frecuentemente, así se evita el congestionamiento de los enlaces en horas pico y se aprovecha el ancho de banda de los enlaces para actualizar paginas de mayor demanda en horas de poca saturación de estos.

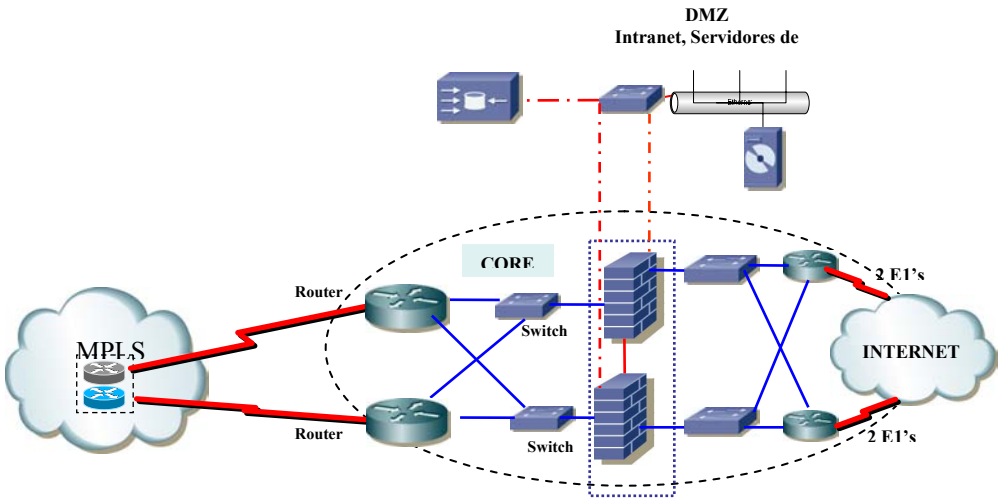


Figura VI.10 Elementos de Core.

VI.2.1.2 DISTRIBUCIÓN

En la parte de distribución (figura VI.11) se tiene un switch multicapas en el cual concentramos los diferentes switches de acceso mediante una topología estrella y cuenta con enlaces redundantes hacia los switches de Core para obtener un alta disponibilidad de red LAN.

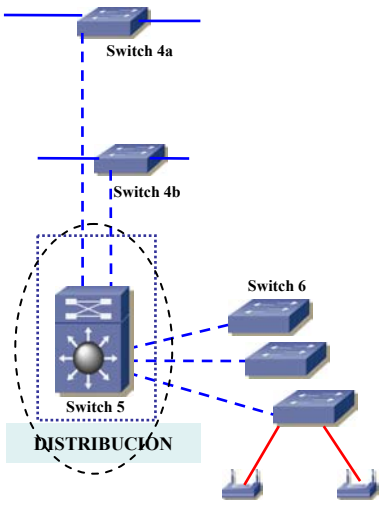


Figura VI.11 Elemento de Distribución.

VI.2.1.3 ACCESO

En la parte de acceso (figura VI.12), se tienen switches que conectan a cada uno de los elementos de la red, estos colocados en una topología estrella, tanto switch como elementos de *access points* de la red inalámbrica, confiando en la alta disponibilidad que ofrece el switch multicapas en la parte de distribución.

Dentro de los aspectos LAN que hay que destacar es la movilidad de los equipos de cómputo personales por medio de la integración de una red híbrida inalámbrica con tecnología OFDM, la cual ofrece un mayor ancho de banda y en conjunto con aplicaciones de autentificación WEP podemos crear una red inalámbrica segura capaz de autentificar a los usuarios.

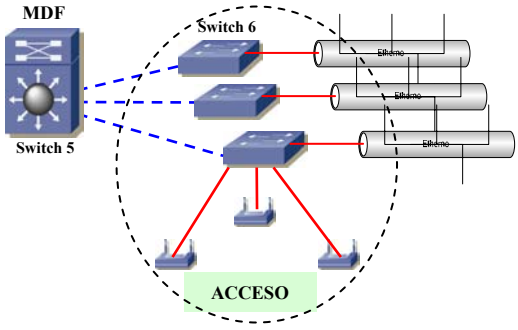


Figura VI.12 Elementos de Acceso.

VI.2.1.4 VOZ SOBE IP

Otro aspecto importante a notar en esta propuesta de red MPLS, es que la red de voz ya se encuentra integrada como otro elemento de la red de datos, con lo cual la

comunicación entre los sitios solo será como si se tratara de una simple extensión dentro de la misma organización, haciendo que no se dependa de la PSTN para enlazarse con dependencias dentro de la misma organización, con lo que se reducen los costos que esto originaría.

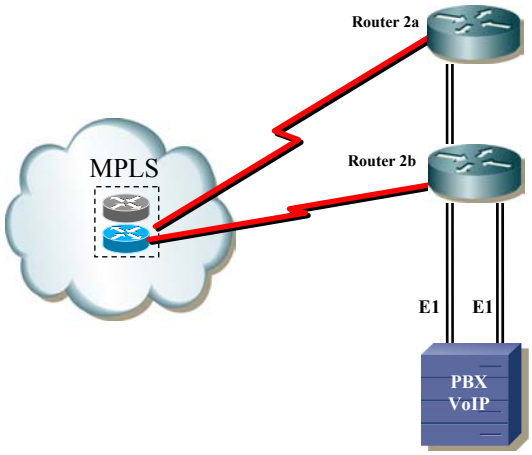


Figura VI.13 Integración de la Red de Voz sobre la misma Red de Datos

También se han propuesto enlaces de gran capacidad hacia la red MPLS, con lo cual se asegura un acceso rápido a los recursos de la red, poca latencia de los servicios de voz y multimedia dentro de la misma y su posible crecimiento, además de las ventajas con que cuenta la arquitectura MPLS, ya que la diferencia más significativa entre las tecnologías MPLS y la tradicional WAN es la forma en que se asignan las etiquetas y la capacidad de transportar una pila de etiquetas adjuntas a un paquete. El concepto de una pila de paquetes habilita nuevas aplicaciones; como la ingeniería de tráfico, las redes privadas virtuales (VPN), el reenrutamiento rápido alrededor de un enlace y los fallos de los nodos.

VI.2.1.5 VPN´s

También se sugiere la implantación de VPNs a través de Internet, con el fin de continuar trabajos pendientes desde el hogar (*home office*) o bien el colocar pequeños abonados o sucursales, para acceder a la red con seguridad través de Internet por ejemplo.

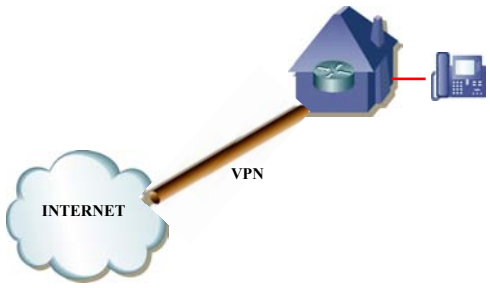


Figura VI.14 Creación de VPN a través de Internet.

Y finalmente la calidad de servicio (QoS) otorgada por la ingeniería de tráfico de la tecnología MPLS, con la cual se puede asegurar el adecuado funcionamiento de las aplicaciones de voz datos y video; además de una mejor administración de la red (tanto LAN como WAN) a través de diferentes tecnologías.

VI.2.2 SITIO REMOTO 1

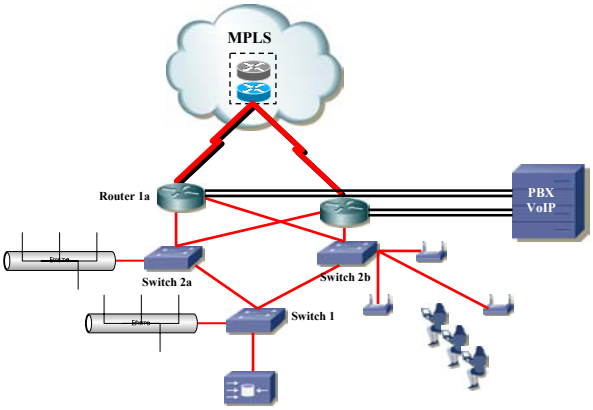


Figura VI.15 Diagrama de Red Sitio Remoto 1.

Los cambios sugeridos para el sitio remoto 1 (figura VI.15) son la utilización de dos routers con enlaces redundantes de mayor ancho de banda para aumentar la disponibilidad de la red, la utilización de la tecnología MPLS como medio de transporte WAN hacia el sitio Local por los beneficios ya mencionados, el cambio en la topología de los switches de la red LAN, la utilización nuevamente del elemento de *contenido* para administrar anchos de banda, la integración de a*ccess points* para tener una red hibrida y obtener los beneficios de movilidad dentro de la red; y por último la integración de los servicios de voz como un elemento más de la red por medio del PBX, con enlaces redundantes hacia cada uno de los routers para aumentar la disponibilidad.

VI.2.3 SITIO REMOTO 2

Al igual que en el sitio remoto 1 los cambios sugeridos, son el uso de enlaces redundantes hacia la red WAN y el uso de la tecnología MPLS como medio de transporte para la comunicación hacia los otros sitios.

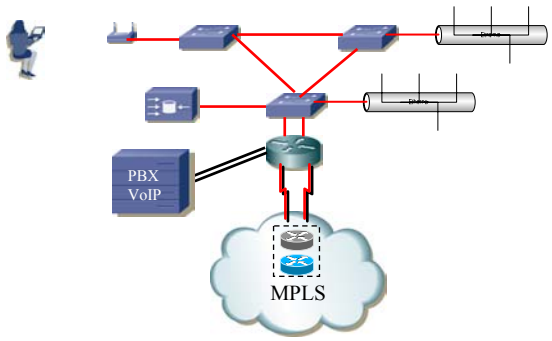


Figura VI.16 Diagrama de Red Sitio Remoto 2.

También se propone el cambio de la topología de la red LAN para tener múltiples caminos dentro de ésta por medio de un anillo y el uso *access points* para tener una red hibrida (figura VI.16); el uso de elemento de *contenido* para disminuir la carga de trafico por medio del enlace MPLS y finalmente, la integración de la red de voz por medio del PBX

VI.3 DISPONIBILIDAD RED FRAME RELAY

Como vimos en capítulos pasados la disponibilidad de las redes depende tanto de las topologías de estas como de los elementos de contra falla que se puedan utilizar. A continuación se muestra como con el simple cambio de una topología de la red se puede aumentar la disponibilidad de ésta, para lo cual se usarán los diagramas de red antes vistos.

Para calcular la disponibilidad de una red hay que tomar en cuenta el método de "Divide y Vencerás", para lo cual es necesario seguir sus pasos que se vieron con anterioridad.

VI.3.1 PASO 1: DETERMINAR ESCENARIOS Y RBD

En este caso se toma como ejemplo el escenario de comunicar un equipo de la red ETH1 con otro equipo de la red ETH2 de la red Frame-Relay mostrada en el diagrama VI.17 y relacionada con la figura VI.1.

Para este escenario se considera el siguiente RBD mostrado en el diagrama de bloques de la siguiente figura VI.17 en el cual se toman los diferentes caminos posibles de la transmisión.

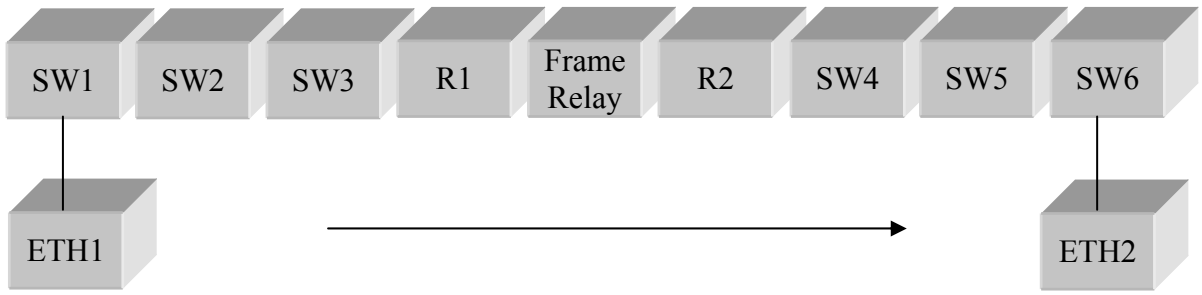


Figura VI.17 Diagrama de Bloques para el RBD de la Red Frame-Relay.

VI.3.2 PASO 2: CALCULAR LA DISPONIBILIDAD DE LOS COMPONENTES DE LA RED

Ahora que se han explorado los flujos de datos para el escenario creado, se puede comenzar a realizar los cálculos de disponibilidad de los componentes de la red, para lo cual se necesita hacer una lista de los aparatos que se incluirán en los cálculos de disponibilidad.

En la tabla VI.1 se describe la disponibilidad de los sistemas para cada aparato usado en nuestro escenario.

Sistema	Disponibilidad
Equipo IP 1	0.99995
Switch 1	0.99993
Switch 2	0.99975
Switch 3	0.99995
Router 1	0.99885
Frame Relay	0.99880
Router 2	0.99885
Switch 4	0.99999
Switch 5	0.99997
Switch 6	0.99995
Equipo IP 2	0.99999

Tabla VI.1 Disponibilidad para cada uno de los elementos de la red Frame-Relay

VI.3.3 PASO 3 CÁLCULOS DE REDUNDANCIA DE CADA ESCENARIO

En esta sección se muestran los cálculos hechos en el paso 3 del algoritmo "Divide y Vencerás". Para cada escenario, se combina la disponibilidad de los aparatos de red

en serie y paralelo hasta estar listos para realizar los cálculos punto a punto de los escenarios. En este caso, de acuerdo con el diagrama, sólo tenemos un escenario para la comunicación, es decir que solo hay una ruta a seguir y por lo tanto no existen secciones paralelas por lo que solo calcularemos una sección serie.

Cálculo de toda la subsección serie.

Disponibilidad ETH1 = **0.99995**
Disponibilidad SW1 = **0.99993**
Disponibilidad SW2 = **0.99975**
Disponibilidad SW3 = **0.99995**
Disponibilidad R1 = **0.99885**
Disponibilidad Frame Relay = **0.99880**
Disponibilidad R2 = **0.99885**
Disponibilidad SW4 = **0.99999**
Disponibilidad SW5 = **0.99997**
Disponibilidad SW6 = **0.99995**
Disponibilidad ETH2 = **0.99999**

Disponibilidad de toda la subsección = ***0.995986***

La cual es la disponibilidad para la subsección correspondiente.

VI.3.4 PASO 4: CÁLCULOS DE DISPONIBILIDAD PUNTO A PUNTO PARA CADA ESCENARIO

Ahora se muestra el cuatro y último paso del método "Divide y Vencerás". Se ha creado un RBD, calculado la disponibilidad para cada componente de la red, y determinado la disponibilidad de las secciones redundantes de nuestra red.

El resto del proceso consiste en realizar los cálculos punto a punto para cada escenario usando la ecuación para disponibilidad serial.

En este caso dado que no se tienen secciones redundantes en la red, por lo tanto la disponibilidad punto a punto será la misma que se calculo en el paso anterior de toda la subsección.

Disponibilidad Total = ***0.995986***

Se puede observar que la disponibilidad es una cifra con solo dos nueves lo cual indica que se tiene una disponibilidad muy baja, por ello, se pude deducir que la topología simple de esta red y la tecnología que se utilizó para el diseño influye en el desempeño de la misma.

VI.4 DISPONIBILIDAD RED MPLS

Ahora nuevamente para el diseño de red propuesto se hará el mismo análisis considerando los elementos de contrafalla para mostrar su influencia en la disponibilidad.

VI.4.1 PASO 1: DETERMINAR ESCENARIOS Y RBD

Ahora se tomará como ejemplo el escenario de comunicar un equipo de la red ETH1 con otro equipo de la red ETH2 pero tomando como referencia la red MPLS mostrada en el diagrama VI.2

En este ejemplo se observa que el diagrama de bloques muestra diferentes caminos del RDB para comunicarse la red ETH1 con la red ETH2 debido a los enlaces redundantes de tal forma que presenta varios casos diferentes tal como se ilustra en la siguiente figura VI.18

VI.4.2 PASO 2 CALCULAR LA DISPONIBILIDAD DE LOS COMPONENTES DE LA RED.

Nuevamente se tienen que explorar los flujos de datos para los diferentes escenarios creados los RBD y así poder comenzar a realizar los cálculos de disponibilidad de los componentes de la red. Así, considerando los mismos valores para los diferentes equipos se tiene:

Sistema	Disponibilidad
Equipo IP 1	0.99995
Switch 1	0.99993
Switch 2ª	0.99995
Switch 2b	0.99995
Router 1ª	0.99885
Router 1b	0.99885
MPLS	0.99980
Router 2ª	0.99885
Router 2b	0.99885
Switch 4ª	0.99999
Switch 4b	0.99999
Switch 5	0.99997
Switch 6	0.99995
Equipo IP 2	0.99999

Tabla VI.2 Disponibilidad para cada uno de los elementos de la red MPLS.

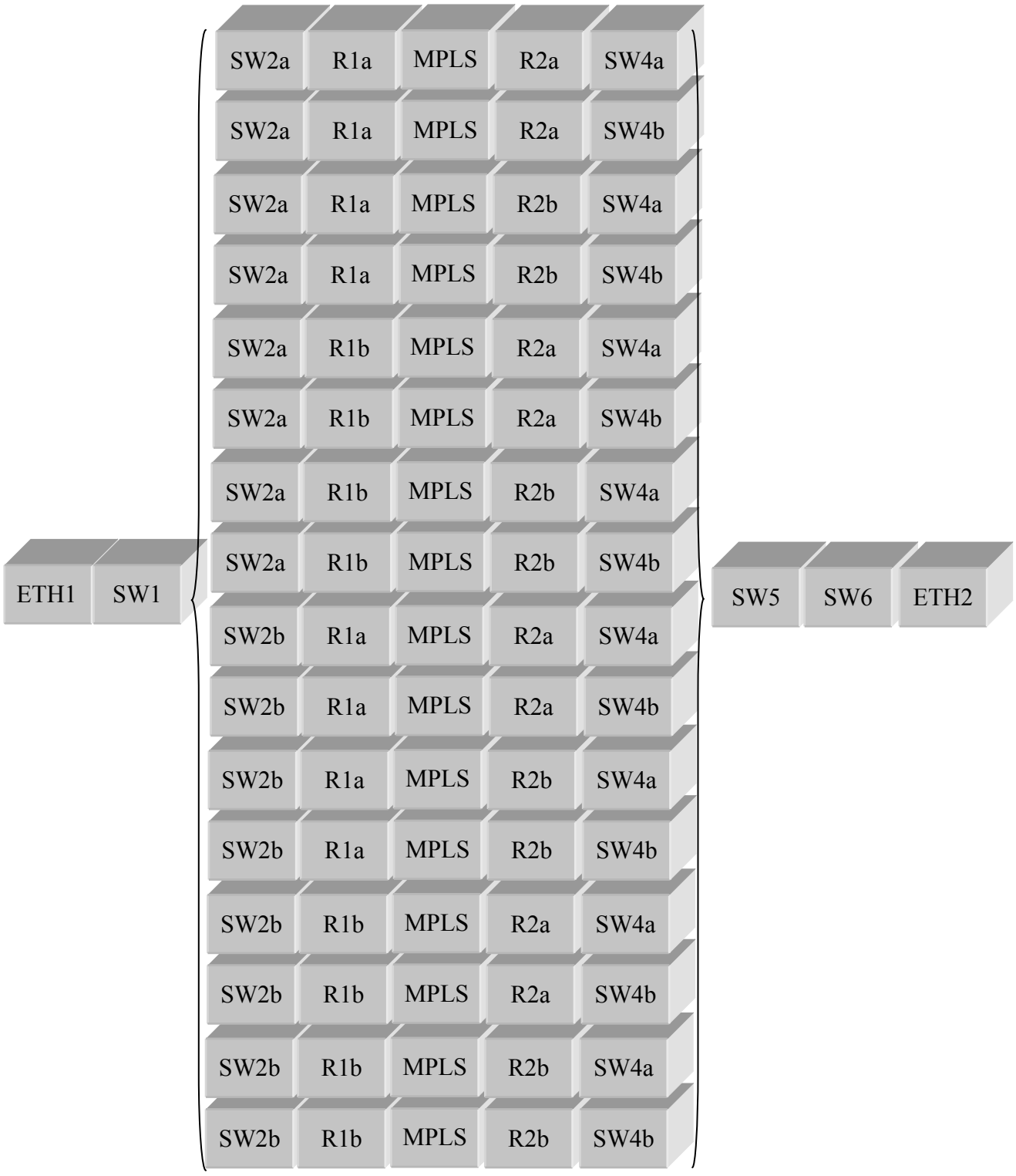


Figura VI.18 Diagrama de Bloques para el RBD de la Red MPLS.

VI.4.3 PASO 3 CÁLCULOS DE REDUNDANCIA ESCENARIO POR ESCENARIO.

Ahora se vuelve a realizar los cálculos para cada escenario, así se encuentran las disponibilidades en las secciones serie y paralelo para finalmente obtener la disponibilidad punto a punto.

Para todas las secciones serie en los enlaces redundantes se tiene que las disponibilidades de los switches SW2a y SW2b así como los router R1a y R1b son iguales y exactamente del otro lado de la nube MPLS, se tienen las mismas disponibilidades para R2a y R2b así como SW4a y SW4b por lo que las disponibilidades para todas las secciones serie intermedias son iguales; por lo tanto:

disponibilidad serie intermedias = ***0.99944011***

Ahora para calcular la disponibilidad de toda la sección paralela se tiene

disponibilidad paralela = **1 – [(1 – 0.99944011)*(1 – 0.99944011)*(1 – 0.99944011)**
***(1– 0.99944011)*(1 – 0.99944011)*(1 – 0.99944011)**
***(1– 0.99944011)*(1 – 0.99944011)*(1 – 0.99944011)**
***(1– 0.99944011)*(1 – 0.99944011)*(1 – 0.99944011)**
***(1– 0.99944011)*(1 – 0.99944011)*(1 – 0.99944011)**
***(1– 0.99944011)*(1 – 0.99944011)]**

disponibilidad paralela ≅ ***1***

Por lo que se observa que gracias a los equipos y enlaces redundantes se aumenta considerablemente la disponibilidad de la red

VI.4.4 PASO 4 CÁLCULOS DE DISPONIBILIDAD PUNTO A PUNTO PARA CADA ESCENARIO

Finalmente, obtenida la disponibilidad paralelas y serie intermedias, sólo queda obtener la disponibilidad serie punto a punto en ambas redes para lo cual se tiene que multiplicar el resultado por la disponibilidad del SW1, SW5, SW6 y las disponibilidad de ambos equipos de la red como se muestra con los siguientes cálculos:

disponibilidad total = **(0.99995*0.99993*1*0.99997*0.99995*0.99999)**

Disponibilidad total = ***0.99979002***

Puede observarse que la diferencia es de casi dos nueves con respecto a la red anterior (de *0.995986* a *0.99979002*) con lo cual se ve claramente que aunque se utilizaron equipos con las mismas características, se ha mejorado la disponibilidad de la red, y aun más al poner los equipos en stanby con enlaces redundantes.

Además de lograr mejoras la disponibilidad de la red, con ayuda de estas nuevas tecnologías, se pueden obtener beneficios extras como son: la movilidad (gracias a las redes híbridas inalámbricas), seguridad con la red MPLS, así como la facilidad de poder poner *home office* mediante VPNS a través de Internet y aprovechar el ancho de banda de los enlaces gracias al uso de elementos que disminuyen el tráfico en horas pico de la red, aprovechando así los enlaces para las aplicaciones multimedia y en demanda de datos dentro de horarios de mucho trafico.

VI.5 CONSIDERACIONES EXTRAS

Todas aquellas organizaciones que cuentan aún con redes tradicionales, analizan sus presupuestos en tecnologías de información y sólo aquellos proyectos que aportan un aumento inmediato de beneficios o importantes ahorros, tienen posibilidad de recibir apoyo o ser actualizados.

Sin embargo, es muy importante tomar decisiones acertadas, tanto en los negocios como en la tecnología, para asegurar que la plataforma tecnológica evolucione sin dejar de satisfacer las necesidades de los usuarios, a la vez que maximiza la flexibilidad y explota las economías de escala posibles.

En este entorno la flexibilidad ha sido de mayor importancia y ha ganado posiciones en el orden de prioridades gracias al aumento de las reubicaciones de usuarios y al desarrollo de nuevas aplicaciones. La flexibilidad también es esencial para lograr los objetivos del entorno *e-business*, el cual es conectar los sistemas internos con los clientes, socios y proveedores en las aplicaciones de Gestión de Relaciones con los Clientes (CRM "*Customer Relationship Management*") y de la cadena de suministro. Las redes tradicionales basadas en circuitos fijos, ya sean líneas alquiladas o PVC (circuitos virtuales permanentes) dentro de una red Frame Relay o ATM (modo de transferencia asíncrona), no son las más adecuadas para este nuevo entorno *e-business*. Por ello se requiere una red que soporte todo tipo de conexiones y se pueda reconfigurar con facilidad para introducir nuevos usuarios o añadir servicios adicionales. Esta red también debe permitir la variación de las calidades de servicio para poder hacer frente tanto a sencillas transferencias de archivos sin limitación de tiempo como a aplicaciones multimedia en tiempo real, y el flujo de vídeo y voz.

Vale la pena remarcar que los servicios tradicionales como ATM, Frame Relay y de conexión telefónica siguen teniendo su lugar y que lo conservarán por varios años más. Actualmente, el interés por realizar migraciones fulminantes a las redes IP creadas con nuevos objetivos es, en efecto, poco notable.

VI.6 VENTAJAS EXTRAS DE MPLS

El ideal de las organizaciones es una tecnología que facilite esta transición y, sobre todo, que genere beneficios lo más rápido posible al menor costo. Así pues la solución mas factible es *Multi Protocol Label Switching* (MPLS), el cual se ha ganado el apoyo casi universal del sector como avance para las redes IP e Internet. La principal ventaja de MPLS es que combina los beneficios de la transmisión de datos sin conexión "entre dos puntos cualquiera" y de la transmisión con conexión punto a punto, a la vez que elimina sus inconvenientes. Estas características aparentemente técnicas son, o deberían ser, importantes para los diseñadores de redes empresariales ya que presentan implicaciones de gran alcance. Ahora pueden migrar a una infraestructura escalable y de gran flexibilidad, que les permita conectarse con quien deseen y con la calidad de servicio necesaria, aprovechando, al mismo tiempo, las economías de escala de la red central IP global.

La transmisión punto a punto tiene la ventaja de ser segura, fiable y capaz de ofrecer la calidad de servicio (QoS) necesaria para todo tipo de datos, incluyendo el tráfico en tiempo real como la voz, pero presenta los inconvenientes de ser poco flexible e incapaz de aprovechar al máximo las tecnologías que una red compartida puede ofrecer. Hasta la aparición de MPLS, las redes IP sin conexión, donde no hay una configuración completa de sesiones, eran justo lo contrario. Tenían la ventaja de evitar los defectos de las redes con conexión y el inconveniente de no aprovechar sus ventajas. A finales de los años 90, se produjeron los primeros intentos de eliminar todos los defectos y crear redes VPN IP seguras y sólidas, aunque tuvieron un éxito parcial, debido en gran medida, a un excesivo sacrificio de la flexibilidad. En concreto, se aplicó la idea de *tunnelling* de IP para conseguir sesiones completamente protegidas, pero se tenía que configurar una relación punto a punto antes de poder iniciar la comunicación. Esto representa gastos generales excesivos para muchas aplicaciones de transacciones en las que la cantidad de información que se transmite es relativamente pequeña, lo que es bastante frecuente en el comercio electrónico y *e-business*. En realidad, se sobrepuso una estructura punto a punto con conexión encima de la red central IP sin conexión.

MPLS logra el mismo nivel de seguridad que el *tunnelling* IP, no necesita esta superposición al mantener una separación estricta entre cada VPN y asegura que cada paquete IP del cliente se coloca correctamente en la red.

También es de vital importancia contar con soporte para los diferentes niveles de QoS si sólo se dispone de una red para todos los formatos de información, incluyendo aplicaciones de voz, vídeo, correo electrónico, transferencia de archivos y programas por lotes existentes. MPLS facilita este soporte para QoS mediante unas etiquetas que permiten a los direccionadores o conmutadores de la red identificar los requisitos de cada paquete de IP y darles la prioridad adecuada. Otro aspecto de crucial importancia es que las etiquetas también identifican la ruta que hay que seguir y evitan tener que comprobar las tablas en cada paso.

Por encima de todo, las organizaciones desean migrar a su propio ritmo, lo que significa que los nuevos servicios deben poder coexistir e interoperar con los ya existentes. Esta exigencia hace imprescindible la elección de un socio tecnológico capaz de soportar una mezcla de servicios que incluya conexiones ATM, Frame Relay y de conexión telefónica, así como redes VPN IP. El socio tecnológico debe ofrecer y soportar las distintas opciones, pero MPLS también puede desempeñar una función esencial al poder trabajar tanto con ATM y Frame Relay como con IP. Esta tecnología facilita el establecimiento de servicios coherentes en las redes con una mezcla de protocolos IP, ATM y Frame Relay.

VI.7 COMPARACIÓN DE GASTOS DE LA RED FRAME RELAY Y MPLS

Ahora bien para aclarar el punto de beneficios que puede traer el invertir en nuevas tecnologías hacemos un pequeño análisis comparativo del costos y que trae el invertir en nueva tecnología tomando en cuenta los diagramas de red mostrados en las figuras VI.1 y VI.8.

Hemos considerando que en ambas redes el mayor trafico de las llamadas son llamadas internas de la misma organización y que en el primer diagrama de red para hacer dichas llamadas es necesario hacerlas por medio de la PSTN, para este escenario tenemos que los gastos de la organización seria en llamadas de larga distancia si se considera que se tienen lugares remotos, o llamadas locales en el mejor de los casos. Ahora bien considerando ahora la red de la figura VI.8 todas esas llamadas internas ya no viajarían a través de la PSTN si no que estas se realizarían a través de la misma red de la organización (como una simple extensión) aprovechando los enlaces de la misma red MPLS, lo cual se traduciría en el ahorro de esas llamadas, y tendría el beneficio de asegurar una buena calidad de voz debido a los diferentes niveles de QoS que soporta la misma tecnología.

Por ejemplo para hacer una ejemplificación de gastos, se consideran muchas veces dentro de la misma organización, que es necesario contar un centro de atención de

llamadas las cuales la gran mayoría son llamadas internas de ayuda ó dudas de gente que labora dentro de la misma organización, ahora si se consideran los siguientes gastos de llamadas telefónicas para dichas llamadas aparte de los gastos de los enlaces rentados para la comunicación de datos resulta que:

Gasto por llamada local 1.48
Gasto por llamada larga distancia nacional 3.48 por minuto

Precios mensuales de los circuitos permanentes virtuales servicio de Frame Relay nacional:

Kbps/Distancia	**0 – 49 Kms.**	**50 – 99 Kms.**	**100 – 199 Kms.**	**200 – 399 Kms.**	**400 – 749 Kms.**	**750 – 1199 Kms.**	**1200 o más Kms.**
10	42	75	113	225	360	600	900
16	53	133	200	399	638	1,064	1,596
20	59	146	219	439	702	1,170	1,756
24	64	161	241	483	772	1,287	1,931
32	67	166	250	499	798	1,330	1,995
40	73	183	275	549	878	1,463	2,195
48	80	201	302	603	966	1,609	2,414
64	95	238	356	713	1,140	1,900	2,850
96	143	356	534	1,069	1,710	2,850	4,275
128	190	485	728	1,455	2,328	3,880	5,820
192	285	738	1,106	2,212	3,540	5,900	8,850
256	380	980	1,470	2,940	4,704	7,840	11,760
384	570	1,485	2,228	4,455	7,128	11,880	17,820
512	760	1,980	2,970	5,940	9,504	15,840	23,760
768	1,140	2,970	4,455	8,910	14,256	23,760	35,640
1024	1,520	3,960	5,940	11,880	19,008	31,680	47,520
1792	1,948	4,950	7,920	14,850	22,869	37,125	53,460
2048	2,375	5,940	9,900	17,820	26,730	42,570	59,400

Tabla VI.3 Costos de los Servicios Frame-Relay.

Como observamos, si los sitios de nuestra organización se encuentran cercanos sigue siendo muy barato seguir con la misma tecnología pero entre mas alejados se encuentren los sitios suben los costos, tanto de los enlaces como los de las llamadas con lo cual es posible considerar una posible migración de tecnología que si bien aunque es un poco mas cara, vale la pena valorar los beneficios extras que quedemos obtener de dicha tecnología nueva.

Ahora bien considerando la propuesta de red tenemos que las llamadas internas por medio de la PSTN ya no serian necesarias, ya que estas viajarían a través de la propia red teniendo solo los gastos de la renta de los enlaces a la red MPLS por medio de VPN a los cuales sus costos se muestran a continuación:

Puerto / Capacidad (Kbps)	Precio
64	$1,926.55
128	$ 2,146.98
2048	$10,635.31

Tabla VI.4 Costos de los Servicios MPLS

Con lo que vemos que si bien los gastos de renta mensual de los enlaces son ligeramente mayores, el gasto vale la pena ya que se ahorrarían las llamadas realizadas por medio de la PSTN, con la seguridad de tener una buena calidad de voz y seguridad de los datos entre otros beneficios antes mencionados.[e]

CONCLUSIONES

Con el crecimiento y desarrollo de la tecnología cada día tenemos más posibilidades de soluciones a los diferentes problemas que se nos presentan en el diseño de las redes de telecomunicaciones.

Pero si bien es cierto que cada día tenemos más tecnologías para implantar en el diseño de las redes, hay varios aspectos muy importantes que hay que considerar. Entre los principales tenemos la interoperabilidad, flexibilidad de crecimiento y sobre todo los gastos que repercute ocupar nuevas tecnologías. Todos estos aspectos que tienen que ver con la adecuada solución a los requerimientos que se busca en el diseño de la red.

Cabe señalar que por su gran popularidad resulta obvio que todos los sistemas y tecnologías que cumplen y cumplan con las características que propone el modelo de referencia OSI tendrán una mejor aceptación debido a que aseguramos la interoperabilidad de estas nuevas tecnologías, así como la flexibilidad de crecimiento de las redes y es en estos casos cuando es posible buscar una solución de crecimiento con tecnologías que se adecuen a las necesidades de crecimiento de las redes ya instaladas.

El reto de hoy en día es buscar la solución a las nuevas necesidades que exigen las aplicaciones de los usuarios, la disponibilidad en todo momento de los servicios que se ofrecen a través de estas y la confidencialidad de la información que transita por dichas redes. Pero para esto es necesario saber y conocer las diferentes tecnologías existentes en el mercado.

Casi siempre se toma como base las tecnologías existentes que ya están probadas pero es necesario valorar y considerar sus limitaciones las cuales son en gran parte la base de las propuestas de diseño de las redes nuevas.

Cabe destacar que las principales tecnologías LAN ocupadas actualmente están basadas en la tecnología Ethernet, con sus diferentes características tanto para la parte alambrica CSMA/CD y la parte inalámbrica DSSS, así como Frame Relay, ATM, ISDN, XSDL, etc. para enlaces dedicados en la parte WAN. Todas estas son tecnologías en las cuales se basan la mayor parte de las redes ya instaladas.

Dichas redes que si bien en su tiempo fueron diseñadas para solucionar las demandas, se enfrentan a nuevas necesidades tales como ancho de banda, disponibilidad, seguridad, movilidad, interoperabilidad, etc. Principalmente las limitantes del ancho de banda son más evidentes al querer integrar soluciones de voz, video y a su vez varios protocolos y aplicaciones por el mismo medio.

Todas estas nuevas necesidades nos hacen recurrir a las tecnologías emergentes de hoy en día, que se ofrecen o pretenden ser ofrecidas en gran medida por los proveedores de servicios (ISP, carriers, operadores telefónicos, bancos, etc.).

Como se ha mencionado a lo largo de este trabajo la necesidad de diseños de redes confiables y de alta disponibilidad se ha vuelto una necesidad implícita para el funcionamiento y operación de las empresas que ofrecen servicios y transacciones de negocios en cualquier momento, ofreciendo como valor agregado la seguridad en sus operaciones.

Dentro de los aspectos primordiales a considerar para una red de alta disponibilidad, tenemos: l*a confiabilidad y disponibilidad de la red*, que consiste en tener la red disponible las 24 horas los 365 días del año y con la certeza de que las transferencias de información sean confiables a través de la utilización de topologías con enlaces redundantes de alta capacidad, *la eficiencia,* la cual optimiza el uso de recursos de la red utilizando por ejemplo diseños que segmenten el tráfico en la red, *la sensibilidad de la red* para responder a las múltiples demandas de la red (voz, video, multimedia, etc.), ya que gracias a implementaciones de QoS, es posible clasificar el tráfico por prioridades, *la adaptabilidad* para convivir e ínter operar con diversos tipos de tecnologías y finalmente *la accesibilidad* y a la vez *la seguridad*, lo cual sugiere tener la capacidad de poder acceder a la red, desde cualquier punto, no importando la

forma de acceso (dial-up, enlace dedicado, VPN, servicios conmutados, etc.), siempre y cuando manteniendo la integridad de la red.

Para complementar el diseño de alta disponibilidad es necesario considerar el uso de tecnologías de ultima generación como algunas posibles soluciones a las limitaciones de las tecnologías utilizadas actualmente, dentro de las cuales tenemos y proponemos MPLS, VPN, OFDM, PWE3, IPV6, etc.

Resaltando el uso de tecnologías de última generación hay que considerar que estas aun se siguen complementando con el uso de tecnologías pasadas como lo es IPV4, Ethernet, PDH, SDH, X.25, Token-Ring, Frame Relay, ATM, etc., las cuales se tienen muy arraigadas en la operación primordial de muchas empresas. Es por ello que las tecnologías propuestas deben cumplir con el compromiso de adaptabilidad, el cual es necesario para ir desplazando poco a poco el uso de tecnologías obsoletas como lo es por ejemplo X.25 y Token-Ring. No obstante cabe destacar que el desalojo de viejas tecnologías generalmente se lleva de manera moderada debido a los altos costos que implica el cambio de plataformas tecnológicas, aunque la recuperación de inversión es lenta, el desempeño de la red se ve beneficiado y se tiene la posibilidad de explotar nuevos nichos de mercado.

En nuestro análisis de propuesta de red, podemos observar una serie de cambios a la antigua red ya instalada, con la finalidad de lograr primeramente la integración de la red de voz y video dentro de la red de datos, así como aumentar la disponibilidad de dicha red. Para lograr esto se proponen varios cambios drásticos como son: cambiar las topologías utilizadas en la red, reemplazar equipos con distintas capacidades técnicas y tecnológicas, incrementar los anchos de banda en los enlaces y sobre todo la redundancia de los mismos para lograr una mejora en el desempeño de la red.

Por último cabe destacar que con el simple cambio de las topologías podemos logar un gran aumento de la disponibilidad de nuestra red y aun más si lo complementamos con la integración de enlaces redundantes hacia la parte WAN, y con la implementación de la tecnología MPLS como tecnología de transporte pretendemos clasificar el tráfico, a través de prioritizar el tráfico de voz y video sobre el tráfico convencional y asegurar la entrega correcta de estos servicios, así mismo que esta tecnología brinda una gran flexibilidad en el manejo de tráfico de voz, datos y video por lo cual pretende y apunta a ser en los próximos años la tecnología principal a utilizar y sobre todo a ser comercializada por los grandes proveedores de servicios debido al gran desarrollo de estándares sobre la misma.

Finalmente podemos decir que las redes de comunicaciones se han vuelto una parte fundamental en nuestras vidas y por lo tanto es necesario contar con redes sumamente confiables, esto solo puede ser posible a través de un excelente diseño de red en el cual se toman a las tecnologías emergentes como

herramientas necesarias para lograr este propósito o bien para proporcionar una mejora a las nuevas demandas que exigen hoy en día las nuevas aplicaciones.

ANEXO

LAS SERIES DE FOURIER

En general, una serie de Fourier puede escribirse para cualquier función periódica como una seire de términos que incluyen funciones trigonométricas con la siguiente expresión matemática:

$$f(t) = A_0 + A_1 \cos\alpha + A_2 \cos 2\alpha + A_3 \cos 3\alpha + ... + A_n \cos n\alpha +$$
$$B_1 sen\beta + B_2 sen2\beta + B_3 sen3\beta + ... + B_n sennn\beta$$

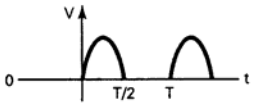
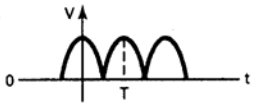
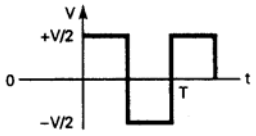
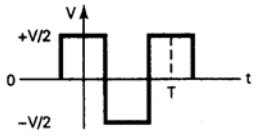
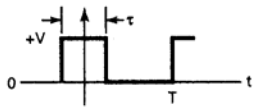
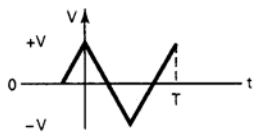
en donde α=β.

La ecuación anterior afirma que la forma de onda *f(t)* consiste de un valor promedio, una serie de funciones coseno, en las cuales cada término sucesivo tiene una frecuencia que es un múltiplo entero de la frecuencia del primer término coseno

en la serie, y una serie de funciones seno en las cuales cada término sucesivo tiene una frecuencia que es un múltiplo entero de la frecuencia del primer término seno se la serie. No existen restricciones sobre los valores o valores relativos de las amplitudes para los términos seno o coseno. La ecuación II.2 se expresa en palabras de la siguiente manera: Una forma de onda periódica consiste de una componente promedio y una serie de armónicas de ondas seno y coseno relacionadas. Una armónica es un múltiplo entero de la frecuencia fundamental. La frecuencia fundamental es la primera armónica y es igual a la frecuencia de la forma de onda. El segundo múltiplo de la frecuencia fundamental se llama la segunda armónica, etc. La frecuencia fundamental es la mínima cantidad de frecuencia necesaria para representar una forma de onda. Por lo tanto la ecuación II.2 puede reescribirse como:

$F(t)$= cd + fundamental + 2ª armónica + 3ª armónica +….n armónica

La tabla es un resumen de la serie de Fourier para varias de las formas de onda periódicas no senoidales más comunes.

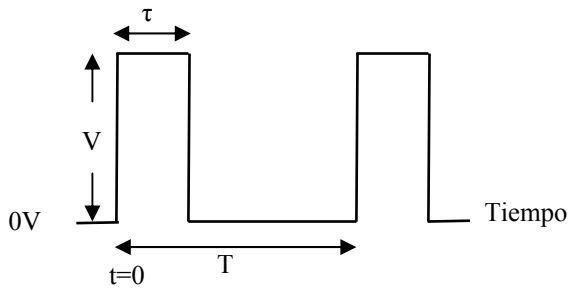
Forma de onda	**Serie de Fourier**
	$v(t) = \frac{V}{\pi} + \frac{V}{2}\operatorname{sen}\omega t - \frac{2V}{3\pi}\cos 2\omega t - \frac{2V}{15\pi}\cos 4\omega t + \cdots$ $v(t) = \frac{V}{\pi} + \frac{V}{2}\operatorname{sen}\omega t + \sum_{N=2}^{\infty} \frac{V[1+(-1)^N]}{\pi(1-N^2)}\cos N\omega t$
	$v(t) = \frac{2V}{\pi} + \frac{4V}{3\pi}\cos\omega t - \frac{4V}{15\pi}\cos 2\omega t + \cdots$ $v(t) = \frac{2V}{\pi} + \sum_{N=1}^{\infty} \frac{4V(-1)^N}{\pi[1-(2N)^2]}\cos N\omega t$
	$v(t) = \frac{2V}{\pi}\operatorname{sen}\omega t + \frac{2V}{3\pi}\operatorname{sen} 3\omega t + \cdots$ $v(t) = \sum_{N=\text{impar}}^{\infty} \frac{2V}{N\pi}\operatorname{sen} N\omega t$
	$v(t) = \frac{2V}{\pi}\cos\omega t - \frac{2V}{3\pi}\cos 3\omega t + \frac{2V}{5\pi}\cos 5\omega t + \cdots$ $v(t) = \sum_{N=\text{impar}}^{\infty} \frac{V\operatorname{sen} N\pi/2}{N\pi/2}\cos N\omega t$
	$v(t) = \frac{Vt}{T} + \sum_{N=1}^{\infty}\left(\frac{2Vt}{T}\frac{\operatorname{sen} N\pi t/T}{N\pi t/T}\right)\cos N\omega t$
	$v(t) = \frac{4V}{\pi^2}\cos\omega t + \frac{4V}{(3\pi)^2}\cos 3\omega t + \frac{4V}{(5\pi)^2}\cos 5\omega t + \cdots$ $v(t) = \sum_{N=\text{impar}}^{\infty} \frac{4V}{(N\pi)^2}\cos N\omega t$

Resumen de la Serie de Fourier

SERIES DE FOURIER PARA UNA FORMA DE ONDA RECTANGULAR

Para las comunicaciones de datos es frecuente utilizar pulsos rectangulares. Una forma de onda que enseña una cadena de pulsos rectangulares se muestra en la figura siguiente. El ciclo de trabajo para la forma de onda es la relación del tiempo activo del pulso al periodo de la forma de onda. Matemáticamente un ciclo de trabajo es:

$$DC = \frac{\tau}{T}$$



Forma de onda de pulso rectangular

No obstante del ciclo de trabajo, una forma de onda rectangular consiste de una serie de armónicas relacionadas con ondas seno. De este modo, la amplitud de las componentes espectrales depende del ciclo de trabajo. La serie de Fourier para una forma de onda de voltaje rectangular con simetría par es:

$$v(t) = \frac{2V_T}{T}\left[\frac{senx}{x}(\cos\omega t) + \frac{sen2x}{2x}(\cos 2\omega t) + ... + \frac{sennx}{nx}(\cos n\omega t)\right]$$

Las siguientes características se aplican para todas las formas de onda rectangulares repetitivas:

- La componente cd es ingual a los tiempos de la amplitud del pulso del ciclo de trabajo.
- Existen componentes de 0 V en la frecuencia 1/τ hertz y todos los múltiplos enteros de esta frecuencia cuando T=n τ, en donde n= cualquier entero impar.
- La envolvente del tiempo de amplitud contra frecuencia de las componentes espectrales toma la forma de una onda seno amortiguada en la cual todas las componentes espectrales el los lóbulos impares son

positivos y todas las componentes espectrales en los lóbulos pares son negativos.

TRANSFORMADAS DISCRETAS Y RÁPIDAS DE FOURIER

Muchas formas de onda encontradas en los sistemas de comunicaciones típicos no pueden definirse satisfactoriamente por expresiones matemáticas. De este modo, su comportamiento en el dominio de la frecuencia de las señales que se están coleccionando en el dominio del tiempo (es decir, en el tiempo real). Esta es la razón por la cual fue elaborada la transformada discreta de Fourier. Con la transformada discreta de Fourier, una señal en el dominio del tiempo se muestra en tiempos discretos. Las muestras se alimentan a una computadora en donde un algoritmo calcula la transformada. En consecuencia, el tiempo de cálculo es proporcional a n^2, donde n es el número de muestras. Para cualquier número razonable de muestras, el tiempo de cálculo es excesivo. Consecuentemente en 1965 se desarrolló un nuevo algoritmo llamada la *Transformada Rápida de Fourier* o FFT . Con el FFT el tiempo de cálculo es proporcional a $2n$ en vez de n^2.

ESTÁNDARES DE TRANSMISIÓN SÍNCRONA

SONET[1] y SDH[2] superan los inconvenientes de las redes PDH y permiten a los proveedores de servicios otorgar conexiones de alta tasa de bits "*high-bit-rate*", por arriba de los 155 Mbps.

Estas conexiones son típicamente requeridas hoy en día donde se han incrementado las necesidades de transporte de datos. SONET y SDH permiten construir servicios de redes TDM[3] sobre plantas de fibra óptica. A pesar de que SONET es un estándar TDM sincróno Norte Americano, SDH es un estándar TDM comúnmente utilizado en Europa y Japón. Porque SDH puede verse como un estándar global (y SONET se halla como un subconjunto de SDH), la interoperabilidad puede ser asegurada en ciertos niveles.

Tanto SONET como SDH definen jerarquías digitales de multiplexado y debe asegurarse su compatibilidad de equipos e implementación de redes síncronas. La funcionalidad básica, es que la señal del cliente de diferentes tipos de servicios, tales como E0, E1, DS0, T1, ATM, y otros, son mapeados dentro de un apropiado

[1] SONET: Red Óptica Síncrona (*Synchronous Optical Network*)
[2] SDH: Jerarquía Digital Síncrona (*Synchronous Digital Hierarchy*)
[3] TDM: Multiplexado por División de Tiempo (*Time Division Multiplexing*)

contenedor de carga útil (*payload*) que es entonces multiplexado dentro de una señal óptica síncrona.

Tanto SONET como SDH adecuan jerarquías TDM no-síncronas. SONET incluye jerarquías Norte Americanas, las cuales están basadas en señales DS1, combinando 24 DS0s (canales de 56 Kbps) dentro de un stream[4] de 1.54 Mb. SDH integra las jerarquías Europeas, las cuales están basadas sobre señales de E1, combinando 32 E0s (canales de 64 Kbps) dentro de un E1 con una velocidad de 2.048 Mbps, como puede observarse en la tabla.

Tasa norte americana			tasa europea		
Señal	**Velocidad**	**Canales**	**Señal**	**Velocidad**	**Canales**
DS0	64 Kbps	1 DS-0	E0	64 Kbps	1 E-0
DS1	1.54 Mbps	24 DS-0s	E1	2.048 Mbps	32 E-0s
DS2	6.3 Mbps	96 DS-0s	E2	8.45 Mbps	128 E-0s
DS3	44.8 Mbps	28-DS-1s	E3	34 Mbps	16 E-1s
No definida			E4	140 Mbps	64 E-1s

Jerarquías TDM Norte Americanas y Europeas

SONET, el cual fue desarrollado primero, especificando una tasa de transmisión básica de 51.48 Mbps, llamado *Señal de Transporte Síncrona 1* (STS-1)[5]. El equivalente de señal óptica es llamado *Portadora Óptica 1* (OC-1)[6]. Para asegurar que tanto SONET y SDH correspondan dentro de un jerarquía común de multiplexado, SDH define como nivel básico, el *Módulo de Transporte Síncrono 1* (STM-1)[7], con 155.52 Mbps, el cual es tres veces el nivel básico de SONET. Las tasas ópticas de ambas jerarquías se muestran en la tabla.

Sonet	TASA DE BITS	sdh
STS-1 / OC-1	51.84 Mbps	-
STS-3 / OC-3	155.52 Mbps	STM-1
STS-12 / OC-12	622.08 Mbps	STM-4
STS-24 / OC-24	1244.16 Mbps	-
STS-48 / OC-48	2488.32 Mbps	STM-16
STS-192 / OC-192	9953.28 Mbps	STM-64

Tasa de interfaces de Jerarquías de Multiplexado SONET/SDH.

[4] stream: Para propósitos de esta tesis se manejará como flujo de datos
[5] STS: Señal de Transporte Síncrona (*Synchronous Transport Signal 1*)
[6] OC: Portadora Óptica (*Optical Carrier*)
[7] STM: Módulo de Transorte Síncrono (*Synchronous Transport Module*)

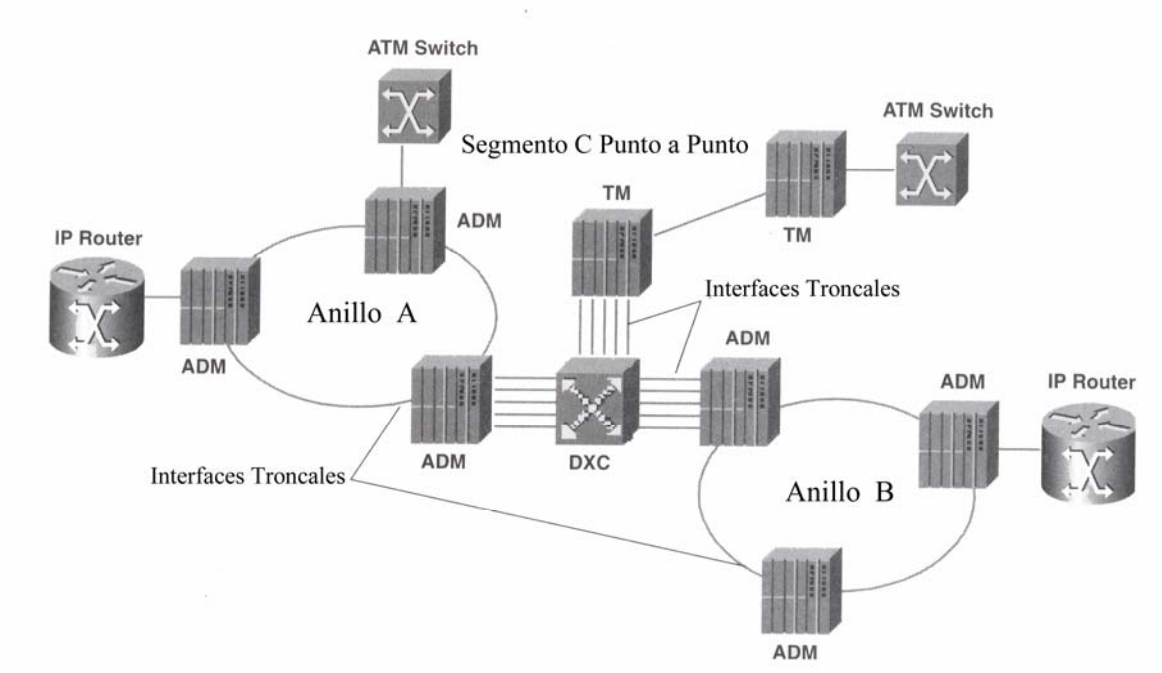
CONSTRUYENDO UNA RED COMPLEJA DE TRANSPORTE SONET/SDH

Una red típica básica SONET/SDH consiste de cuatro diferentes elementos de red:

1. Multiplexor Adición/Sustracción (ADM)[8]
2. Multiplexor Terminal (TM)[9]
3. Cross-Conector Digital (DXC)[10]
4. Regenerador

Todos estos elementos son interconectados utilizando las platas de fibra óptica instalada de los proveedores de servicio típicamente redes SONET/SDH, como se muestra en la figura IV-1.

Los ADM son usados para los anillos de redes y los TMs son utilizados en topologías lineales y pueden ser interconectados directamente con fibra obscura. Si la distancia entre dos multiplexores excede de aproximadamente 40 km, un regenerador deberá ser colocado entre los multiplexores. El regenerador asegura la apropiada transmisión a través de la regeneración de la señal óptica, la cual se va degradando durante la transmisión óptica a través de la fibra.



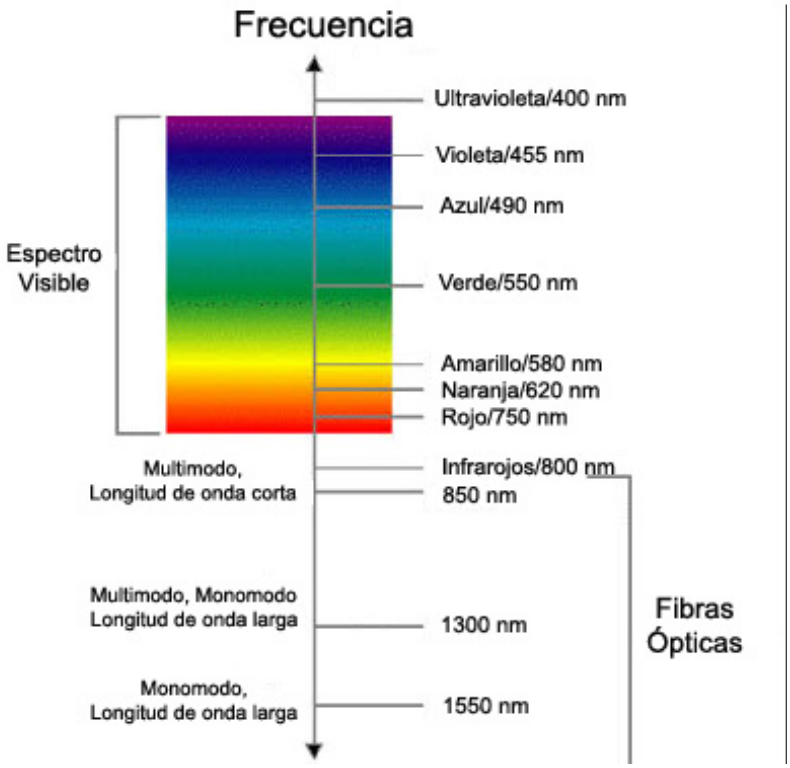
Red SONET/SDH típica

[8] ADM: Multiplexor Adición/Sustracción (*Add/Drop Multiplexer*)
[9] TM: Multiplexor Terminal (*Terminal Multiplexer*)
[10] DXC: Cross-Conector Digital (*Digital Cross-Connect*)

ÓPTICA GEOMÉTRICA

La propagación de la luz en una fibra óptica puede analizarse mediante el empleo de las leyes de la óptica geométrica. Esta primera aproximación permite definir simplemente una característica importante de la fibra óptica: su apertura numérica. La luz se compone de ondas electromagnéticas que se propagan en el vacío a una velocidad v del orden de 300,000 km/s. Estas ondas transportan energía y se caracterizan por sus frecuencias de oscilación f; asimismo, puede determinarse por medio de otro parámetro: la longitud de onda λ, que se define como la relación entre su velocidad de propagación y sus frecuencias, ambas se encuentran relacionadas por:

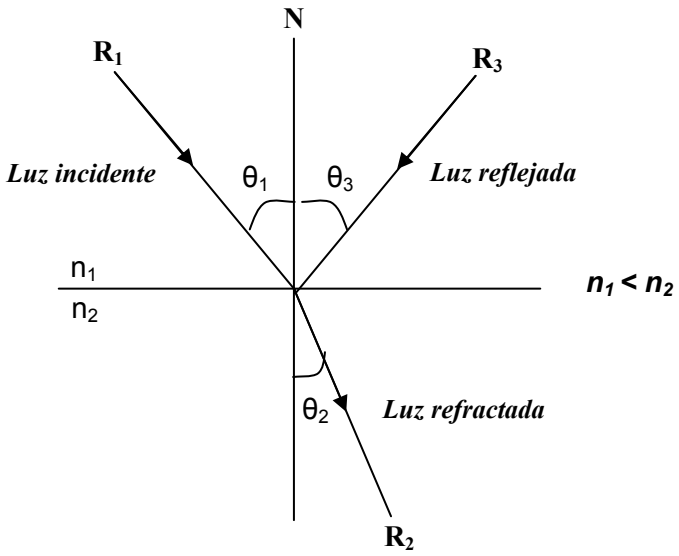
$$\lambda = \frac{v}{f} \ [m]$$



Espectro de Longitud de onda

La clave de cómo guiar la luz a través de la fibra óptica que puede ser de décenas de kilómetros de longitud, radica en la óptica geométrica.

La luz pueda transmitirse, reflejarse o refractarse en la superficie de separación existente entre dos medios diferentes (aire, vidrio, plástico, etc.), es decir, su dirección inicial sufre una desviación.



Representación de la reflexión y transmisión de un rayo al incidir en la frontera de dos medios

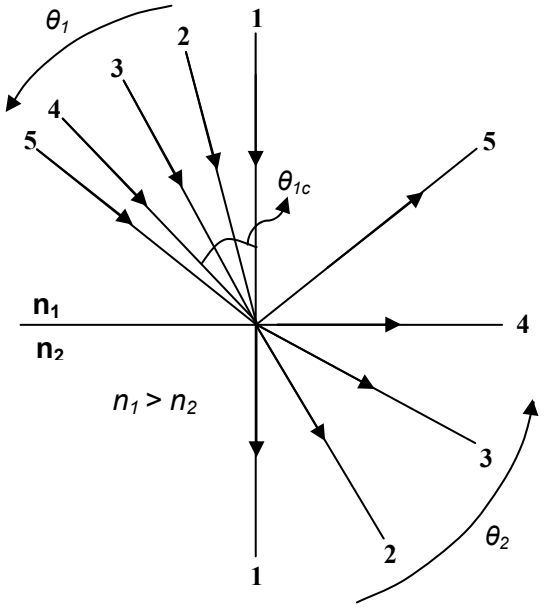
$$\theta_1(incidencia) = \theta_3(reflexión)$$

Si parte de la potencia del rayo incidente es transmitido al otro medio, la dirección del rayo transmitido está determinado por la *Ley de Snell*

Cuando se tiene $n_1 > n_2$. La luz pasa de un medio a otro que tiene un índice menor (por ejemplo del vidrio al aire).

$$sen\,\theta_2 = \frac{n_1}{n_2} sen\,\theta_1$$

Otro factor importante sucede si $\theta_1 > \theta_{1c}$, la luz ya no se refracta, por el contrario, se refleja totalmente en el medio original cuyo índice es n_1. θ_{1c} se conoce como *ángulo crítico o ángulo mínimo de reflexión total interna*. Será entonces una reflexión total interna, si la luz alcanza la interfaz ($n_1 > n_2$) con un ángulo superior al ángulo crítico.



Reflexión total interna ($n_1 > n_2$). Cuando θ_1 es mayor que θ_{1c} (rayo 5), la luz deja de ser refractada o que se refleja totalmente.

El concepto de apertura numérica es extrema importancia, ya que corresponden a la propiedad de la fibra para recolectar la luz y propagarla. La apertura numérica de una fibra depende de los índices de refracción del núcleo y de la cubierta, pero no de sus dimensiones. Las aperturas numéricas de las fibras comerciales varían entre 0.1 y 0.6. Cuanto mayor sea la diferencia entre el índice de refracción del núcleo fiel de la cubierta, mayor será la apertura numérica por lo que aumentará el número de ángulo de entrada que permiten la propagación de la luz.

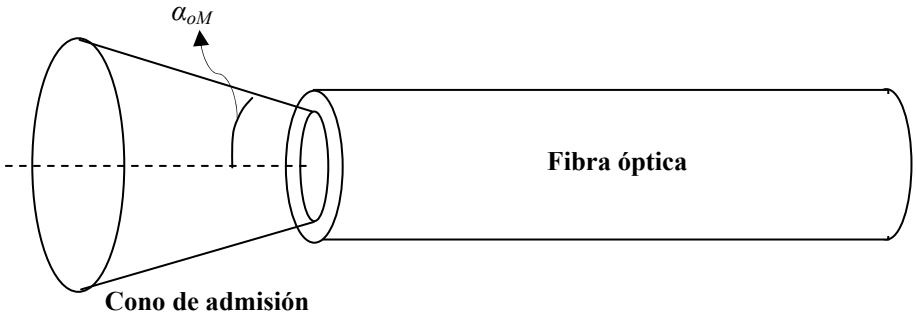


Figura II.31 *Cono de admisión de una fibra. Todo rayo de luz que entra con un ángulo α_o inferior a α_{oM} se propaga en la fibra.*

ELEMENTOS Y TIPOS DE CABLES ÓPTICOS

Las fibras ópticas son inherentemente frágiles y sin protección se vuelven aun más frágiles, debido a esto se han hecho dentro de cables que soportarán el manejo en la instalación y los frecuentes ambientes hostiles, en los cuales deben operar confiablemente. Trabajando en: ambientes que se encuentran en el rango de los casi constantes 2 a 4°C del fondo del mar (para cables submarinos intercontinentales), en los cambios bruscos de temperatura (desde los -55 a los 155°C) de algunas aplicaciones en aviación; desde presiones normales a los 70 MN/m^2; y líquidos corrosivos. El número de cables puede variar de uno, para cableado en racks, hasta varios miles, para distribución de cableado. El cable puede ser todo dieléctrico, conteniendo solo fibras, o pueden incorporarse varios conductores metálicos u otros elementos más complejos.

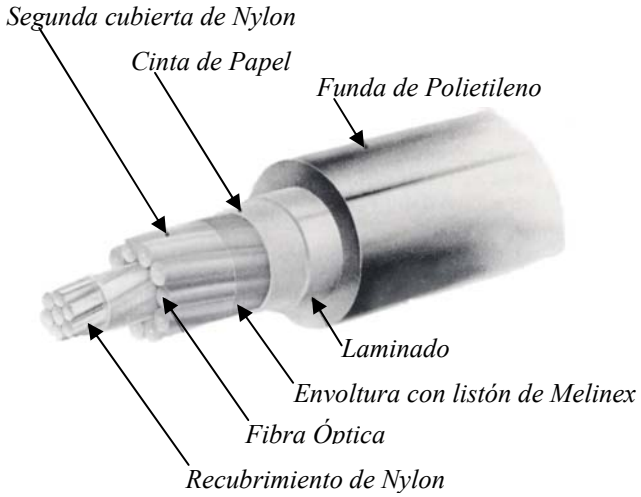
La gran variedad de diseños de cables se debe a la diversidad de aplicaciones que existen actualmente, la ingeniería de cableado tiene dos tareas principales, que son:

1. Minimizar el incremento de atenuación óptica, asociado con la manufactura y el uso de los cables.
2. Mantener la integridad física de la fibra durante el proceso de cableado, instalación y servicio.

CLASIFICACIÓN DE LOS CABLES ÓPTICOS

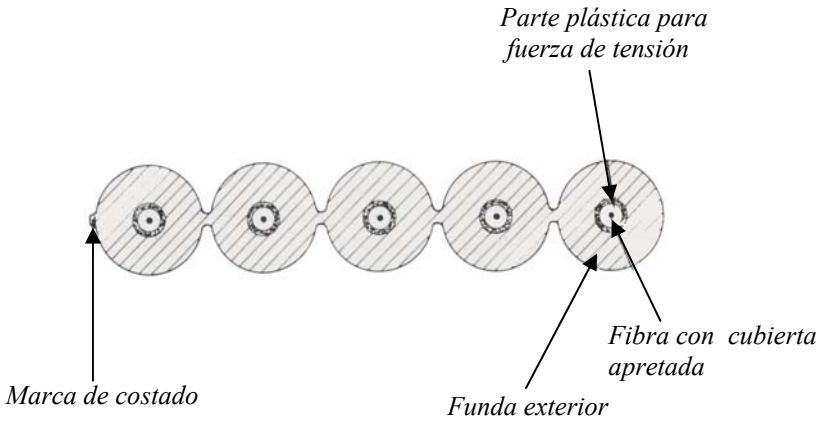
Se puede hacer una clasificación de los cables que existen dependiendo a la aplicación para la cual se vallan a emplear, a continuación se listan y se ilustranlas más usuales:

- ✓ ***Cable de Propósito General***



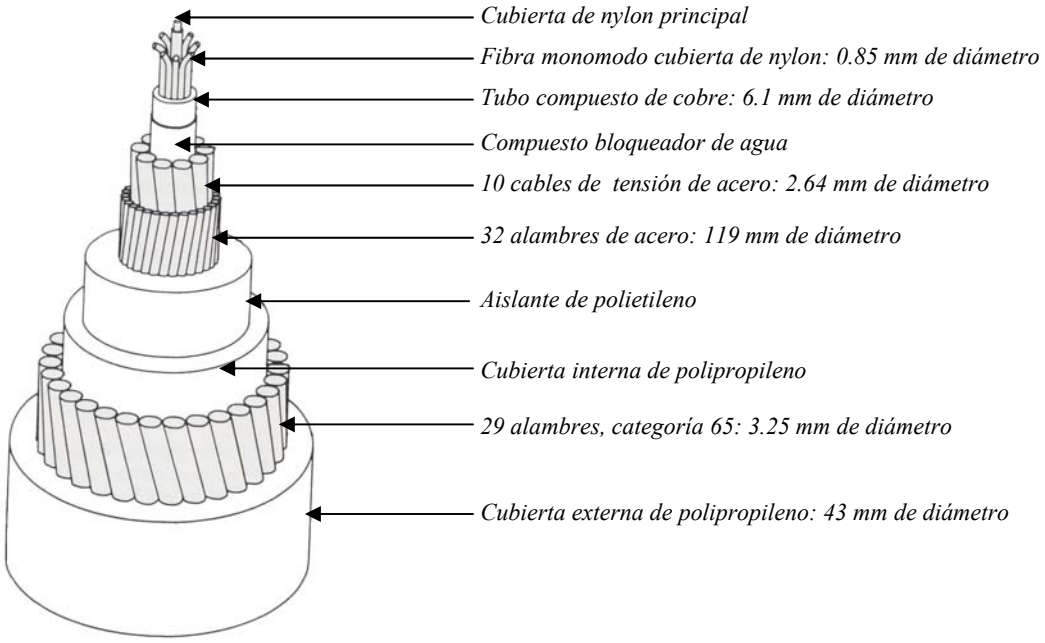
Cable de propósito general

✓ *Cable Industrial*



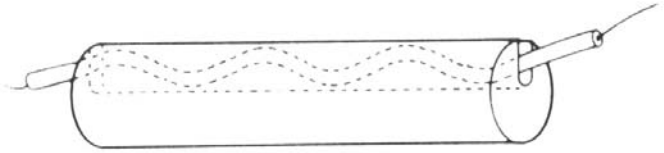
Cable Industrial

✓ *Cable Submarino*

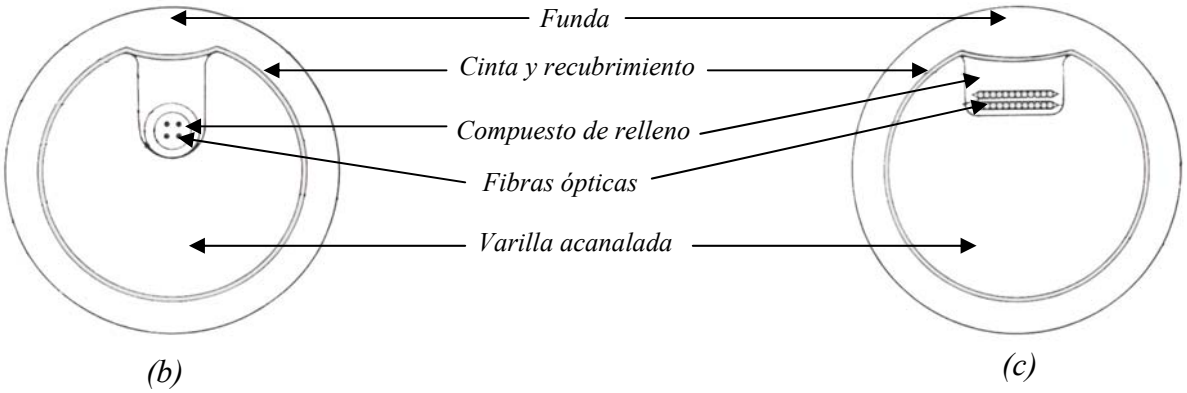


Cable submarino

✓ *Cable Aéreo*

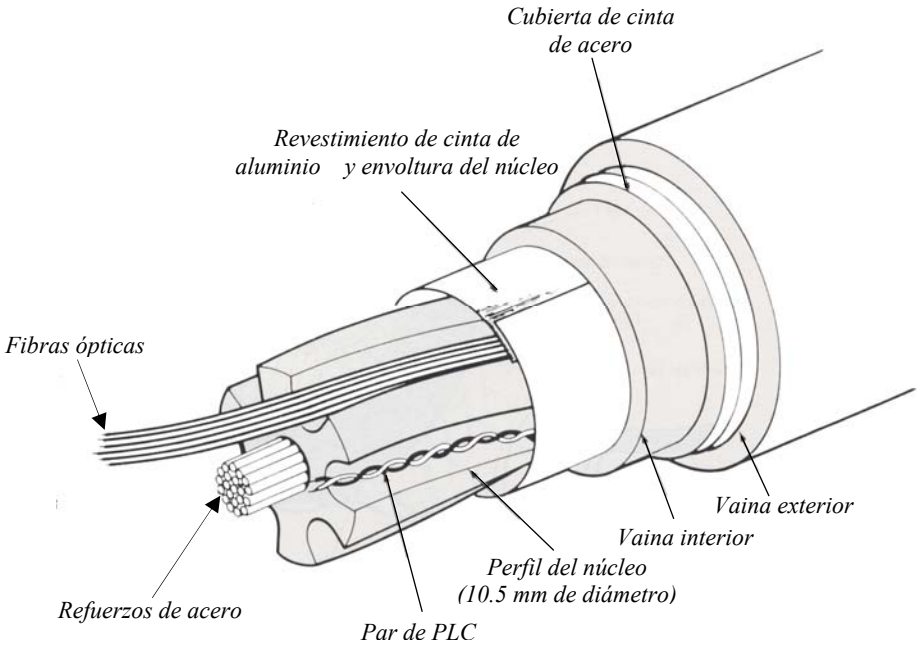


(a)



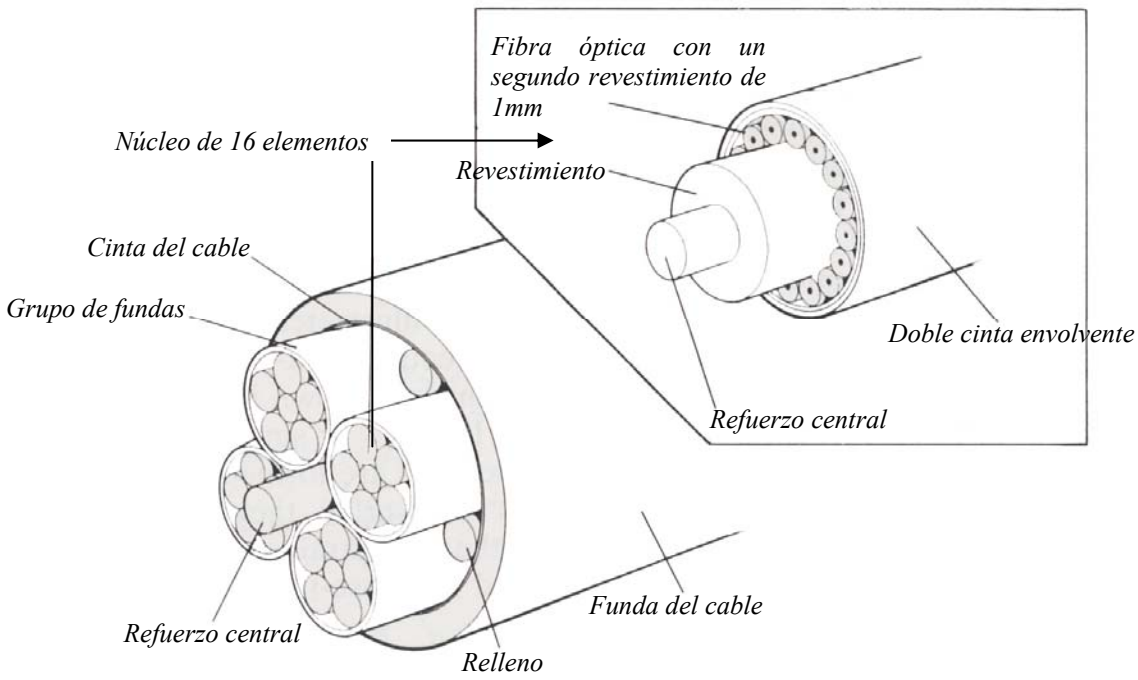
Ejemplo de un cable aéreo (a) Cable de fibra holgado, visto de costado, (b) Vista del extremo de un cable acanalado que contiene un conjunto de fibras, (c) Vista del extremo de un cable acanalado que contiene una cinta con fibras.

✓ *Cable Subterráneo*



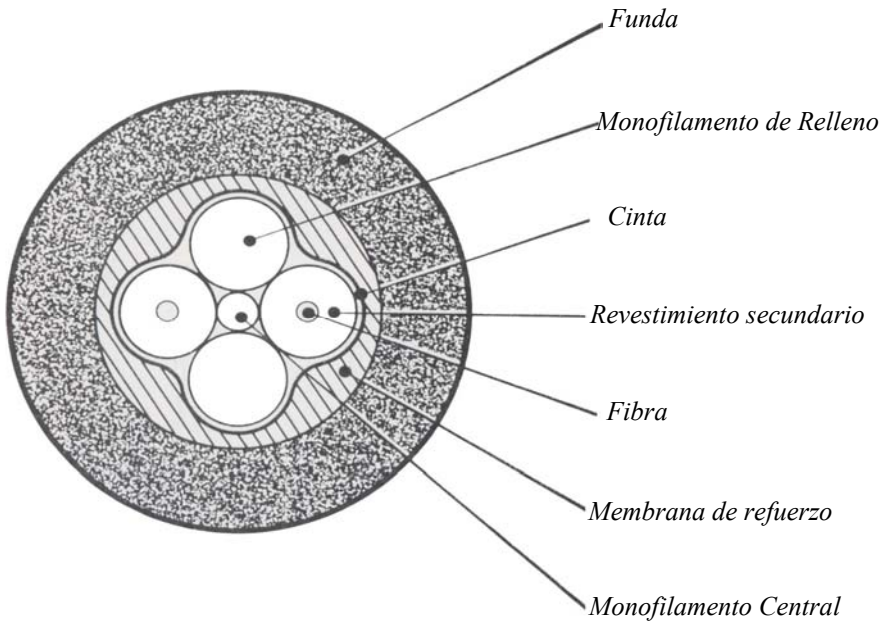
Cable subterraneo

✓ *Cable para Telecomunicaciones*



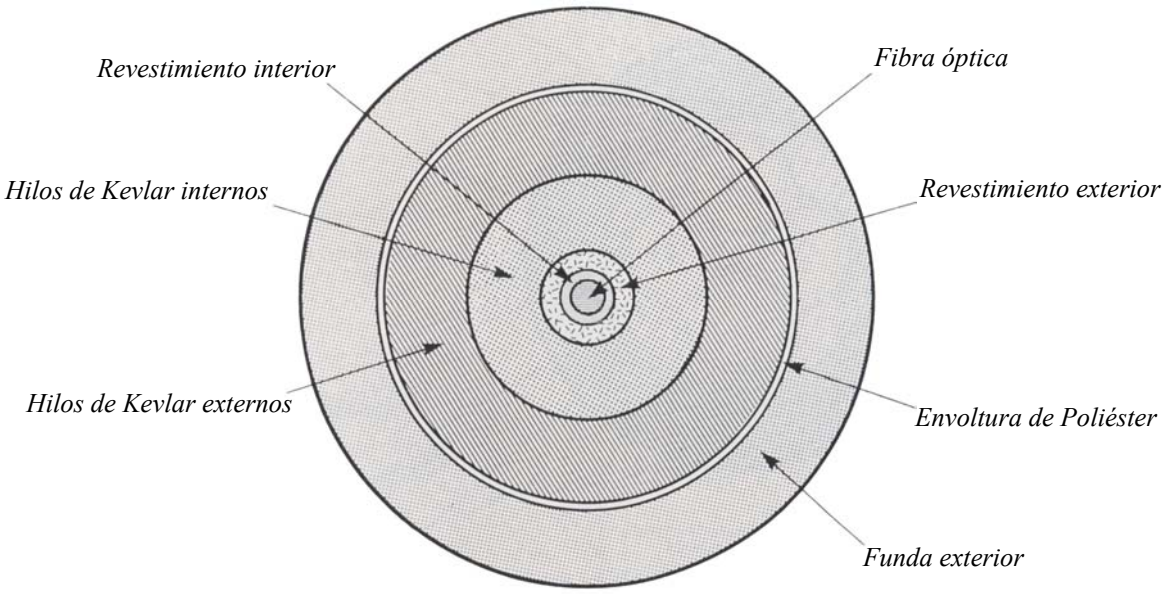
Cable para telecomunicaciones

✓ *Cable para Comunicaciones Militares*



Cable para comunicaciones militares

- ✓ ***Cables para Propósitos Especiales***



Cable par propósitos especiales

TIPOS DE CABLES

Como vimos anteriormente, los cables se pueden clasificar por aplicación, así mismo también se pueden clasificar por el tipo de cable, esto es dependiendo a la forma o tamaño del cable. A continuación se nombran los más comunes así como una breve descripción.

Cable Simplex: El tipo del cable es de construcción de buffer apretado *(tight buffer)*, disponible en dos versiones SMF y MMF, para aplicaciones de datos y dentro de edificios. Reforzado con Kevlar y un recubrimiento de PVC, lo que forma una estructura de cable de peso ligero y robusto. Recomendado para usarse en cables de interconexión (patch cords). Está clasificado en U.L. como OFNR[11]. (cable de fibra óptica no inflamable).

Cable Duplex: El cable duplex está disponible en diferentes tamaños de fibra óptica (núcleo y revestimiento), fabricación de tipo doble o redondo para aplicaciones de conectores FDDI, con características "Plenum o Riser". El cable de tipo doble es un cable formado por dos fibras revestidas individualmente y unidos sus recubrimientos en el proceso de fabricación, cada una de ellas dentro de un tubo

[11] OFNR:

de 900 μm reforzado con Kevlar y un recubrimiento de PVC de 2.92 mm. Existe también la posibilidad de solicitar el recubrimiento del cable con clasificación U.L. Riser (OFNR) ó Plenum (OFNP[12]).

Cable Micro: Este cable ofrece todas las características de un cable normal con la ventaja de estar empacado en un recubrimiento miniatura. Ideal para el empleo en condiciones de alta concentración de cables. Se suministra con SMF y MMF, con recubrimiento de 250 μm, refuerzo de Kevlar y cubierta exterior de Hytrel con un diámetro de 900 μm. El cable Micro es excepcionalmente competitivo en precio.

CONECTORES

Un conector para fibra óptica es un dispositivo de unión que asegura un acoplamiento eficiente entre dos extremos de fibra o bien entre fibras con dispositivos de telecomunicaciones, permitiendo un fácil manejo al conectar y desconectar, todas las veces que sea necesario.

Los empalmes permanentes son encontrados típicamente a lo largo de la línea de transmisión, mientras que los conectores desmontables son más localizados en los distribuidores de fibra y con los dispositivos transmisores y receptores. Estos permiten una fácil reconfiguración de los enlaces o para permitir un servicio fácil en los equipos terminales.

Los parámetros clave, definen la calidad de un conector de fibra para un sistema de transmisión dado, dichos parámetros incluyen:

- Pérdidas por inserción
- Facilidad de ensamble en campo
- Estabilidad ambiental
- Repetitividad de pérdidas
- Confiabilidad
- Perturbación del sistema (realimentación óptica, ruido modal)
- Costo.

Para lograr bajas perdidas por acoplamiento, los conectores deben alinearse con exactitud los núcleos de los extremos de las dos fibras. El grado de precisión mecánica que se requiere para mantener las pérdidas por debajo de un valor específico depende de las características de la fibra, ya que por ejemplo las SMF son más sensibles a errores de alineación que las MMF, por el pequeño tamaño de la longitud de onda comparado con el tamaño del núcleo.

[12] OFNP:

TIPOS DE CONECTORES

A continuación se muestra una lista de los conectores comerciales más usados:

- ✓ **El conector SC**, fabricado con una forma amoldada y con un sistema de cerrado "empuja-jala" *(push-pull)*. Es ideal para oficinas, CATV[13] y aplicaciones de telefonía. Se puede encontrar en versiones Simplex y Duplex.

Se pueden hallar con conectores con pulido APC, SPC y UPC, aunque los parámetros de estos cambian, como a continuaciones muestra:

Pérdida de Inserción	*Típica: ≤0.20dB Máxima:< 0.50dB*
Pérd. de Retorno APC	*Típica: ≥65dB Mínima:> 60dB*
Repetibilidad	*Pérdida de Inserción ± 0.1dB en 1000 conexiones*
Forma de Pulido	*Convexo-angular con ángulo de (8±0.2º)*
Vida Operativa	*Mínima: 1000 conexiones/desconexines*
Estabilidad Térmica*	*< 0.2dB en C.T. de -20 a 70º*
Estabilidad Calor Húmedo*	*< 0.2dB a +60º y 95% de H.R.*
Resistencia Mecánica	*Caída, Impacto y Vibración: ≤0.10 dB* *Tracción cable 1,6mm: ≤0.20dB para 40N mínima* *Tracción cable 2,0mm: ≤0.20dB para 80N mínima*
Normativa	*Son compatibles con conectores SC de pulido*
	APC de diseños NTT (CECC86000)

Tabla II.26 *Características genéricas con conectores SC con pulidos APC*

Aplicaciones usuales:

- ✓ Terminación componentes pasivos y activos específicos
- ✓ Redes de comunicación de datos y CATV
- ✓ Sensores e Instrumentación de laboratorio

[13] CATV: Televisión por Cable *(Cable TV)*.

Pérdida de Inserción	*Típica: ≤0.20dB Máxima:< 0.50dB*
Pérd. de Retorno SPC	*Típica: ≥45dB Mínima:> 40dB*
Pérd. de Retorno UPC	*Típica: ≥55dB Mínima:> 50dB*
Repetibilidad	*Pérdida de Inserción ± 0.1dB en 1000 conexiones*
Vida Operativa	*Mínima: 1000 conexiones/desconexiones*
Estabilidad Térmica*	*< 0.2dB en C.T. de -20º a 70º*
Estabilidad Calor Húmedo*	*< 0.2dB a +60º y 95% de H.R.*
Resistencia Mecánica	*Caída, Impacto y Vibración: ≤0.10 dB* *Tracción*: ≤0.20dB para 100N mínima*
Normativa	*SC: NTT-SC CECC 86260*

Características genéricas con conectores SC con pulidos SPC y UPC

Aplicaciones usuales:

- ✓ Terminación de componentes pasivos y activos
- ✓ Industriales, medicina, etc.
- ✓ Instrumentación de laboratorio
- ✓ Redes de área local y procesamiento de datos

(a) *(b)*

Conectores SC (a) Simplex y (b) Duplex.

- ✓ **El conector ST**, el cual usa un sistema de cerrado con bayoneta, la abrazadera de refuerzo en cerámica, asegura su alto desempeño, es el conector más común.

Se pueden hallar generalmente con conectores con pulido PC y SPC:

Pérdida de Inserción	*Típica: ≤0.30dB Máxima:< 0.70dB*
Pérd. de Retorno PC	*Típica: ≥40B Mínima:> 30*
Pérd. de Retorno SPC	*Típica: ≥45dB Mínima:> 40dB*
Repetibilidad	*Pérdida de Inserción ± 0.1dB en 1000 conexiones*
Vida Operativa	*Mínima: 1000 conexiones/desconexiones*
Estabilidad Térmica*	*< 0.2dB en C.T. de -20º a 70º*
Estabilidad Calor Húmedo*	*< 0.2dB a +60º y 95% de H.R.*
Resistencia Mecánica	*Caída, Impacto y Vibración: ≤ 0.20 dB Tracción*: ≤0.20dB para 100N mínima*
Normativa	*IEC 874-10 CECC BFOC/2.5*

Características genéricas con conectores ST con pulidos PC y SPC

Aplicaciones usuales:

- ✓ Terminación componentes pasivos y activos específicos
- ✓ Redes de comunicación de datos y CATV
- ✓ Sensores
- ✓ Instrumentación de laboratorio

Conectores ST en versión Simplex

- ✓ **El conector MT-RJ**, es un conector con una forma pequeña del estilo del conector RJ convencional, fabricado con una forma amoldada y utiliza una concha que se puede dividir y retirar.

Se pueden hallar generalmente con conectores con pulido SPC:

Pérdida de Inserción multimodo	*Típica: ≤0.30dB Máxima:< 0.40dB*
Pérdida de Inserción monomodo	*Típica: ≤0.40dB Máxima:< 0.50dB*
Pérd. de Retorno SPC monomodo	*Típica: ≥45dB Mínima:> 40dB*
Repetibilidad	*Pérdida de Inserción ± 0.1dB en 1000 conexiones*
Vida Operativa	*Mínima: 1000 conexiones/desconexiones*
Estabilidad Térmica*	*< 0.2dB en C.T. de -20º a 70º*
Estabilidad Calor Húmedo*	*< 0.2dB a +60º y 95% de H.R.*
Resistencia Mecánica	*Caída, Impacto y Vibración: ≤ 0.10 dB Tracción*: ≤0.20dB para 100N mínima*
Normativa	*TIA-568A IEC874*

Características genéricas con conectores MT-RJ con pulido SPC

Aplicaciones usuales:

- ✓ Terminación componentes pasivos y activos
- ✓ Redes de área local y procesamiento de datos
- ✓ Instrumentación de planta/laboratorio
- ✓ Industriales, medicina, etc.

Conector MT-RJ

- ✓ **El conector FDDI**, viene con una holgura flotante de 2.5 mm en la abrazadera y un recubrimiento fijo para minimizar las perdidas de luz. Este conector es utilizado generalmente con adaptadores para terminar en conectores del tipo SC o ST, así no se sacrifica la compatibilidad con este tipo de tecnología. Existen de 62.5/125 μm para aplicaciones multimodo.

Conector FDDI

- ✓ **El conector LC**, es un conector de forma pequeña, de alta densidad y de nueva generación, la abrazadera esta hecha de cerámica y se ve como un conector SC o ST en miniatura. Diseñado para reducir considerablemente el espacio de las conexiones en gabinetes de cableado. Diseñado para cable de 1.6mm Simplex y Duplex.

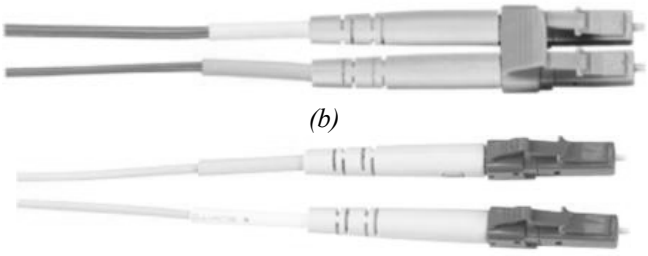
Se pueden hallar generalmente con conectores con pulido SPC y UPC:

Pérdida de Inserción	*Típica: ≤ 0.20dB Máxima:< 0.50dB*
Pérd. de Retorno SPC	*Típica: ≥ 45dB Mínima:> 40dB*
Pérd. de Retorno UPC	*Típica: ≥ 55dB Mínima:> 50dB*
Repetibilidad	*Pérdida de Inserción ± 0.1dB en 1000 conexiones*
Vida Operativa	*Mínima: 1000 conexiones/desconexiones*
Estabilidad Térmica*	*< 0.2dB en C.T. de -20º a 70º*
Estabilidad Calor Húmedo*	*< 0.2dB a +60º y 95% de H.R.*
Resistencia Mecánica	*Caída, Impacto y Vibración: ≤ 0.10 dB Tracción*: ≤ 0.20dB para 100N mínima*
Normativa	*GR326 IEC874*

Características genéricas con conectores LC con pulido SPC y UPC

Aplicaciones usuales:

- ✓ Terminación componentes pasivos y activos
- ✓ Redes de area local y procesamiento de datos
- ✓ Instrumentación de planta/laboratorio
- ✓ Industriales, medicina, etc.



(b)

(a)

Conectores LC Duplex, (a) para SMF, (b) para MMF.

- ✓ **El conector VF-45**, es otro conector de forma pequeña .El conector VF-45 brinda tecnología de fibra óptica aplicada a su escritorio. El cable VF-45 combina la simplicidad del conector RJ-45 con confiabilidad y seguridad de fibras ópticas, además de ser pequeño y económico. El cable VF-45 cumple con los estándares TIA, ISO, IEC y especificaciones 3M esta construido con fibra multimodo de en índice escalonado, con 100µm de diámetro de revestimiento y 125µm de diámetro de recubrimiento de polímero. Esta fibra es totalmente compatible con las fibras de vidrio estándar.

Pérdida de Inserción	*850nm media 0.28dB;* *1310 nm media 0.21dB*
Repetibilidad	*Pérdida de Inserción ± 0.1dB en 500 conexiones*
Vida Operativa	*Mínima: 510 conexiones/desconexiones*
Estabilidad Térmica*	*< 0.3dB en C.T. de -10º a 60º*
Estabilidad Calor Húmedo*	*< 0.3dB a +60º y 95% de H.R.*
Resistencia Mecánica	*Caída, Impacto y Vibración: ≤ 0.3 dB por eje* *Tracción*: ≤ 0.75dB para 66N*

Características genéricas con conectores VF-45.

Aplicaciones usuales:

- ✓ Redes de telecomunicaciones
- ✓ Redes de área local y procesamiento de datos
- ✓ Ideal para conexiones en gabinetes de cableado y escritorios

Conector VF-45 para MMF

- ✓ **El conector FC**, es un conector con cuerpo de rosca, este se asegura se empareje el cuerpo del conector con la fibra, enroscándose. Es utilizado en ambientes donde existe mucha vibración. Estos conectores es común hallarlos con terminación SC y se utilizan con SMF, en cables Simples y Duplex.

Se pueden hallar con conectores con pulido APC, SPC y UPC, aunque los parámetros de estos cambian, como a continuaciones muestra:

Pérdida de Inserción	*Típica: ≤ 0.20dB Máxima:< 0.50dB*
Pérd. de Retorno APC	*Típica: ≥ 65dB Mínima:> 60dB*
Repetibilidad	*Pérdida de Inserción ± 0.1dB en 1000 conexiones*
Forma de Pulido	*Convexo-angular con ángulo de (8±0.2º)*
Vida Operativa	*Mínima: 1000 conexiones/desconexines*
Estabilidad Térmica*	*< 0.2dB en C.T. de -20º#+70º*
Estabilidad Calor Húmedo*	*< 0.2dB a +60º y 95% de H.R.*
Resistencia Mecánica	*Caída, Impacto y Vibración: ≤ 0.10 dB* *Tracción*: ≤ 0.20dB para 100N mínima*
Normativa	*Son compatibles con conectores FC de pulido* APC de diseños NTT (CECC86000)

Características genéricas con conectores FC con pulido APC

Aplicaciones usuales:

- ✓ Terminación componentes pasivos y activos
- ✓ Redes de área local y procesamiento de datos
- ✓ Instrumentación de laboratorio
- ✓ Sensores

Pérdida de Inserción	*Típica: ≤ 0.20dB Máxima:< 0.50dB*
Pérd. de Retorno SPC	*Típica: ≥ 45dB Mínima:> 40dB*
Pérd. de Retorno UPC	*Típica: ≥ 55dB Mínima:> 50dB*
Repetibilidad	*Pérdida de Inserción ± 0.1dB en 1000 conexiones*
Vida Operativa	*Mínima: 1000 conexiones/desconexiones*
Estabilidad Térmica*	*< 0.2dB en C.T. de -20º#+70º*
Estabilidad Calor Húmedo*	*< 0.2dB a +60º y 95% de H.R.*
Resistencia Mecánica	*Caída, Impacto y Vibración: ≤ 0.10 dB* *Tracción*: ≤ 0.20dB para 100N mínima*
Normativa	*FC:IEC 874-7 CECC 86 115-801*

Características genéricas con conectores FC con pulido SPC y UPC

Aplicaciones usuales:

- ✓ Terminación componentes pasivos y activos
- ✓ Redes de área local y procesamiento de datos
- ✓ Instrumentación de planta/laboratorio
- ✓ Industriales, medicina, etc.

(a)

(b)

(c)

Conectores FC Duplex, (a) FC/UPC-FC/UPC , (b) FC/APC-FC/APC y (c) conectores FC/UPC - SC

- ✓ **El conector MU**, es un conector de alta densidad y de nueva generación, diseñado para reducir considerablemente el espacio de las conexiones en gabinetes de cableado, se encuentra para SMF y MMF.

Se pueden hallar con conectores con pulido SPC y UPC:

Pérdida de Inserción	*Típica: ≤ 0.10dB Máxima:< 0.50dB*
Pérd. de Retorno SPC	*Típica: ≥ 45dB Mínima:> 40dB*
Pérd. de Retorno UPC	*Típica: ≥ 55dB Mínima:> 50dB*
Repetibilidad	*Pérdida de Inserción ± 0.1dB en 1000 conexiones*
Vida Operativa	*Mínima: 1000 conexiones/desconexiones*
Estabilidad Térmica*	*< 0.2dB en C.T. de -20º#+70º*
Estabilidad Calor Húmedo*	*< 0.2dB a +60º y 95% de H.R.*
Resistencia Mecánica	*Caída, Impacto y Vibración: ≤ 0.10 dB* *Tracción*: ≤ 0.20dB para 100N mínima*
Normativa	*CECC 86 305 801 IEC60874-1*

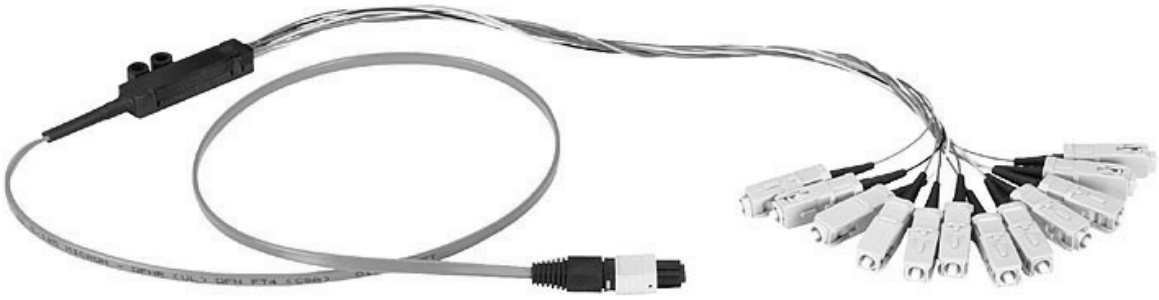
Características genéricas con conectores MU con pulido SPC y UPC

Conector MU para MMF

- ✓ **El conector MTP**, es un conector de fibra que utiliza 12 cables de fibra, es utilizado en conexiones de alta densidad para backbone[14] y zonas de cableado, el conector MTP es el conector más compacto de cable multi-hebras de fibra, generalmente se encuentra disponible para panel de

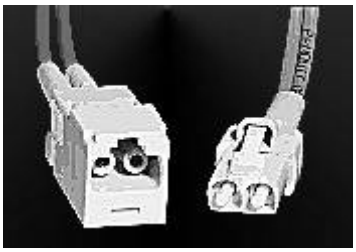
[14] Backbone: Parte de una red que actúa como una ruta primaria para el tráfico que con mayor frecuencia, proviene de, y se destina a otras redes.

parcheo o distribuidor de varios conectores disponibles en LC, SC, ST, FC, MU o MT-RJ.



Conector MTP con conectores SC

- ✓ **El conector OPTI-JACK,** es lo último en conectores de fibra óptica de escritorio. Su abrazadera de 2.5 mm le proporciona la robustez requerida. El diseño de la interfase de conexión macho/hembra FJ resulta familiar para el usuario final y está polarizada para prevenir el desacoplamiento de los cables. La modularidad con los conectores alámbricos permite una solución completa para las comunicaciones de datos en cada estación de trabajo en una sola toma.



Conector Opti-Jack.

ADAPTADORES Y ACOPLADORES

Los adaptadores para fibra, son utilizados para acoplar cables de fibra óptica, ya sea con otros cables o con un panel de montaje.

A continuación se muestran los más comerciales:

Acoplador MT-RJ–MT-RJ Multimodo (A)

- ✓ Utilizado en aplicaciones de alta densidad multimodo
- ✓ Creado para panel de montaje rectangular.

Acoplador LC–LC Multimodo/Monomodo (B)
- ✓ Adecuado para aplicaciones multimodo o monomodo
- ✓ Creado para panel de montaje.

Adaptador ST–ST Multimodo (C)
- ✓ Utilizado en aplicaciones multimodo para acoplar los bujes de la fibra.

Adaptadores ST–SC (D)
- ✓ Convertidor de conector de SC a ST
- ✓ Utilizado en aplicaciones monomodo y multimodo
- ✓ Adaptadores duplex admiten dos conectores simplex o duplex

Acopladores receptores SC–SC (F)
- ✓ Viene con alineadores cerámicos
- ✓ Puede ser utilizado con todos los tipos de conectores SC
- ✓ Utilizado en aplicaciones monomodo y multimodo
- ✓ El modelo duplex admite dos conectores simplex o un conector duplex

Particionador FDDI–ST (G)
- ✓ Conecta un conector FSD a dos conectores tipo ST
- ✓ Un alineador propio, con interfaz de libre flotación, provee baja perdida por acoplamiento
- ✓ Utilizada en modo duplex
- ✓ Cumple con la rigurosa especificación ANSI X3T9.

Particionador MTP–MTP (H)
- ✓ Utilizado para aplicaciones de alta densidad multimodo y monomodo
- ✓ Diseñado en una sola pieza, para proveer una optima durabilidad para una exacta alineación núcleo a núcleo en cada interconexión
- ✓ Polarizado para asegurar una correcta inserción.

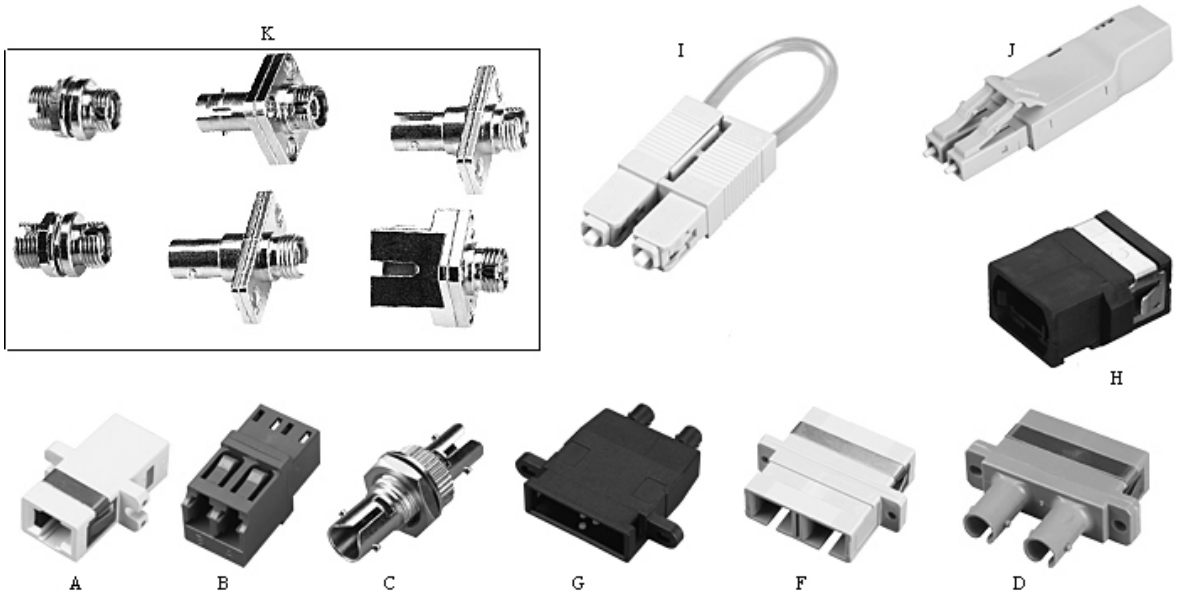
Conector Loopback[15] SC Multimodo (I)
- ✓ Utilizado para aplicaciones de redes de fibra óptica multimodo y equipos de prueba
- ✓ Caracterizado con una perdida de inserción de 0.5dB y 0.5“de armazón con linea de centrado.

Adaptador Loopback LC (J)
- ✓ A elegir en monomodo o multimodo
- ✓ Caracterizado con un conector LC a prueba de jalones.

[15] Loopback: *Retorno de bucle*, utilizado para realizar pruebas de señal, ya que lo mismo que se transmite debe ser lo mismo que regresa.

Adaptadores FC-FC, ST-FC, SC-FC (K)

- ✓ Diseñado para montaje en panel
- ✓ Creados en bronce para mayor durabilidad, comparado con los fabricados en bronce. Estos son mejores para aplicaciones MMF donde la alineación no es crítica.
- ✓ Los adaptadores cerámicos ofrecen alineación más precisa, pero son menos durables que los fabricados en bronce.



Adaptadores y Acopladores.

ATENUADORES

Cuando un dispositivo de fibra esta muy cercano a otro, por ejemplo a 10m, la señal es extremadamente fuerte. La luz de la señal no tiene tiempo para atenuarse o perder fuerza en el trayecto de la fibra. Esto es conocido como *saturación del receptor*. El nivel de energía de la señal de la fibra óptica es muy alto y excede el rango de operación del equipo receptor. Y cuando la luz alcanza el final, esta se refleja de regreso a lo largo del cable. Esta reflexión distorsiona la señal y perturba los datos.

Para resolver el problema se utilizan los atenuadores. Estos tienen como característica garantizar perdidas por retorno, controladas para atenuar la señal. Para lograr evitar las perdidas por retorno, los atenuadores utilizan SMF dopada, con una longitud de onda de 1310 a 1550 nm.

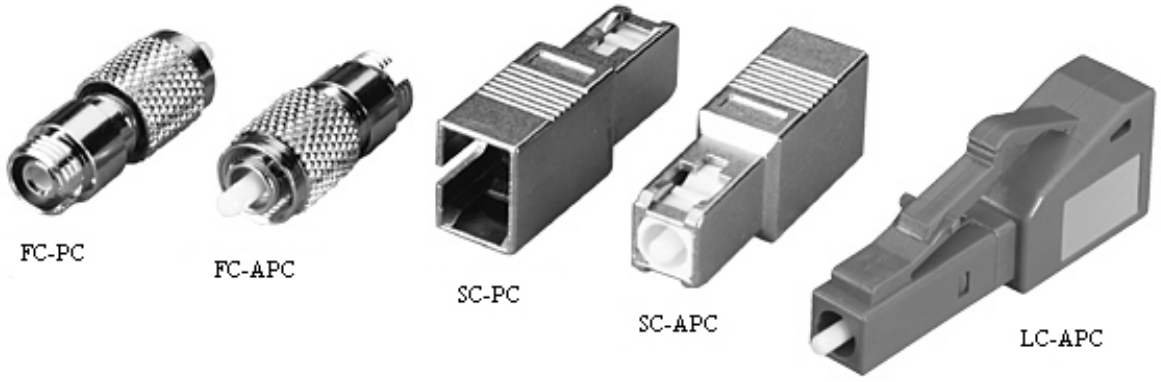
Los atenuadores son utilizados frecuentemente en aplicaciones, tales como CATV, LAN, WAN y algunas otras aplicaciones para telecomunicaciones. Como conclusión se puede decir entonces, que los atenuadores son utilizados en sistemas donde se requiere que la señal opere con los mismos niveles ópticos en todos los equipos, también se pueden utilizar como parte de equipos de pruebas, para verificar los niveles ópticos.

En la figura, se muestran los modelos más comerciales utilizados, los cuales se tienen con conectores del tipo FC, SC o LC con pulido PC o APC, y sus especificaciones.

Especificaciones:

Atenuación	*2, 5, 10, 15, o 20 dB*
Tolerancia de atenuación	*Modelos FC y SC: 2 o 5 dB: ± 1.0 dB; 10 dB: ± 1.5 dB; Modelos LC: 5 dB: ± 0.5 dB; 10, 15, or 20 dB: ± 1.0 dB*
Tipo de Cable	*SMF*
Perdidas por retorno	*Contactos PC: Todos los modelos: -55 dB típica; Contactos APC: Modelos FC, SC y LC: -60 dB típica*
Longitud de onda	*1310/1550 nm*
Conectores	*FC, SC o LC con contacto de pulido PC o APC.*

Características genéricas de los atenuadores.



Atenuadores.

MODELO DE PROPAGACIÓN EN EL ESPACIO LIBRE

Todo modelo de propagación se basa en el modelo de espacio libre, ya que este es nuestra referencia de la potencia máxima que tendríamos en el receptor. El modelo de espacio libre es usado para predecir la potencia de señal recibida cuando el transmisor y el receptor tienen una línea de vista sin obstrucciones entre ellos. En

las comunicaciones satelitales y enlaces de microondas tienen enlaces en los cuales la antena transmisora y la antena receptora tienen línea de vista entre ellas, y en estos enlaces las ondas electromagnéticas típicamente experimentan una propagación en el espacio libre. Como con la mayoría de los modelos de amplia-escala, el modelo de espacio libre predice que la potencia recibida decae en función de la distancia entre transmisor y receptor. La potencia recibida por una antena que esta separada por una distancia *d* de la antena transmisora esta dada por la ecuación:

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L}$$

Donde P_t es la potencia transmitida, $P_r(d)$ es la potencia recibida en función de la distancia entre el receptor y el transmisor, G_t es la ganancia de la antena transmisora, G_r es la ganancia de la antena receptora, *d* es la distancia de separación de las antenas. Y L son las perdidas en el sistema no relacionadas con la perdidas de propagación, como perdidas en los filtros y perdidas en la antena y generalmente es mayor a 1, y λ es la longitud de onda en la que se esta operando.

P_t es la potencia transmitida en miliwatts. El producto de $P_t G_t$ es referido al EIRP (*effective isotropic radiated power)* y representa la máxima potencia radiada por un transmisor en dirección de la ganancia máxima, comparada con una radiación isotropica.

Otro parámetro interesante es la pérdida en el espacio libre en la cual se considera que la ganancia de las antenas es unitaria y esta dada por:

$$L_{free} = -20\log_{10}\left(\frac{\lambda}{4\pi d}\right) dB$$

La ecuación del EIRP puede ser usada para estimar la potencia recibida a cualquier distancia del transmisor usando la ecuación

$$P_r(d) = P_r(d_{ref})\left(\frac{d_{ref}}{d}\right)^2$$

donde d_{ref} es una distancia de referencia. La distancia de referencia puede ser más pequeña que las distancias típicas encontradas en los sistemas de comunicaciones inalámbricos y puede llegar a la región de campo lejano de la antena, por lo tanto las pérdidas mas alejadas a un punto son puramente efectos dependientes de la distancia. Este valor suele estar en el rango de 100 a 1000 metros. Con esto podemos escribir la ecuación como

$$p_r(d)dBm = 10\log_{10}\left[P_r\left(d_{ref}\right)\right] + 20\log_{10}\left[\frac{d_{ref}}{d}\right]$$

Las perdidas actuales sufridas por una señal a una frecuencia de f_0 (MHz) a una distancia *d*(Km) bajo las condiciones donde tenemos línea de vista sin obstrucciones, L_{free}, puede ser rescrita en la siguiente ecuación:

$$L_{free} = -20\log_{10}\left(\frac{c/f}{4\pi d}\right)dB$$

donde c es la velocidad de la luz en el espacio libre y *f* es la frecuencia de donde nuevamente tenemos que:

$$L_{free} = 32.44 + 20\log_{10}(f) + 20\log_{10}(d)$$

donde *d* puede ser tan grande como 1 Km, *f* esta en megahertz, y *d* esta en kilómetros.

MODELOS DE AMPLIA ESCALA

La potencia recibida es generalmente el parámetro más importante a predecir para los modelos de amplia-escala, y los cuales se basan principalmente en describir la física de la Reflexión, Difracción, Difracción y la Refracción.

MODELOS DE PROPAGACIÓN EN EXTERIORES

Las radio transmisiones en sistemas de comunicaciones móviles a menudo se dan sobre superficies irregulares. Esto tipo de superficies deben de ser consideradas para estimar las perdidas en la trayectoria. La curvatura de la tierra, montañas, árboles, construcciones y otros obstáculos, son solo algunos de los factores que deben ser tomados en cuenta, y hay un gran número de modelos que predicen todos estos tipos de pérdidas sobre superficies irregulares. Todos estos modelos están enfocados en predecir la potencia de la señal recibida en un punto ó área específica, pero estos métodos varían ampliamente en su aproximación, complejidad y sobre

todo en su precisión. La mayoría de estos modelos están basados están basados en una interpretación sistemática de mediciones de datos obtenidos en la practica. Algunos ejemplos de estos modelos son:

Outdoor Models

- Longley-Rice Model
- Durkin´s Model
- Okumura Model
- Hata Model
- Lee´s Model
- PCS Extensión to Hata Model
- Wideband PCS Microcell Model

MODELOS DE PROPAGACIÓN EN INTERIORES

Los modelos de propagación en Interiores están enfocados en los mismos fenómenos que los modelos de propagación en exteriores: reflexión, refracción, difracción y dispersión, pero con la diferencia de que ahora las condiciones son mucho más variables. Ahora los niveles de la señal dependen en gran medida de los diferentes muebles y obstáculos que se encuentren dentro del lugar. Un modelo que pueda predecir la perdida de la señal dentro una habitación debe de tomar en cuenta diferentes aspectos.

Una construcción puede tener una gran cuarto sin divisiones y pocos obstáculos o bien un cuarto largo pero con bastantes obstáculos y seria la misma situación en cuartos más pequeños. Ahora bien, no solo el número de obstáculos que debe atravesar la señal son el factor principal en la determinación de la perdida de la señal, sino que también hay que tomar en cuenta el material de que están hechos estos, así como del material de que esta hecha la construcción. Todos estos elementos que hay que tomar en cuenta hacen difícil la elaboración de un modelo general que pueda predecir las pérdidas de la señal en Interiores. La mejor aproximación para modelar loa propagación en Interiores se clasifica dependiendo de la configuración de la zona, esta configuración depende donde este localizada la antena transmisora (estación base) y si esta dentro o fuera de la construcción o edificio. Dentro de esta clasificación tenemos:

- Zona Extra Grande. En una zona extra larga hay una sola estación base fuera del edificio, situación ideal para una región que tiene un número pequeño de oficinas o tiendas juntas.

- Zona Grande En una larga zona, los edificios o construcciones son muy grandes pero la densidad de población es pequeña, y en esta clasificación, una simple estación base esta alojada dentro del edificio.

- Zona Media En una zona media, el edificio o construcción solo es grande pero tiene una gran población, una situación común en tiendas departamentales u oficinas grandes. En esta clasificación, hay un número de estaciones base localizadas dentro del edificio para servir a varios usuarios.

- Zona Pequeña En esta zona el edificio o construcción puede tener varias divisiones, en las cuales la pérdida por penetración de la señal depende del material de que estén hechas estas, y por lo general requiere de poner una estación base en cada cuarto del edificio.

MODELOS DE PEQUEÑA-ESCALA

Como se menciono párrafos anteriores los modelos de Pequeña-Escala se encargan de observar las pérdidas de la transmisión que fluctúan alrededor de un valor medio de la señal. El desvanecimiento ó mejor conocido como *fading*, es usado para describir estas fluctuaciones rápidas de la amplitud de una señal de radio en un corto periodo de tiempo o pequeña distancia. El desvanecimiento es causado por la interferencia entre 2 ó mas versiones de la señal transmitida, las cuales llegan con una diferencia de tiempo al receptor. A este efecto donde las señales llegan con una diferencia en amplitud y fase se les conoce como desvanecimiento por multitrayectorias, y depende de la relativa propagación de las ondas y del ancho de banda de las señales transmitidas.

El desvanecimiento puede ser descrito en cualquiera de los siguiente términos: Multitrayectorias o efecto Doppler, por su distribución estadística de la envolvente recibida (*Rayleigh, Rician, o lognormal*), por la duración del desvanecimiento (*long-term ó short-term*) ó por el rápido vs lento desvanecimiento.

Debido a la complejidad que sobrelleva el estudio de todos estos términos solo describiremos los principales factores que influyen en el desvanecimiento (*fading*), y a la vez solo mencionaremos solo algunos de los modelos ya hechos que toman en cuenta estos diferentes aspectos.

FACTORES DE INFLUENCIA EN EL DESVANECIMIENTO

Varios factores físicos en la propagación de canal de radio influyen en el desvanecimiento de Pequeña-Escale. Estos son:

Propagación por Multitrayectorias. La presencia de objetos reflejantes y dispersantes en el canal contribuyen al constante cambio de las condiciones que alteran a la señal en amplitud, fase y tiempo. Estos efectos resultan en múltiples versiones de la señal transmitida que llegan a la antena receptora, las cuales están desplazadas unas de las otras en tiempo y orientación espacial.

Desplazamiento del receptor. El relativo movimiento entre la estación base y el receptor resulta en una modulación aleatoria debido al efecto Doppler (diferentes corrimientos) en cada una de las componentes de las multitrayectorias.

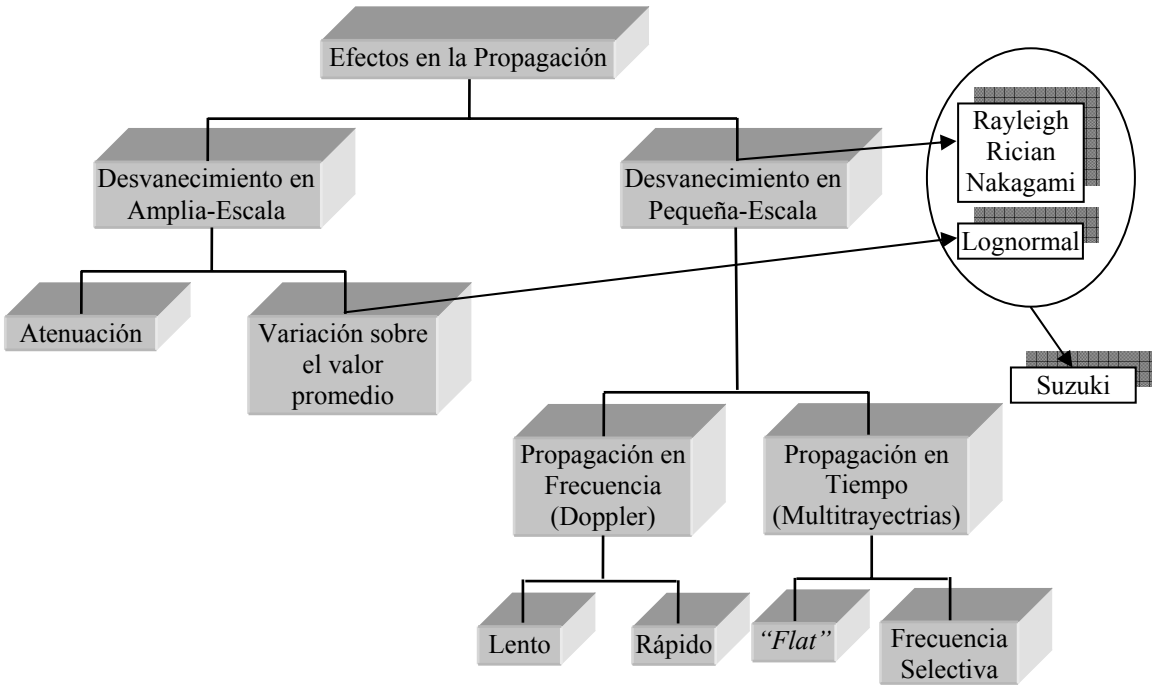
- **Velocidad de objetos cercanos.** Si los objetos que se encuentran dentro del canal de radio están en movimiento, estos también introducen variaciones en el corrimiento de Doppler en las componentes de las multitrayectorias. Si los objetos cercanos se mueven a una velocidad mayor que el receptor, entonces este efecto domina el desvanecimiento.

- **El Ancho de banda en la transmisión de la señal.** Si el ancho de banda de la señal de radio transmitida es mayor que el ancho de banda del canal de las multitrayectorias, la se señal recibida será distorsionada, pero el nivel de potencia de la señal recibida no se desvanecerá mucho sobre una área local.

Estos Factores son descritos por diferentes métodos y modelos que generalmente están basados en técnicas de sondeo del canal, las cuales muestran la respuesta al impulso del canal. En estos métodos se caracterizan las multitrayectorias, el efecto Doppler y la coherencia del ancho de banda que generalmente son los fenómenos más importantes para la caracterización del canal. Ejemplos de estos modelos tenemos:

- Impulse Response Model of a Multipath Channel
- Rayleigh Fading Distribution
- Ricean Fading Distribution
- Lognormal Fading Distribution
- Nakagami Distribution
- Suzuki Distribution
- Clarke's Model for Flat Fading

Finalmente todos los modelos ya sean de Amplia-Escala ó Pequeña-Escala son afectados de alguna manera por cualquiera de los siguientes aspectos que se muestran en los recuadros de la siguiente figura:



Factores de Atenuación y Desvanecimiento

ANTENAS

Las antenas son otro elemento a considerar en los sistemas de los sistemas de comunicaciones inalámbricos, la configuración y diseño de estas afectan en la caracterización del canal de radio como se vio anteriormente.

Haciendo una analogía con los sistemas alambritos, las antenas tomarían el lugar de los conectores, los cuales conectan al sistema transmisor con el medio por el cual se van a propagar las señales, en este caso el medio ambiente.

El IEEE define una antena como aquella parte de un sistema trasmisor o receptor diseñada específicamente para radiar o recibir ondas electromagnéticas. Si bien sus formas son muy variadas, todas las antenas tienen en común el ser una región de transición entre una zona donde existe una onda electromagnética guiada y una onda en el espacio libre, a la que puede además asignar un carácter direccional. La representación de la onda llegan se realiza consultas corrientes (hilos conductores y líneas de transmisión) o por campos (guías de ondas); en el espacio libre, mediante campos.

La visión del antenas el gobierno potencia que se le suministra con las características de direccionalidad adecuadas a la aplicación. Por ejemplo, radiodifusión o comunicaciones móviles se quedará rabia sobre la zona de

coberturas de forma omnidireccional, mientras que radiocomunicaciones fijas interesará que las antenas sean direccionales. En general cada aplicación impondrá unos requisitos sobre la zona del espacio en la que se desee concentrar la energía. Asimismo, para poder extraer información se ha de ser capaz de captar en algún punto del espacio la onda radial, absorberá energía de esa onda y entregarla al receptor. Existen, pues, dos misiones básicas de una antena: trasmitir y recibir, imponiendo cada aplicación condiciones particulares sobre la direccionalidad de la antena, niveles de potencia que debe soportar, frecuencia de trabajo y otros parámetros que son de gran importancia. Esta diversidad de situaciones da origen a un gran número de tipos de antenas.

Toda onda se caracterizan por su frecuencia (f) y su longitud de onda (λ), ambas relacionadas por la velocidad de propagación en el medio, que habitualmente en antenas tiene las propiedades del vacío.

En una forma amplia indicativa, los tipos más comunes de antenas se pueden agrupar los grandes bloques siguientes:

Antenas alámbricas: se distinguen por estar construidas con hilos conductores que soportan las corrientes que dan origen a los campos radiados. Pueden estar formadas por hilos rectos (dipolo, V, rómbica), espiras (circular, cuadrada o de cualquier forma arbitraria) y hélicas.

Antenas de apertura y reflectores. En ellas la generación de la onda radiada se consigue a partir de una distribución de campos soportaba por la antena y suelen excitar con guías de ondas. Son antenas de apertura las bocinas (pirámidas y cónicas), las aperturas y las ranuras sobre planos conductores, y las bocas de guía.

El empleo de reflectores, asociados a un alimentador primario, permite disponer de antenas con las prestaciones necesarias para servicios de comunicaciones a grandes distancias, tanto terrestres como espaciales. El receptor más común es el patagónico.

Agrupaciones de antenas. En ciertas aplicaciones se requieren características de radiación que no puede lograrse con un sólo elemento; sin embargo, con la combinación de varios de ellos se consigue una gran flexibilidad que permite obtenerlas. Estas agrupaciones pueden realizarse combinando, en principio, cualquier tipo de antena.

PARÁMETROS DE ANTENAS.

Una antena formará parte sin sistema más amplio, de radiocomunicaciones. Interesará, por lo tanto, caracterizarla con una serie de parámetros que la descrian y

permitan evaluar el efecto sobre el sistema de una determinada antena, o bien especificar el comportamiento deseado de una antena para incluirla en ese sistema.

Los parámetros conviene diferenciarlos inicialmente según se relacionen con transmisión o recepción, los parámetros principales a tomar en cuenta son:

- Impedancia
- intensidad de radiación
- patrón de radiación
- directividad
- polarización
- ancho de banda

En nuestro estudio todos los parámetros de una antena estarán abordados dentro del estudio de la antena o arreglo de antenas que se vaya a utilizar en la solución propuesta para el diseño de la red.

INDEX

FIGURAS

	PAG.
I.1 RED Y EQUIPO	5
I.2 TIPOS DE CABLES	7
I.3 FORMATO TÍPICO DE UN PAQUETE	11
I.4 RED CONMUTADA	13
I.5 CONMUTACIÓN DE CIRCUITOS	14
I.6 MENSAJE CON INFORMACIÓN DE ENCABEZADO	15
I.7 CONMUTACIÓN DE PAQUETES	16
I.8 COMPARACIÓN ENTRE LOS TIPOS DE CONMUTACIÓN	17
I.9 ANILLO, BUS, RED CON RADIO	18
I.10 OPERACIÓN DE UNA RED	19
I.11 TOPOLOGÍA JERÁRQUICA	21

I.12 Topología Bus 22
I.13 Topología Anillo 24
I.14 Topología Estrella 25
I.15 Topología Anillo-Estrella 27
I.16 Topología Bus-Estrella 27
I.17 Red de Área Local (LAN) 32
I.18 Red de Área Metropolitana (MAN) 33
I.19 Red de Área Amplia (WAN) 37
I.20 Internet 38
I.21 El Modelo OSI 39
I.22 Dos juegos entrelazados de capas superiores de modelo OSI 40
I.23 Capas del modelo OSI comunicándose con otras capas 42
I.24 Usuarios de Servicio, proveedores, interacción con la red y enlace de capas 43
I.25 Proceso de Encapsulamiento de Información 44
I.26 Las aplicaciones de la Capa Física pueden tener especificaciones LAN o WAN 46
I.27 La Capa de Enlace contiene dos subcapas 47
I.28 Componentes básicos de una Capa de Enlace de Datos 51
I.29 Componentes básicos de un Paquete de una Capa de Red 52
I.30 Componentes que constituyen una Celda Típica 52
II.1 Transmisión de una señal 57
II.2 Cable UTP cuatro pares 63
II.3 Cable STP cuatro pares 64
II.4 Función pines/colores normalizados 65
II.5 Conexión de un cable cross-over 65
II.6 Cable coaxial 66
II.7 Codificación Manchester y Manchester Diferencial 68
II.8 Codificación AMI 69
II.9 Codificación HDB3 69
II.10 Evolución de DSL 70
II.11 Sistema básico de xDSL 71
II.12 HDSL 73
II.13 ADSL 75
II.14 CDSL 76
II.15 VDSL 78
II.16 Adaptador portuario de HSSI 79
II.17 Conectores Rs-232 82
II.18 Sistema de comunicación par fibra Óptica 90
II.19 Repetidor óptico 90
II.20 Sistema general de comunicación por fibra óptica con conectores 91
II.21 Fibra óptica 92
II.22 Tipos de fibra óptica 93

II.23 Fibra de índice escalonado sin cubierta 94
II.24 Fibra de índice escalonado con cubierta 94
II.25 Fibra de índice gradual 94
II.26 Fibra monomodo 95
II.27 Pérdidas en una fibra 97
II.28 Multicanalización por división de tiempo (TDM) 103
II.29 Sistema de transmisión haciendo uso de multiplexación por división de longitud de onda 105
II.30 Pérdida de la potencia (atenuación) 107
II.31 Pérdidas en amplia-escala 108
II.32 Pérdidas en pequeña-escala 108
II.33 Señales pasabanda moduladas digitalmente 110
II.34 Constelaciones de señales QPSK 111
II.35 Constelación QUAM de 16 bits 112
II.36 Constelación DQPSK para unos datos posibles 114
II.37 Espectro de banda esparcida 119
II.38 Secuencia binaria pseudoaleatoria 120
II.39 Banda esparcida por saltos de frecuenca 121
II.40 Efecto de las multitrayectorias en el fotodetector de un sistema infrarrojo difuso 123
II.41 Enlace infrarrojo punto a punto 124
II.42 Enlace infrarrojo difuso 125
II.43 Modelo OSI para WLANs 126
II.44 Transmisor y Recptor para DSSS 126
II.45 Preámbulo encabezado para DSSS 127
II.46 Elementos básicos de u Transmisor y Receptor para FHSS 129
II.47 Preámbulo y Encabezado para FHSS 130
II.48 Funcionamiento de Acceso al Medio CSMA/CA 133
II.49 Solución MACA 134
II.50 Envío de RTS y CTS para solucionar el problema del nodo oculto 134
II.51 Subcapa MAC y estandar IEEE 802.3 143
II.52 Formato de una trama MAC 144
II.53 Campo de Control de la trama MAC 145
II.54 Trama HDLC 149
II.55 Trama PPP 151
II.56 Estructura de Datagrama IP 157
II.57 Formato de dirección IP y su agrupación en octetos 159
II.58 IPX 163
II.59 Red interna de Appletalk 164
II.60 Zócalos de uso de los clientes del Zócalo para enviar y recibir Datagramas 165
II.61 Encapsulación de un datgrama en una trama 168
II.62 Cabecera 169

II.63 Formato del segmento TCP 172
II.64 Formato de los campos en un Datagrama UDP 174
II.65 Estratificación conceptual por capas de UDP entre aplicación e IP 175
II.66 Datagrama UDP encapsulado en un datagrama IP para su transmision a través de la Red 175
II.67 Ejemplo de multimplexado de una capa sobre IP 176
III.1 Tiempo fuera de servicio de un componente simple 191
III.2 Disponibilidad Serie en un sistema de 2 componentes 192
III.3 Disponibilidad Serie en un sistema de N componentes 193
III.4 Disponibilidad en un sistema Paralelo 193
III.5 Disponibilidad paralela en un sitemade 2 componentes 193
III.6 Analizando el cmino de la Red1 a la Red2 196
III.7 Análisis del camino 197
III.8 Topología Serie Simple 198
III.9 Topología de Red Paralela Simple 199
III.10 Diagrama de red para ejemplificar un error humano 214
III.11 El RBD para ejemplos de errores humanos 214
III.12 Datos que se necesitan colectar de cada falla 217
IV.1 Nuevas líneas de telefonia IP 227
V.1 Formato de paquete de encabezado de IPv6 235
V.2 Unicast envía paquetes a una interfaz específica 238
V.3 Multicast envía paquetes a la subred y define dispositivos específicos para los paquetes de multicast 238
V.4 Ancast envía paquetesa una interfaz de uan lista específica y puede contener nodos termnales routers 239
V.5 Red UNAM IPv6 de producción 241
V.6 LSR 243
V.7 VPNs MPLS 246
V.8 Ingeniería de trafico MPLS 247
V.9 Modelo de referencia de PWE3 251
V.10 El efecto de adoptar un sistema Multiportadora 255
V.11 Concepto de señal OFDM 257
V.12 Encabezado del PLCP para OFDM 258
V.13 Trasmisor y Receptor para OFDM 260
V.14 Conexión e una VPN 262
V.15 Como funciona una VPN 263
V.16 Ejemplos de enlaces con VPNs 263
V.17 Ejemplo de una red implementando VPNs 266
VI.1 Diagrama de Red Frame Relay 268
VI.2 Diagrama de Red e Sitio Local 269
VI.3 Elementos e Core 270
VI.4 Elementos de Distribución 271
VI.5 Elementos de Acceso 271

VI.6 Sitio Remoto 1 272
VI.7 Sitio Remoto 2 272
VI.8 Diagrama de Red MPLS 274
VI.9 Diagrama de Red Sitio Local MPLS 275
VI.10 Elementos de Core 276
VI.11 Elementos de Distribución 277
VI.12 Elementos de Acceso 277
VI.13 Integración de la red de Voz sobre la red de datos 278
VI.14 Creación de VPN a trvés de Internet 278
VI.15 Sitio Remoto 1 279
VI.16 Sitio Remoto 2 280
VI.17 Diagrama de bloques para el RBD de la red Frame Relay 281
VI.18 Diagrama de Bloques para el RBD de la red MPLS 284

Tablas

I.1 Canales Alámbricos 6
I.2 Bandas de Frecuencias en las que operan los satélites 8
I.3 Aplicaciones del Espectro Electromagnético 10
I.4 Problemas más comunes 29
II.1 Tabla de conversión para conductores sólidos 61
II.2 Categorías de Cable UTP 63
II.3 Rango de Transmisión de datos ADSL 74
II.4 Rango de Transmisión de Datos VDSL 77
II.5 Comparación de Tecnologías xDSL 78
II.6 Características HSSI 79
II.7 Entradas y Salidas del Rs-232 81
II.8 Descripción del Rs-232 82
II.9 Definiciones G.700 83
II.10 Características Eléctricas 83
II.11 Características Eléctricas 84
II.12 Características Eléctricas 84
II.13 Características Eléctricas del T1 84
II.14 Algunas Características para E1 85
II.15 Fijación de especificaciones 85
II.16 V.35 85
II.17 Descripción del V.35 86
II.18 Voltajes X.21 87
II.19 Descripción X.21 87
II.20 Descripción Rs-449 89
II.21 Clasificación de las fibras ópticas 92
II.22 Categorías de fibras multimodo 98
II.23 Tabla de codificación DQPSK 115

II.24 TABLA DE CODIFICACIÓN QPSK 115
II.25 ARACTERÍSTCAS DE IEEE 802.3 136
II.26 BYTES DE DIRECCIONAMIENTO MAC 144
II.27 VARIANTES DE CALIDAD DE SERVICIO 154
II.28 CLASIFICACIÓN DE CALIDAD DE SERVICIO 155
II.29 CLASES DE DIRECCIONES IP 160
II.30 PRIMITIVAS DE DATAGRAMAS 167
II.31 PRIMITIVAS DE SESIONES 167
II.32 PUERTOS ASIGNADOS PARA UDP 178
III.1 FACTORES DE DISPONIBILIDAD Y PÉRDIDAS ANUALES 182
III.2 NÚMERO DE 9S 185
III.3 EFECTO DE UN MTTR EN TÉRMINOS DE DISPONIBILIDAD 200
III.4 EFECTO DEL UPS SOBRE LOS CORTES DE ENERGÍA 206
III.5 IMPACTOS DE LA COMPLEJIDAD 208
III.6 EJEMPLOS DE CONTRIBUCIONES DE TIEMPOS INACTIVOS DEBIDOS A ERRORES HUMANOS Y PROCESOS 212
III.7 LOS NÚMEROS DE DISPONIBILIDAD PARA ERORES HUMANOS 214
V.1 CARACTERES HEXADECIMALES 235
V.2 CONFIGURACIONES POSIBLE PARA LOS BITS DEL CAMPO DE SEÑALIZACIÓN 259
VI.1 DISPONIBILIDAD PARA CADA UNO DE LOS ELEMNTOS DE LA RED FRAME RELAY 281
VI.2 DISPONIBILIDAD PARA CADA UNO DE LOS LEMENTOS DE LA RED MPLS 283
VI.3 COSTOS DE LOS SERVICIOS FRAME-RELAY 289
VI.4 COSTOS DE LOS SERVICIOS MPLS 290

FORMULAS

I.1 NÚMERO DE ENLACES NECESAROS PARA IMPLANTAR UNA TOPOLOGÍA COMPLETA 20
II.1 RELACIÓN SEÑAL/RUIDO EN VOLTAJES 59
II.2 RELACIÓN SEÑAL/RUIDO EN POTENCIAS 59
II.3 CAPACIDAD DE CANAL 59
II.4 SEÑAL DE LA FRECUENCIA PORTADORA 109
II.5 SEÑAL QUAM GENERAL 111
II.6 SEÑAL QUAM GENERAL 111
II.7 CÓDIGOS HAMMING PERMISIBLES 117
III.1 PORCENTAJE DE DISPONIBILIDAD 187
III.2 DISPONIBILIDAD 190
III.3 ECUACIÓN DE DISPONIBILIDAD SERIE 191
III.4 ECUACIÓN DE DISPONIBILIDAD PARALELA 192
III.5 DISPONIBILIDAD TOTAL 194

BIBLIOGRAFÍA

Sistemas de Comunicación.
B.P. Lathi.
Ed. Interamericana, México, 1986.

Introducción a las Telecomunicaciones Modernas.
Enrique Herrera Pérez.
E.d Limusa, México, 1998.

Web Pro Forum Tutorials.
http://www.iec.org
The International Engineering Consortium.

Análisis de Fourier.
Hwei P. Hsu.
Ed. Prentice Hall, México, 2000.
Señales y Sistemas.
Alan V. Oppenheim,
Alan S. Willsky.
Ed. Prentice Hall, 2ª ed., México, 1998.

Sistemas de Comunicaciones Electrónicas.
Wayne Tomasi.
Ed. Pearson Education, México, 1998.

Redes de Computadoras.
TANEMBAUM, Andrew S.
Prentice Hall. Tercera Edición. México. 1997.

Protocolos, normas e interfaces.
BLACK, Uyless
Computec RA- MA. México. 1997.

MICROSOFT TRAINING AND CERTIFICATION TECHNICAL EDUCATION CENTER.
Networking Essentials.Cargraphics S.A. Santa Fe de Bogotá (Colombia).

Redes para proceso distribuido.
GARCÍA TOMAS, Jesús.
Computec Ra-Ma. México. 1997

Tempel Red/com
Referencia de Estándares de Redes LAN
El Comité 802, o proyecto 802, del *Instituto de Ingenieros en Eléctrica y Electrónica* (IEEE) .

OSI REFERENCE MODEL
Copyright 1996 © Cisco Systems Inc.

REDES DE BANDA ANCHA
http://www.ts.es/doc/area/produccion/ral/BANDA.HTM

Laboratorio de Redes.
http://ccdis.dis.ulpgc.es/ccdis/laboratorios/redes.html

http://www.apple.com
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/applet.htm
Posted: Wed Feb 20 21:52:07 PST 2002

COMISION FEDERAL DE TELECOMUNICACIONES
PROYECTO de Norma Oficial Mexicana PROY-NOM-152-SCT1-1999, Interfaz digital a redes públicas
(Interfaz digital a 2 048 kbit/s).

An Overview of IEEE 802.12 Demand Priority
A Albretch, J. Curcio, D. Dove, S. Goody.
Proceedings of GLOBECOM, 1994.

The Demand Priority MAC Protocol.
G. Watson, A Albretch, J. Curcio, D. Dove, S. Goody, J. Grinham, M. Pratt, P Thaler.
IEEE Networks Magazine, January, 1995.

Métodos de acceso.
©Global NT, S.A. de C.V.

Digital Communications.
John G.Proakis.
McGraw-Hill, 3ªEd.,1995.

Digital Communications.
B. Sklar.
Prentice Hall.

High-Speed Cable Modems: Including IEEE 802.14 Standards.
Albert A .
McGraw-Hill Computer Communications Series.

Comunicaciones y redes de computadores
Stallings, W.
quinta edición, Prentice Hall 1997.

Pseudo Wire Edge to Edge (PWE3)
http:community.roxen.com/developers
Thomas H. Nadeu, Monique Morrow, Cisco Systems Inc., Peter Busschbach, Lucent Technologies Editors.
Enero 2004.

IPv6.
http://www.cisco.com/univercd/ cc/td/doc/cisintwk/ito_doc/ipv6.htm.
http://www.cisco.com/ipv6.

IPv6 México
http://www.ipv6.unam .mx
DGSCA UNAM.