2.2.2. Tarjetas de Interfaz (NIC) 63
2.2.3. Estructura de una estación de trabajo y un servidor 64
2.2.4. Sistemas Operativos de Red (NOS) 64
2.3. Métodos de acceso al medio 65
2.3.1. ALOHA simple 65
2.3.2. S-ALOHA (ALOHA Ranurado) 66
2.3.3. CSMA/CD (Acceso múltiple con detección de portadora y detección de colisiones) 67
2.4. Estándares IEEE 802.XX 69
2.4.1. Estándar IEEE 802.1 70
2.4.2. Estándar IEEE 802.2: Control Lógico de Enlace 70
2.4.3. Estándar IEEE 802.3 71
2.4.3.1. Estándar IEEE 802.3: Ethernet ® 71
Procedimiento de generación del CRC 75
Temporizaciones 77
2.4.3.2. Estándar IEEE 802.3u: Fast Ethernet (Ethernet rápido) 78
2.4.3.3. Estándar IEEE 802.3z Ethernet a 1 Gbps 79
2.4.4. Estándar IEEE 802.4: Token Bus 80
2.4.5. Estándar IEEE 802.5: Token Ring 81
2.4.6. Estándar IEEE 802.6: Bus doble de colas distribuidas 83
2.4.7. Estándar IEEE 802.7: Grupo asesor técnico de ancho de banda 83
2.4.8. Estándar IEEE 802.8: Grupo asesor técnico de fibra óptica 84
2.4.9. Estándar IEEE 802.9: Redes integradas de voz y datos 84
2.4.10. Estándar IEEE 802.10: Grupo asesor técnico de seguridad de redes 84
2.4.11. Estándar IEEE 802.11: Redes inalámbricas (WLAN) 85
2.4.12. Estándar IEEE 802.12 (100VG Any LAN) 89
2.4.13. Estándar IEEE 802.13 90
2.4.14. Estándar IEEE 802.14: Protocolo MAC para redes HFC de CATV 91
2.4.15. Estándar IEEE 802.15: Acceso inalámbrico para redes de área personal (PAN) 96
2.4.16. Estándar IEEE 802.16: Acceso inalámbrico fijo de banda ancha (para LAN y MAN) 96
2.4.17 Formas de cableado 100
2.4.17.1 10BASE-5 (Ethernet de coaxil grueso) 100
2.4.17.2. 10BASE-2 (Ethernet de coaxil delgado) 100
2.4.17.3 10BASE-T 100
2.4.18. Dispositivos de Red 101
2.4.18.1. Hub 101
2.4.18.2. Switch 102
Configuración de redes conmutadas 104
Protocolo Spanning Tree (IEEE 802.1d) 104
LAN Virtuales (VLANs) 106
2.5. Redes Área Extendida (WAN) 111
2.5.1 Clasificación de las WANs 111
2.5.2. Ejemplos de WANs 111
2.5.3. Red Telefónica Pública Conmutada (RTPC) 111
2.5.4. Frame Relay 137
2.5.5. SONET 142
2.5.6. Jerarquía Digital Síncrona (SDH) 147
2.5.7. Red Digital de Servicios Integrados (RDSI) 152
2.5.9. Modo de Transferencia Asíncrono (ATM) 164
2.5.10. Redes Satelitales (VSAT) 169
Preguntas de Repaso a la Unidad 2 177
Bibliografía de la Unidad 2 183

UNIDAD 3:
Direccionamiento IP - Administración del Tráfico 185
3.1. Protocolo IP (Protocolo Internet) 186
3.1.1. Direcciones IP (versión 4) 188
3.1.2. Protocolo de configuración dinámica de host (DHCP) 195
3.1.3. IPV6 197

3.1.4. Protocolo ICMP (Protocolo de Control de Mensajes de Internet) 199
3.1.5. Protocolo de Resolución de Direcciones (ARP) 204
3.1.6. RARP 207
3.1.7. Proxy 207
3.1.8. Protocolo de Traducción de direcciones de Red (NAT) 209
3.2. Enrutamiento 212
3.2.1. Introducción 212
3.3. Enrutamiento por la trayectoria más corta 212
3.4. Inundación 213
3.5. Enrutamiento basado en flujo 214
3.6. Enrutamiento por vector de distancia 215
3.6.1. El problema del conteo a infinito 215
3.6.2. Recorte por horizonte dividido 216
3.7. Enrutamiento por estado de enlace 216
3.7.1. Conocimiento de los vecinos 216
3.7.2. Medición del costo de la línea 217
3.7.3. Construcción de los paquetes de estado de enlace 217
3.7.4. Distribución de los paquetes de estado de enlace 217
3.7.5. Cálculo de las nuevas rutas 218
3.8. Enrutamiento jerárquico 222
3.9. Enrutamiento para hosts móviles 222
3.10. Enrutamiento por difusión 224
3.11. Congestión 226
3.11.1. Principios generales del control de congestionamiento 226
3.11.2. Algoritmos de control de congestionamiento 226
3.12. Calidad de Servicio en Redes 231
3.12.1. Introducción 231
3.12.2. Beneficios de la QoS: 231
3.12.3. Arquitectura básica de la QoS 232
3.12.4. Gestión de la QoS 238
EJERCICIOS SOBRE DIRECCIONAMIENTO IP 239
Ejercicios propuestos 239
Ejercicios Resueltos 240
Bibliografía de la Unidad 3 242

UNIDAD 4:
Capa de transporte (TCP) - Capa de Aplicación - Internet 245
4.1. Internet 246
4.1.1. Tipos de acceso 247
4.2. Protocolo TCP (Protocolo de Control de Transporte) 250
4.2.1. La cabecera de segmento TCP 250
4.2.2. Números de puertos TCP 252
4.2.3. Control de Congestionamiento con TCP 253
4.2.4. Interfaces TCP 254
4.2.5. Estados del TCP 255
4.2.6. Protocolo UDP (Protocolo de Datos de Usuario) 256
4.3. DNS (Sistema de nombres de dominio) 257
4.3.1. El espacio de nombres del DNS 257
4.3.2. Registros de recursos 258
4.3.3. Servidores de nombres 259
4.4. SNMP (Protocolo sencillo de administración de redes) 261
4.5. Correo electrónico 264
4.5.1. El agente de usuario 265
4.5.2. Envío de correo electrónico 265
4.5.3. Lectura del correo electrónico 265
4.5.4. Formato de mensaje 267
4.5.5. Transferencia de mensajes 269

4.5.6. Confidencialidad en el correo 270
4.6. World Wide Web 273
4.6.1. Del lado del cliente 273
4.6.2. Del lado del servidor 274
4.6.3. HTTP (Protocolo de transferencia de hipertexto) 275
4.6.4. Localización de información en la Web 276
4.7. Voz sobre IP 276
4.7.1. Justificación tecnológica y económica 276
4.7.2. El estándar VoIP 278
4.7.3. Elementos para Voz sobre IP 280
Bibliografía de la Unidad 4 283
PREGUNTAS DE REPASO INTEGRADOR 284

UNIDAD 5:
Sistemas Operativos de Redes 289
5.1. Sistemas operativos de red 290
5.1.1. Componentes de un sistema operativo de red 290
5.2. Modelos 291
5.2.1. Modelo de redes entre pares 291
5.2.2. Modelo Cliente-Servidor 294
5.2.3. Ejemplos de sistemas operativos para red del tipo cliente servidor 296
Bibliografía de la Unidad 5 323

UNIDAD 6:
Seguridad en las redes 325
6.1. Conceptos de Seguridad Informática 326
6.1.1. Secreto 326
6.1.2. Validación de identificación 327
6.1.3. No repudio 327
6.1.4. Control de integridad 327
6.1.5. Seguridad según la Arquitectura OSI 327
6.2. Amenazas a la seguridad de la información 328
6.2.1. Tipos de ataques a la seguridad 328
6.2.2. Servicios de Seguridad 330
6.2.3. Mecanismos de Seguridad 332
6.2.4. Niveles de Seguridad 333
6.2.6. Arquitectura y niveles de seguridad en LANs 335
6.2.7. Protección de la información 338
6.2.8. Protección de recursos 339
6.2.9. Seguridad con UNIX 340
6.2.10. Seguridad en Novell 340
6.2.12. Respaldo de datos 342
6.2.13. Seguridad global 342
6.2.14. Impacto en la organización 343
6.2.15. Visibilidad del proceso 343
6.2.16. Políticas generales de seguridad 344
6.2.17. Hackers 345
6.2.18. Programas que afectan a los sistemas de computadoras 349
6.2.18.3. Generaciones de Virus 352
6.2.18.5. Especies de Virus 355
6.2.18.6. Daños de los virus 356
6.2.18.7. Síntomas típicos de una infección 356
6.2.18.9. Tácticas Antivíricas 358
6.3. Cifrado Tradicional 361
6.4. Algoritmos de Clave Secreta 365
6.4.1. DES (Estándar de Cifrado de Datos) 366
6.4.2. IDEA (Algoritmo Internacional de Cifrado de Datos) 367

6.5. Algoritmos de Clave Pública 368
6.5.1. RSA 369
6.6. Protocolo de Validación de Identificación 371
6.6.1. Validación de Identificación basada en clave secreta compartida 372
6.6.2. Validación de Identificación usando un centro de distribución de claves 374
6.7. Firmas Digitales 381
6.7.1. Firmas de clave secreta 383
6.7.2. Firmas de clave pública 383
6.8. Firewalls 385
6.8.1. Firewalls y TCP/IP 387
6.9.1. Cómo trabajan las VPNs 406
6.9.2. Definiendo VLANs 408
Bibliografía de la Unidad 6 411

Unidad 1

Arquitectura de Redes

Objetivos

- Especificar conceptos de "red de telecomunicación" y "red de computadoras".
- Destacar las ventajas del uso de redes para comunicación de datos.
- Reconocer las aplicaciones de las redes informáticas.
- Definir la estructura de las redes tipo LAN y WAN.
- Describir las diferentes topologías de las redes.
- Analizar comparativamente las ventajas de una frente a otras.
- Definir la red corporativa, observar su evolución histórica y vislumbrar su futuro.
- Comprender la importancia de la normalización en telecomunicaciones.
- Identificar los organismos de estandarización internacional en telecomunicaciones existentes.
- Estudiar el concepto de arquitectura de redes.
- Explicar el Modelo de Referencia OSI.
- Describir el conjunto de protocolos TCP / IP
- Comparar las arquitecturas OSI y TCP/IP.

1.1. Concepto de Red de Telecomunicación

Es el conjunto de equipos y procedimientos conectados entre sí con la finalidad de compartir datos y recursos (Ver **figura 1.1(a)**).

Otra definición sería: ***"conjunto de medios técnicos instalados, operados, organizados y administrados, con la finalidad de brindar a los usuarios distintos servicios de telecomunicaciones"***. Una red de este tipo está dispuesta para permitir a usuarios distantes intercambiar informaciones entre ellos con un retardo lo más pequeño posible.

Respecto de esta definición podemos realizar un esquema jerárquico como el de la **figura 1.1.(b)** donde se pone de manifiesto que los equipos de usuarios deben conectarse a través de medios técnicos que gracias a los procedimientos nos permiten brindar un servicio.

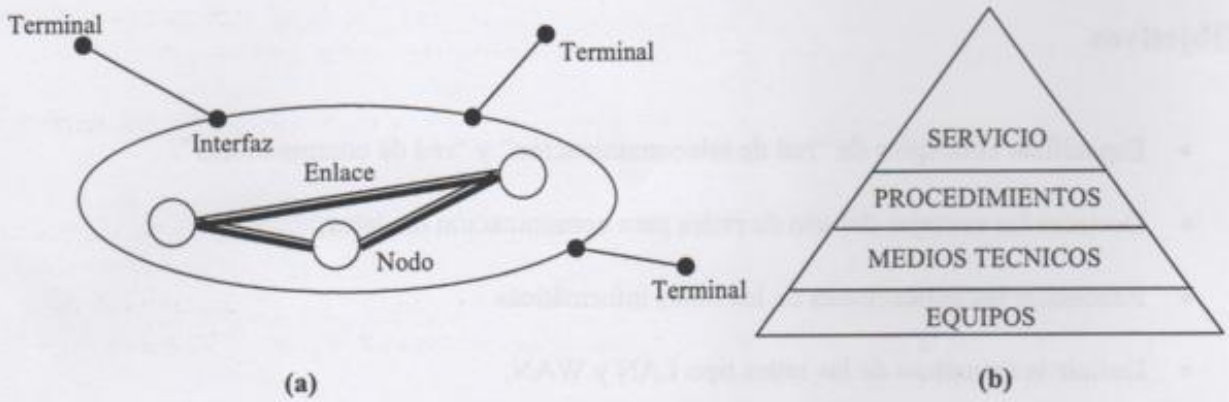


FIGURA 1.1: (a) Esquema de red de telecomunicación. (b) Esquema Jerárquico.

La más simple de las redes conecta dos equipos terminales (por ejemplo computadoras), permitiéndole compartir archivos e impresoras. Una red más compleja conecta todas las computadoras de una empresa en su oficina local y/o las de la compañía en todo el mundo. Entonces, decimos que las redes pueden ofrecer interconectar: personas con personas, personas con sistemas de computación, equipos de uso específico con sistemas de computación, o sistemas de computación entre sí.

1.2. Red Informática

Podemos ensayar una definición de red informática, diciendo que es un sistema de comunicación que interconecta múltiples usuarios, que tienen como objetivo compartir y tener acceso remoto a recursos de computación, como por ejemplo:

- **Recursos de Hardware:** Procesadores, discos, impresoras, *plotters*, *scanners*, etc.
- **Recursos de Software:** Compiladores, paquetes de bases de datos, herramientas varias.
- **Recursos de Información**: Bases de datos, estadísticas, mensajes, etc.

Estas definiciones generales son aplicables a cualquier tipo de red, pero, se debe aclarar que se necesitan ciertos elementos mínimos para estar en presencia de una "red de computadoras", ellos son:

- **Conectividad:** es el conjunto de *hardware* y *software* que permite que una computadora se comunique con otra, al menos del mismo tipo. (Interfaz de red, medio físico, topología, protocolos, dispositivos de interconexión, etc.)

- **Compartición de Recursos:** posibilidad que tiene, al menos una computadora de las conectadas, de utilizar un recurso que le es propio a otra (cuota de disco, archivos, impresoras, salida a Internet, etc.).

- **Administración de Recursos Compartidos:** posibilidad que brinda el Sistema Operativo de red de poder gestionar, en mayor o menor medida (según la versión del sistema operativo y la habilidad del administrador) la compartición de todos los recursos disponibles.

- **Seguridad:** es la estructura de permisos, prioridades, privilegios, tipos de usuarios, etc., que se pueden establecer para los usuarios de los recursos compartidos, de tal manera que no se pierdan, deterioren o inhabiliten dichos recursos debido al mal uso por parte de los usuarios.

A su vez en cualquier red de computadoras existen elementos que de acuerdo a su funcionamiento se clasifican en:

- Las **Estaciones de trabajo** son computadores que aprovechan o tienen a su disposición los recursos que ofrece la red así como los servicios que proporcionan los servidores a los cuales pueden acceder. Las estaciones de trabajo son las máquinas que no son servidores pero que forman parte de la red de cómputo y en las cuáles se centraliza todo el trabajo a realizar y las cuales están en intercomunicación permanente.

  Se pueden clasificar en:

  - **Terminales Bobas:** en este tipo de estación, los procesos los realiza el servidor.

  - **Terminales Inteligentes:** esta estación solicita el paquete al servidor, instalándolo en su memoria y luego trabaja con él en forma local.

- Los **Servidores** son aquellos computadores que van a compartir sus recursos de *hardware* y/o *software* con los demás equipos de la red. Son las máquinas que se encargan de administrar los recursos con los que cuenta la red, tales como: el sistema operativo, paquetes de cómputo, programas de aplicación, información, intercambio de la misma, conexión a Internet, etc.

  Tipos de servidores:

  - **Servidores Dedicados:** aquellos que están exclusivamente a disposición de la red.

  - **Servidores No Dedicados:** también pueden utilizarse como estaciones de trabajo.

  Ejemplos:

- **De Archivo:** prestan el servicio de transacciones de archivos (consultar, borrar, modificar, agregar, etc.)
- **De Proceso:** prestan la memoria y su capacidad de proceso a las estaciones (bobas.)
- **De Aplicaciones:** en ellos residen las aplicaciones a las cuales demandan servicio los clientes
- **De Señal:** envían señales de información a las estaciones (estudios de T.V. o radio.)
- **De Impresión:** manejan los servicios y elementos de impresión (cola, trabajo, etc.)

1.3. Componentes de una Red de Computadoras

El *hardware* está constituido por el cableado o líneas de comunicación (que unen los distintos computadores), las placas o tarjetas de conexión (que convierten las señales que circulan por los cables en datos accesibles al sistema) y los elementos de interconexión. Estos están determinados por la arquitectura o topología de la red. El cableado resulta fundamental al ser el encargado de transportar físicamente las señales de un computador a otro. El tipo y las características del cable utilizado dependen del modelo de red elegido, así como de las limitaciones impuestas por la localización física de la red.

El *software* de red (los protocolos de comunicaciones, el sistema operativo de red y programas de aplicación) intenta dar la sensación de que los recursos remotos a los que accede el usuario son locales al computador desde el cual está trabajando el usuario, de esta manera el usuario (o el programa de aplicación más exactamente) no verá la diferencia y funcionará compartiendo los recursos de los demás.

Resumiendo, se tiene como componentes (en orden descendiente):

- Aplicaciones.
- Sistema Operativo de Red.
- Protocolos de Comunicaciones
- Recursos de interconexión.
- Servidores.
- Clientes.
- Interfaces de Red.
- Sistema de Cableado.

Nota: se puede cambiar el *hardware* de una red cuando sea necesario, sin necesidad de cambiar el *software* y viceversa, es decir, cambiar el *software* sin cambiar el *hardware*. Una red debe estar estructurada en niveles para que un cambio en un nivel no afecte a los demás.

1.4. Ventajas de las Redes

- Las empresas están dispersas geográficamente. Las redes permiten que las distintas sucursales de una empresa puedan **compartir e intercambiar datos y programas** entre todo su personal.

- **Compartir recursos.** Recursos costosos como impresoras láser, *plotters*, etc. Además si una computadora se satura por exceso de trabajo, éste se puede dirigir a través de la red a otra computadora (la compartición de la carga de trabajo, redunda en una mejor utilización de recursos).

- **Tolerancia a fallos.** Si una computadora falla, otra puede asumir sus funciones y su carga. Ej: control de tráfico aéreo (no puede dejar de funcionar).

- **Entorno de trabajo flexible.** El uso de las redes permite disponer de un entorno de trabajo muy flexible. Los empleados pueden trabajar en su casa, conectados mediante redes a la computadora de su oficina. También se utilizan computadoras portátiles y se conectan cuando es necesario a la red, para obtener o entregar información a la empresa.

- **Alta fiabilidad.** Todos los archivos podrían duplicarse en dos o tres máquinas, por si alguna no funciona, se pueden utilizar estas copias.

- **Ahorro económico.** Las computadoras pequeñas tienen una mejor relación costo /rendimiento, comparada con las máquinas grandes (del tipo "*mainframe*").

- **Medio de comunicación entre personas.** Mediante una red, varias personas que viven en lugares muy distantes pueden trabajar bajo un mismo informe o investigación. En la actualidad estamos en la "era de la información". La sociedad actual se basa en la información para funcionar y los sistemas de comunicación de las redes proporcionan un rápido intercambio de información, incluso entre distintos países.

1.5. Aplicaciones de las Redes

Las aplicaciones de las redes se presentan en los más diversos campos de la actividad humana y van abarcando cada vez más; sólo a modo de ejemplo podemos presentar los siguientes:

- Programas de simulación de economía, proyectando qué sucedería si aumenta o disminuye la inflación, inversiones, etc.
- Acceso a bases de datos remotas. Reserva de trenes, aviones, hoteles, restaurantes, teatro. Realización de operaciones bancarias.
- Medio de comunicación. Envío de correo electrónico, fotos digitalizadas, voz, etc.
- Transacciones comerciales (*compra-venta*).
- Tablones de anuncios electrónicos (compra y venta).
- Tele trabajo.
- Educación a distancia.

1.6. Ejemplos de Redes de Telecomunicación

Según la naturaleza del servicio básico prestado, se distinguen en general, la Red Telefónica (intercambio de palabras), la RDSI[1] (voz y datos digitales), la red de CATV (imágenes de TV), Internet (datos y multimedia), etc.

1.6.1. La Red Telefónica

Por su cobertura geográfica y por la cantidad de abonados es la mayor del mundo. Está formada por:

- Los **aparatos de abonado**, que convierten la voz en señales eléctricas y viceversa.
- Las **centrales** que garantizan la conmutación y encaminamiento del tráfico de los abonados a ella unidos.
- Los **soportes de transmisión**, llamados líneas o circuitos según el caso, que garantizan la propagación de las señales a corta o larga distancia. (El término **línea** suele designar el soporte que une el abonado con su central, mientras que las conexiones entre centrales suelen llamarse **circuitos** o **enlaces troncales**.)

Para establecer una comunicación entre el abonado que llama y el abonado llamado (seleccionado por el número marcado), se conectan progresivamente centros de conmutación unidos mediante medios de transmisión. Las centrales intercambian entre ellas y con los abonados ciertas informaciones en el momento del establecimiento de la conexión y su ruptura; informaciones que constituyen la señalización.

La generalización del servicio telefónico en todo el mundo ha hecho de esta red, uno de los medios más difundidos para ser usado en la transmisión de datos, de ahí la importancia de su estudio en el conocimiento de las técnicas teleinformáticas.

Esta red se trata con más detalle en la unidad 2 (Redes WAN).

1.6.2. La red de CATV

Una red de CATV está compuesta básicamente por una cabecera de red, la red troncal, la red de distribución, y el último tramo de acometida al hogar del abonado.

La **cabecera** es el órgano central desde donde se gobierna todo el sistema. Suele disponer de una serie de antenas que reciben los canales de TV y radio de diferentes sistemas de distribución (satélite, microondas, etc...), así como de enlaces con otras cabeceras o estudios de televisión y con redes de otro tipo que aporten información susceptible de ser distribuida a los abonados a través del sistema de cable. Las redes de CATV originalmente fueron diseñadas para la distribución unidireccional de señales de TV, por lo que la cabecera era simplemente un centro que recogía las señales de TV y las adaptaba a su

[1] Red Digital de Servicios Integrados: es un estándar del CCITT para una red que acomoda una variedad de servicios de transmisión digital. En Inglés: ISDN (Integrated Services Digital Network).

transmisión por el medio cable. Actualmente, las cabeceras han aumentado considerablemente en complejidad para satisfacer las nuevas demandas de servicios interactivos y de datos a alta velocidad.

La **Red troncal** es la encargada de repartir la señal compuesta generada por la cabecera a todas las zonas de distribución que abarca la red de cable. El primer paso en la evolución de las redes clásicas todo-coaxial de CATV hacia las redes de telecomunicaciones por cable HFC consistió en sustituir las largas cascadas de amplificadores y el cable coaxial de la red troncal por enlaces punto a punto de fibra óptica. Posteriormente, la penetración de la fibra en la red de cable ha ido en aumento, y la red troncal se ha convertido, por ejemplo, en una estructura con anillos redundantes que unen nodos ópticos entre sí. En estos nodo ópticos es donde las señales descendentes (de la cabecera a usuario) pasan de óptico a eléctrico para continuar su camino hacia el hogar del abonado a través de la red de distribución de coaxial. Esto es lo que se llama una **Red HFC** que es una red de cable que combina en su estructura el uso de la fibra óptica y el cable coaxial. (Ver **figura 1.2**) Este tipo de redes representa la evolución natural de las redes clásicas de televisión por cable (CATV). En los sistemas bidireccionales, los nodos ópticos también se encargan de recibir las señales del canal de retorno o ascendentes (del abonado a la cabecera) para convertirlas en señales ópticas y transmitirlas a la cabecera.

La **Red de Distribución** está compuesta por una estructura tipo bus de coaxial que lleva las señales descendentes hasta la última derivación antes del hogar del abonado. La acometida a los hogares de los abonados es, sencillamente, la instalación interna del edificio, el último tramo antes de la base de conexión.

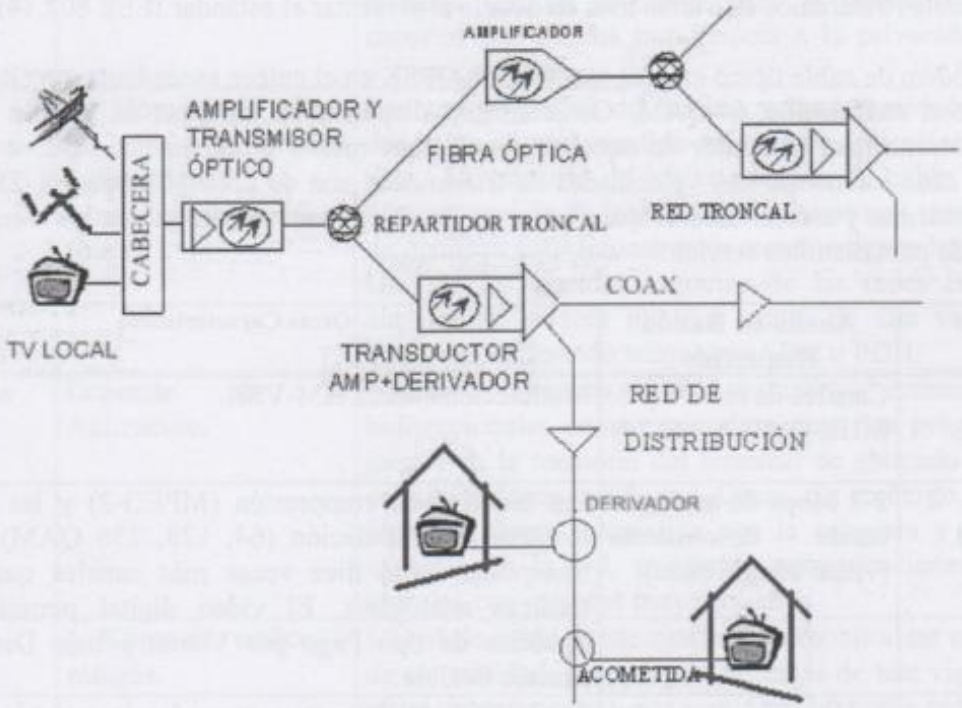


FIGURA 1.2: Ejemplo de una red CATV.

Una red moderna HFC con capacidad para comunicaciones bidireccionales puede ofrecer una gran variedad de servicios de telecomunicación (Ver el estándar IEEE 802.14 en el apartado 2.4.14). El diseño

de un sistema de cable requiere un conocimiento detallado de las aplicaciones y servicios que deberá soportar, ya que si no sabemos esto no podremos determinar las prestaciones de la red. Una idea que ha de tenerse siempre presente es la de que las aplicaciones evolucionan con el tiempo, y posiblemente lo harán de maneras que hoy todavía no podemos prever. Debemos tener en cuenta esta evolución tanto si la producen factores externos a las redes de cable (el progreso de la tecnología de computación, los usos cambiantes de la comunicación electrónica, etc.), como si es la propia tecnología del cable la responsable. Pero tanto en un caso como en el otro, predecir su dirección se reduce a menudo a mera especulación.

Normalmente se hace una distinción entre aplicación y servicio. Se puede ver claramente la diferencia con un par de ejemplos: las comunicaciones de voz y fax son dos aplicaciones soportadas por el servicio telefónico convencional; el servicio de Internet (basado en el protocolo de transporte IP) soporta una multitud de aplicaciones tales como correo electrónico, acceso remoto, WWW, ftp, etc.

En cualquier caso, el servicio limita a las aplicaciones; el servicio telefónico no puede, por ejemplo, soportar aplicaciones que requieran un gran ancho de banda.

En el caso del servicio de televisión por cable, gracias al gran ancho de banda disponible (86 a 862 MHz. para el canal descendente; y 5 a 55 MHz. para el canal de retorno), pueden soportarse aplicaciones de reproducción de video (canales digitales comprimidos mediante MPEG, por ejemplo) que son muy poco sensibles a retardos fijos de transmisión (hasta un par de segundos).

Últimamente se habla mucho del acceso a Internet mediante módems de alta velocidad a través de las redes de cable (trataremos este tema más en detalle al presentar el estándar IEEE 802.14).

Un módem de cable típico emplea modulación QPSK en el enlace ascendente y recibe los datos de la cabecera con modulación 64-QAM. Generalmente disponen de sistemas de gestión dinámica del espectro de retorno para transmitir en aquellos canales que menos problemas de ruido e interferencias presentan en cada momento. Las velocidades de transmisión son de unos 10Mbps y 1-2Mbps para los canales descendentes y ascendentes, respectivamente. En el siguiente cuadro se ven los requerimientos de ancho de banda para distintos servicios

Aplicación	Ancho de Banda Requerido	Otras Características
Difusión de Video Analógico	Canales de entre 6 y 8 MHz.	Modulación clásica AM-VSB.
Difusión de vides Digital	2-3 Mbps de ancho de banda descendente (video comprimido).	Las técnicas de compresión (MPEG-2) y las eficientes técnicas de modulación (64, 128, 256 QAM) permiten transportar hasta diez veces más canales que con las técnicas analógicas. El vídeo digital permite ofrecer servicios de tipo Pago por Visión y bajo Demanda de manera flexible.
Video Bajo Demanda	3 Mbps de capacidad del canal descendente (comprimido) y una pequeña capacidad del canal de retorno que permita la interactividad (del orden de 1 Kbps).	Posibilidad de detener y reanudar la reproducción por parte del usuario. El operador de red necesita una serie de mecanismos de seguridad para las aplicaciones de Pago por Visión. Se requiere un servidor especial de vídeo en la cabecera para simular las funciones de un aparato de vídeo casero convencional.

Televisión Avanzada	10 Mbps de ancho de banda descendente (comprimido).	Los estándares propuestos de televisión de alta definición (HDTV) requieren mucha mayor capacidad de la red. Una imagen de alta definición de 1240 x 720 pixel (no comprimida) requiere tres veces la velocidad de transmisión necesaria para una imagen de vídeo ordinario no comprimida.
Audio Digital	1 Mbps de ancho de banda descendente.	Exigencias de reproducción análogas a las del vídeo bajo demanda. Las técnicas de compresión permiten reducir de 1.4 Mbps a 384 Kbps la velocidad de transmisión necesaria para un canal de audio de calidad CD.
Telefonía	600 Kbps bidireccional (no comprimido). Mediante técnicas de compresión, la capacidad requerida es considerablemente menor.	Teóricamente basta con 128 Kbps (64 Kbps en cada sentido), pero ha de hacerse frente a problemas de Retardo de Paquetización y otros retardos que introduce la red y que precisan de técnicas de cancelación de ecos. Los usuarios demandan privacidad en las comunicaciones y los estándares de servicio telefónico exigen una alta fiabilidad del sistema.
vides-Conferencia	118 Kbps bidirec-cional (comprimido).	Tasas de bit muy variables. Hay aplicaciones de baja calidad que funcionan a 28 Kbps en Internet. La red de cable puede ofrecer un servicio de mayor calidad empleando capacidades de entre 100 Kbps y 1 Mbps. Los retardos son un problema para la interactividad. Los usuarios dan mucha importancia a la privacidad de sus comunicaciones.
Redes de Computadoras	10 Mbps a 100 Mbps (ó más) de tráfico bidireccional, generalmente a ráfaga (bursty).	Las características del tráfico y las necesidades futuras dependen en gran medida del tipo de aplicaciones que se usen. La mayoría de los operadores de cable tienden a ofrecer servicio de Internet, que soporta una gran cantidad de distintas aplicaciones muy atractivas para los usuarios. Uno de los grandes negocios de las redes HFC es el alquiler de enlaces punto a punto de alta velocidad a empresas, utilizando tecnología SDH o PDH.
Video-Juegos	Depende de la Aplicación.	Algunos sistemas no requieren comunicaciones bidireccionales puesto que almacenan los programas de juegos en la memoria del terminal de abonado y no hay comunicaciones con la red. Otros, sin embargo, permiten jugar de forma interactiva con la cabecera y con otros usuarios de la red, exigiendo comunicaciones bidirec-cionales con retardos muy pequeños.
Telemetría	1 Kbps de tráfico a ráfagas.	La red de cable puede usarse para monitorizar contadores de electricidad, gas, y agua; sistemas de tele vigilancia; y otros sistemas como, por supuesto, la propia red de cable. La seguridad y la fiabilidad son esenciales para muchas aplicaciones.

FIGURA 1.3: Características de las principales aplicaciones que puede soportar el servicio de cable.

1.7. Concepto de Teleinformática

La palabra Teleinformática está constituida por la contracción de las palabras **telecomunicaciones** e **informática**. Se la podría definir como la ciencia que estudia el conjunto de técnicas que es necesario usar para poder transmitir datos dentro de un sistema informático o entre puntos de él, situados en lugares remotos y usando redes de telecomunicaciones.

Esencialmente, se trata de estudiar la implicancia que tiene la conexión de computadoras, equipos informáticos auxiliares y equipos terminales de datos a redes de comunicaciones.

El problema fundamental que busca resolver, por lo tanto, es el de lograr que un computador pueda dialogar con equipos situados geográficamente distantes, reconociendo las características esenciales de la información como si la conexión fuera local, usando redes de telecomunicaciones.

A continuación se citan dos definiciones más de **Sistema Telemático**:

- "En el campo de la Telemática entra toda la tecnología, sistema, red o servicio en los que operativamente y en la proporción que sea se imbriquen computadores y comunicaciones; y más específicamente, la Telemática es el campo genuino de aplicaciones de la informática como soporte de las comunicaciones."

- "Conjunto de conceptos, técnicas y servicios surgidas de la transmisión de datos, la telefonía y de su crecimiento y acercamiento natural posibilitado por el desarrollo de la microelectrónica y el uso del computador y la ingeniería del *software* como procesador para comunicaciones."

Por lo tanto, un **sistema telemático** puede definirse como el **conjunto de recursos distribuidos que emplean los procesos para comunicarse**.

Dentro de esta última definición, hay que aclarar dos conceptos: el primero es **proceso**, que se define como una entidad informática que realiza algún tipo de tarea o tareas y se está ejecutando en una estación; por otra parte, se define la **comunicación entre procesos** al conjunto de técnicas de intercambio de información utilizadas por los procesos se estén ejecutando en una misma o en diferentes máquinas.

Al tratar sobre sistemas telemáticos se tendrá que realizar una distinción entre lo que son sistemas distribuidos y redes de computadores. Los primeros son aquellos en que cada elemento del sistema se encarga de la realización de una tarea con el fin de lograr un objetivo global y entre los diferentes elementos del sistema se produce un intercambio de información con este fin. Un ejemplo muy claro de sistema distribuido es un conjunto de autómatas interconectados en una cadena de montaje. En cambio, una red de computadores es un conjunto de máquinas conectadas entre sí y que pueden emplear todos los recursos disponibles sobre los que tengan autorización, siendo cada uno de los elementos de este sistema telemático independiente de los demás.

1.7.1. Evolución de los Sistemas Telemáticos

La telemática es una disciplina relativamente joven, que comenzó a ser conocida como tal a comienzos de la década de los 70. Los primeros sistemas de proceso de datos de los años 50 y 60 (computadores de primera, segunda y tercera generación), no consideraban la comunicación y la

transferencia de información como una de sus principales características; en aquel momento, la importancia radicaba en la mejora de la velocidad de proceso. Con el aumento y el abaratamiento del *hardware*, los dispositivos de *entrada / salida*, y por tanto las comunicaciones entre los computadores, comenzaron a tener un mayor interés, fundamentalmente para lograr el objetivo de distribuir y descentralizar en dos sentidos:

- Distribución de los datos o información, como es el caso del acceso a las bases de datos remotas.
- Distribución del procesamiento, mediante el reparto de las tareas entre las diferentes máquinas dentro de un sistema telemático.

Los objetivos de la distribución tienen tres motivos importantes:

- Economía de recursos.
- Flexibilidad en el crecimiento.
- Seguridad por redundancia.

1.8. Clasificación de las Redes de Telecomunicación

1.8.1. De acuerdo con el Tipo de Transmisión

1.8.1.1. Redes de Difusión (*Broadcast*)

Son aquellas que utilizan canales de difusión; en ellas existe un solo canal de comunicación compartido por todos los terminales de la red.

El punto clave es determinar quién tiene derecho a usar el medio (canal) cuando existe competencia por éste. Los mensajes cortos que envía una máquina son recibidos por todas las demás. Un campo de dirección dentro del paquete especifica a quién se dirige. Al recibir un paquete, una máquina verifica el campo de dirección. Si el paquete está dirigido a ella, lo procesa; si está dirigido a otra máquina, lo ignora.

Los sistemas de difusión generalmente ofrecen la posibilidad de dirigir un paquete a todos los destinos colocando un código especial en el campo de dirección. Cuando se transmite un paquete con este código, cada máquina en la red lo recibe y lo procesa. Este modo de operación se llama **difusión** (*broadcasting*).

La **multidifusión** es una forma de transmisión a un subconjunto de máquinas. Esto se maneja con un número de grupo. Cada máquina se puede suscribir a cualquier grupo o a todos.

1.8.1.2. Redes Punto a Punto o Redes Conmutadas

Son aquellas que utilizan conexiones punto a punto, es decir, consisten en muchas conexiones entre pares individuales de máquinas. Cuando se dispone de un solo canal, la determinación de quien utilizará es servicio, se hace más fácil. Para ir del origen al destino, un paquete en este tipo de red puede tener que visitar primero una o más máquinas intermedias. A veces son posibles múltiples rutas de diferentes longitudes, por lo que los algoritmos de enrutamiento desempeñan un papel importante en este tipo de redes.

Como regla general (aunque hay muchas excepciones), las redes pequeñas geográficamente localizadas tienden a usar la difusión, mientras que las redes más grandes suelen ser punto a punto.

1.8.2. De acuerdo con su propiedad

1.8.2.1. Públicas

Son redes que prestan servicios a terceros. El servicio que prestan puede ser simplemente transporte de información o servicios de valor agregado. Como es necesario cobrar por dicho servicio, tienen muy desarrollados los esquemas de tarifación. Por lo general son redes de amplia cobertura. Ejemplo: Red Telefónica Conmutada.

Se dice también que una red de telecomunicaciones tiene carácter público, cuando las solicitudes de servicio o los requerimientos necesarios para ser usuario de la misma, no tienen otra restricción, que las disponibilidades de los medios técnicos. Este tipo de red puede ser operada en cada país por: una o varias administraciones de capital estatal; una o varias administraciones de capital privado; una o varias administraciones de capital fijo.

1.8.2.2. Privadas

Son propiedad de una empresa o entidad en particular y están sólo al servicio de ésta; es decir, cuando es operada para un fin determinado y sus usuarios pertenecen a una o varias corporaciones que tienen intereses en la misma.

Por lo general no tienen muy desarrollados los esquemas de tarifación y control. Son utilizadas para aumentar la productividad y para dar soporte a la operación de dichas entidades.

Los casos de redes privadas que pueden señalarse como más significativos son:

Redes para aplicaciones específicas simples

Son aquellas que se utilizan para resolver una única aplicación, que puede intercomunicar a una o varias organizaciones o empresas.

Redes de empresas

Son aquellas que responden a las necesidades de una organización o empresa, interconectando sus instalaciones y brindando un servicio dedicado y orientado a las aplicaciones que les resultan más convenientes.

Redes para usos militares

Son aquellas diseñadas para uso exclusivo de las Fuerzas Armadas.

Redes multiorganizativas

Son aquellas que a diferencia de las anteriores, responden a las necesidades de una aplicación común a varias empresas, o a un determinado conjunto de intereses comunes.

1.8.3. De acuerdo con el Tipo de Tráfico

Los diferentes tipos de tráfico presentan características distintas, lo cual ha hecho que los desarrollos para los diferentes tipos de tráfico se hayan hecho por separado, creando dos mundos muy diferentes.

1.8.3.1. Voz

Tráfico que no admite retardos, ni adelantos (Isócrono). Admite pérdidas de pequeños pedazos de la información. Ocupa un ancho de banda constante, por ejemplo para transmitir voz se necesitan 64 Kbps.

1.8.3.2. Video

Tráfico que no admite retardos, ni adelantos (Isócrono). Admite pérdidas de pequeños pedazos de información. Ocupa un ancho de banda variable, mucho mayor que el de voz; se reduce algo si se utiliza algún tipo de compresión de video.

1.8.3.3. Datos

Tráfico que admite retardos o adelantos. No admite pérdidas de la información, ni alteración de la misma. Ocupa un ancho de banda variable; por ráfagas, en ocasiones hay mucho tráfico y en otras nada.

1.8.4. De acuerdo a su Cobertura Geográfica

1.8.4.1. PAN (Red de Área Personal)

Son redes que cubren las necesidades de comunicación personal que pueda tener un individiuo dentro de su hogar o dentro de su ambiente de trabajo (oficina, fábrica, etc). Interconectan dispositivos de comunicación de voz, datos, video, sensores, alarmas, etc. Generalmente se refieren al uso de tecnologías inalámbricas para transmisión de señales.

1.8.4.2. LAN (Red de Área Local)

Es un sistema de interconexión de equipos informáticos basado en líneas de alta velocidad (decenas, cientos o miles de megabits por segundo) y que suele abarcar, como mucho, un edificio o un campus. Son aquellas diseñadas en el ámbito de una empresa u organización para satisfacer sus necesidades internas. Sin embargo, las mismas pueden estar conectadas a la red pública de telecomunicaciones.

Este tipo de red es operada por personal de la misma organización a la que presta sus servicios.

1.8.4.3. MAN (Red de Área Metropolitana)

Es un sistema de interconexión de equipos informáticos distribuidos en una zona que abarca diversos edificios, por medios pertenecientes a la misma organización propietaria de los equipos.

Habitualmente, este tipo de redes se utiliza para interconectar redes de área local.
Redes Urbanas: son aquellas que cubren las necesidades geográficas de un pueblo, una ciudad o un área densamente poblada que incluye a varias ciudades. Son operadas por organizaciones técnicas especializadas. Se caracterizan por tener una tarifa única para cada servicio y para toda el área, independientemente de la ubicación de los usuarios (distancia geográfica), a condición de que estén dentro del área considerada.

Redes Interurbanas: son aquellas que enlazan a dos o más ciudades o áreas urbanas diferentes. Normalmente, en el servicio telefónico los servicios interurbanos se tarifan en función de la distancia existente entre los usuarios intercomunicados.

1.8.4.4. WAN (Red de Área Amplia)

Es un sistema de interconexión de equipos informáticos geográficamente dispersos, incluso en continentes distintos. Las líneas utilizadas para realizar esta interconexión suelen ser parte de las redes públicas de transmisión de datos.

Son aquellas que interconectan a usuarios en países diferentes. Estos vínculos que enlazan a las redes de cada país son mayoritariamente enlaces satelitales a través de cables submarinos, a excepción de los enlaces denominados fronterizos (que unen dos países que tienen fronteras comunes), que en general, usan radioenlaces de microondas o cables (terrestres o submarinos).

Estas redes tienen como principio de tarifación, acuerdos entre las administraciones de los distintos países, basadas en los medios técnicos usados en cada Estado y en las conveniencias comerciales en cada uno de ellos.

1.8.4.5. SAN (Red de Área de Almacenamiento)

Se refieren a las redes utilizadas en el almacenamiento de grandes bases de datos, cuando estos tienen que distribuirse en distintos servidores, en distintas bases de datos, dentro de una locación. Generalmente los equipos constituyen "clusters" donde grandes volúmenes de datos fluyen entre equipos de gran capacidad de procesamiento y/o de almacenamiento.

1.9. Estructura de una red de computadoras

1.9.1. Estructura de una LAN

Las **Redes de Área Local (LANs [2])** son redes de propiedad privada dentro de un solo edificio o campus de hasta unos cientos de metros de extensión. Se usan ampliamente para conectar computadoras personales y estaciones de trabajo con objeto de compartir recursos (por ejemplo, impresoras) e intercambiar información. Se distingue de otro tipo de redes por tres características: **(1)** su tamaño, **(2)** su tecnología de transmisión, **(3)** su topología y **(4)** su administración.

Están restringidas en tamaño, lo cual significa que el tiempo de transmisión del peor caso está limitado y se conoce de antemano. Conocer este límite hace posible usar ciertos tipos de diseños que de otra manera no serían prácticos, y también simplifica la administración de la red.

A menudo usan una tecnología de transmisión que consiste en un cable específico al cual están conectadas todas las máquinas. Las LANs tradicionales operan a velocidades de 10 a 100 Mbps, tienen bajo retardo (décimas de milisegundos) y experimentan muy pocos errores. Las más nuevas pueden operar a velocidades muy altas, del orden de los Gigabit /seg. (Un Gigabit es 1.000 Mbps).

Las LANs están relacionadas con canales de acceso múltiples (son Redes de Difusión). Como el medio físico de comunicación es propio de la organización, el ancho de banda del mismo no significa un precioso recurso como lo es en las grandes redes. El cable de la LAN es muy fiable, su tasa de error es inferior al obtenido en una WAN.

Componentes:

- Sistema Operativo de Red (***NOS***[3]).
- Protocolo de Comunicaciones
- Servidor: dedicado, no dedicado.
- Estaciones de trabajo.
- Recursos para compartir (dispositivos de seguridad, de almacenamiento, de impresión, etc).
- Medios de conexión (sistema de cableado).
- Placas de red.
- Elementos de interconexión y/o segmentación.
- Políticas de administración
- Políticas de seguridad

[2] En Inglés: Local Area Network.
[3] En Inglés: Network Operating System.

Entre los protocolos más utilizados para la transmisión de datos en estas redes, están:

- CSMA/CD: desarrollado por Xerox para sus redes LAN-Ethernet. Este protocolo, aunque con algunas pequeñas variantes, se ha transformado hoy en día en un estándar de facto en el mundo de las redes de computadoras
- TOKEN RING: desarrollado por IBM, y que presenta alta fiabilidad y capacidad de servicio.
- FDDI: utilizado para redes de Fibra Óptica en un doble anillo.
- CSMA/CA: protocolo utilizado por las redes inalámbricas (WLAN)

1.9.2. Estructura de una WAN

Las **Redes de Área Amplia (WAN[4]s)** se extienden sobre un área geográfica extensa, a veces un país o un continente. Cuando una red necesita establecer contacto con máquinas que se usan en localidades remotas (otra ciudad, otro país o incluso otro continente) sería prácticamente imposible colocar un cable que conectara físicamente todos los elementos de la red; así que hay que recurrir a medios de comunicación más complejos como enlaces vía microondas o incluso transmisiones vía satélite. En estos casos se tiene una red WAN. En su mayoría utilizan enlaces punto a punto.

Una red de este tipo contiene una colección de máquinas dedicadas a ejecutar programas de usuario (de aplicación). Estas máquinas (***hosts***) están conectadas por una **subred** de comunicación. El trabajo de la subred es conducir mensajes de un *host* a otro.

En muchas de estas redes, la subred tiene dos componentes distintos: las **líneas de transmisión** y los **elementos de conmutación**. Las primeras (también llamadas circuitos, canales o troncales) mueven bits de una máquina a otra. Los elementos de conmutación son computadoras especializadas que conectan dos o tres líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación debe escoger una línea de salida para reenviarlos. No hay una tecnología estándar para designar estas computadoras; se les denomina **nodos conmutadores de paquetes, sistemas intermedios** y **centrales de conmutación de datos**. Como término genérico para las computadoras de conmutación, se utiliza la palabra **enrutador**. Cada *host* generalmente está conectado a una LAN en la cual está presente un enrutador, aunque en algunos casos un *host* puede estar conectado directamente a un enrutador.

En casi todas las WANs, la red contiene numerosos cables o líneas de telecomunicaciones de largas distancias y gran ancho de banda, cada uno conectado a un par de enrutadores. Si dos enrutadores que no comparten un cable desean comunicarse, deberán hacerlo indirectamente, por medio de otros enrutadores. Cuando se envía un paquete de un enrutador a otro a través de uno o más enrutadores intermedios, el paquete se recibe completo en cada enrutador intermedio, se almacena hasta que la línea de salida requerida está libre, y a continuación se reenvía. Una subred basada en este principio se llama, de **punto a punto**, de **almacenar y reenviar**, o de **paquete conmutado**. Casi todas las redes de área amplia (excepto aquellas que usan satélites) tienen subredes de almacenar y reenviar.

[4] En Inglés: Wide Area Network.

Una segunda posibilidad para una WAN es un sistema de satélite o de radio en tierra. Cada enrutador tiene una antena por medio de la cual puede enviar y recibir. Por su naturaleza, las redes de satélite son de difusión y son más útiles cuando la propiedad de difusión es necesaria.

Componentes:

- **Nodo:** en una red de datos, es el punto donde una o varias unidades funcionales se conectan a líneas de transmisión de datos (enlaces). Es el centro de conmutación o de tránsito de una red de telecomunicaciones. Es el punto de conexión física de dispositivos en una WAN.
- **Host:** Todo dispositivo que posea facilidades de comunicaciones para llevar a cabo el intercambio de información y que pueda ser individualizado dentro de la red (mediante una dirección única).
- **Terminal:** equipo situado en las cercanías inmediatas del usuario, que presenta a éste la información recibida de la red en forma inteligible.
- **Interfaz:** punto en donde el terminal se conecta a la red.
- **Enlace:** es el conjunto de medios de comunicaciones que permiten establecer uno o más canales de transmisión entre dos puntos de una red. Se denomina "enlace troncal" al que une dos nodos y "enlace de usuario" al que une un nodo con un equipo terminal.

1.10. Topologías de Redes

La topología es la forma de interconectar las estaciones de una red. Este concepto se aplica a la instalación de redes para analizar la mejor forma de distribuir los componentes dentro de una habitación, edificio o conjunto de edificios. De ésta depende en buena medida, tanto la operación como el mantenimiento de la red; las posibilidades de expansión por agregados de nuevos nodos; las características de la implementación física necesaria en los puntos de conexión entre la estación y el medio de transmisión; y la facilidad de detección de nodos en fallas, así como su aislamiento del resto del sistema.

Existen dos tipos de topologías: la **física** y la **lógica**.

La primera es la descripción del camino seguido por la señal en los cables de la red para enlazar los nodos. Describe donde está cada nodo de la red en relación al resto de los nodos y muestra la configuración general.

La segunda describe cómo fluyen los mensajes por las estaciones, es decir, cómo se transmite la información por la red. Su función es determinar, entre otras cosas, el formato del paquete; cuánta información llevará el paquete y el método de seguimiento del mismo a través de la red.

1.10.1. Topologías Físicas

Entre las topologías físicas se tiene:

1.10.1.1. Bus

Es un diseño simple con un solo tramo de cable como bus o tronco que es compartido por todos los dispositivos de la red. (Ver **figura 1.4**) Consta de un único cable que se extiende de una computadora a la siguiente en modo serie al que se conectan las computadoras; los extremos del cable se terminan con una resistencia.

Cualquier computadora conectada puede enviar señales por el cable y todas las demás la recibirán. Debido a que todas las computadoras conectadas al cable pueden detectar señales eléctricas, cualquiera de ellas puede transmitir datos a otra, porque un nodo no depende del siguiente para que el flujo de información continúe (a diferencia del anillo). Las computadoras conectadas deben coordinarse para asegurarse que sólo una computadora envíe señales a la vez. Los equipos conectados al bus, no toman decisiones sobre enrutamiento o encaminamiento, la responsabilidad de la administración de la red recae en cada nodo a través del protocolo de comunicaciones.

Este tipo de topología fue la más usada en las LANs, hasta que fue desplazada por la de estrella.

No tiene controlador central; cuenta con dispositivos transceptores en cada punto de conexión con el bus, adoptando una configuración que se denomina transmisión **multipunto**.

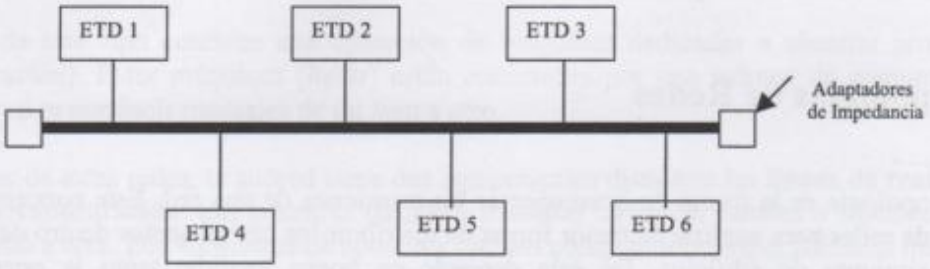


FIGURA 1.4: Red con topología Bus.

Ventajas:

- Aumenta notablemente la confiabilidad del sistema, dado que el medio es pasivo totalmente.
- Sencillez.

Desventajas:

- El precio que se debe pagar es que cada nodo debe transmitir, recibir y resolver problemas relativos a la colisión de mensajes.
- Como los transceptores no actúan como regeneradores de la señal (como ocurre en el anillo), a medida que el mensaje recorre el medio alejándose de la estación transmisora se produce una degradación de las señales eléctricas y en consecuencia habrá una longitud máxima admisible para el medio de transmisión.
- Imposibilidad de insertar /extraer estaciones con la red en funcionamiento.

1.10.1.2. Estrella

Es una topología centralizada; está basada en un elemento que actúa como concentrador de todo el tráfico de comunicaciones existente, al que están conectados los equipos terminales correspondientes. (Ver **figura 1.5**) Una topología de este tipo dispone los nodos de tal forma que todas las transmisiones pasan por un dispositivo central. No utiliza cables compartidos, cada dispositivo tiene su propio cable dedicado. Se utilizan *hubs, switchs, access points, etc* para enviar las señales a cada terminal.

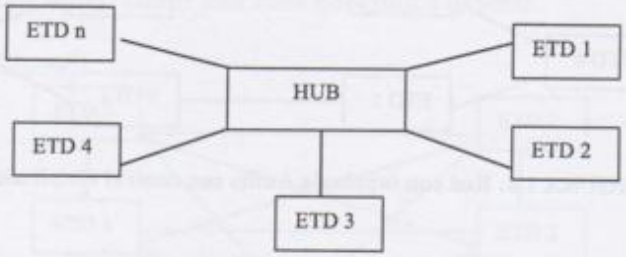


FIGURA 1.5: Red con topología Estrella.

Ventajas:

- Es una estructura de diseño simple.
- Es modular.
- Es escalable.
- Es fácil de aislar un terminal en caso de falla.
- Brinda la posibilidad de insertar /extraer máquinas con facilidad.

Desventajas:

- Mayor costo.
- Si el *hub* deja de funcionar, la red también lo hace y este factor limita en consecuencia la confiabilidad de la red.

1.10.1.3. Anillo

Es una topología distribuida. Una red con esta topología dispone los nodos en un ciclo cerrado, con cada nodo enlazado a los nodos contiguos a la derecha y la izquierda.

Esta topología es poco usada en las LANs.

Será el modo de empleo de la red el que determinará la necesidad de contar con un control central o distribuido.

1.10.1.3.1. Anillo con Control Distribuido

Se organiza de forma tal que cada estación o nodo está conectado sólo a otros dos. (Ver **figura 1.6**) Los datos pasan de un nodo al siguiente, mediante repetidores conectados entre sí secuencialmente con cables u otro medio físico de transmisión, hasta cerrar un círculo. El mensaje que entra en un anillo debe contener la dirección del destinatario y circulará de un terminal a otro, hasta ser reconocida dirección a quien se envía el mensaje.

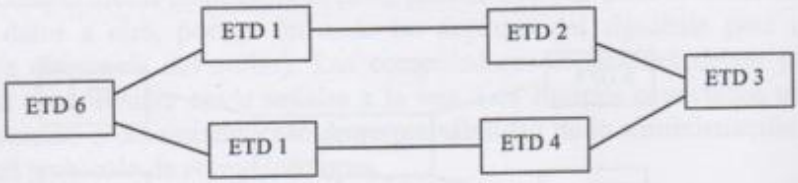


FIGURA 1.6: Red con topología Anillo con control distribuido.

Ventaja:

- Como el control es distribuido, proporciona más flexibilidad y confiabilidad.

Desventajas:

- Si un nodo o elemento de la red se detiene, toda la red podría dejar de funcionar al ser cortada la circulación de los mensajes; sin embargo, se han desarrollado técnicas para evitar esto.

- Puede quedar disminuida la velocidad de la red. Por ejemplo, como los datos tienen un sentido único de circulación, si éstos van hacia la derecha del nodo transmisor y el nodo receptor se encuentra a la izquierda de aquél, el mensaje deberá pasar por toda la red antes de llegar al receptor.

1.10.1.3.2. Anillo con Control Centralizado

Se presenta cuando a uno o dos nodos o estaciones, se le confieren atributos mayores, es decir una mayor jerarquía y por consiguiente el control (centralizado) de las comunicaciones. (Ver **figura 1.7**) Todos los nodos están conectados cerrando un anillo, pero con una estación de control que es la que determina en cada instante qué nodo utilizará el medio de transmisión.

Ventaja y Desventaja: facilidad de control, dado que existe una cierta dependencia del elemento controlador.

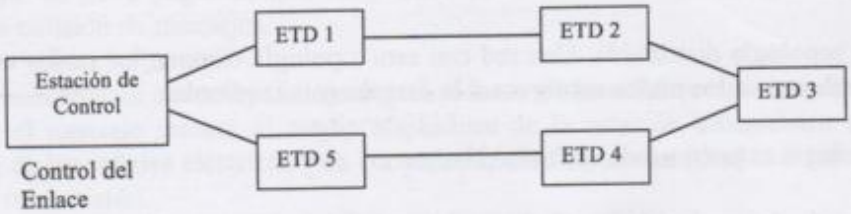


FIGURA 1.7: Red con topología Anillo con control distribuido.

1.10.1.4. Malla

Los nodos están conectados cada uno con todos los demás; están conectados de forma que no existe una preeminencia de un nodo sobre otros, en cuanto a la concentración del tráfico de comunicaciones. (Ver **figuras 1.8** y **1.9**)

En muchos casos, es complementada por enlaces entre nodos no adyacentes, que se instalan para mejorar las características del tráfico. Puede organizarse con equipos terminales solamente (en lugar de nodos), para aquellos casos en que se trate de redes de transmisión de datos. Es especialmente apta para ser usada cuando varios nodos deben cubrir una zona geográfica extensa.

Se utiliza como *backbone*[5].

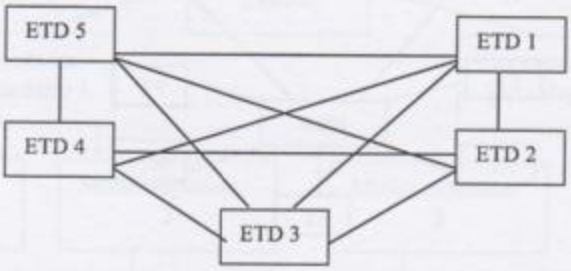


FIGURA 1.8: Red con topología de Malla regular.

Ventajas:

- Son las redes más fiables.
- Permiten en el caso de una interrupción, mantener el enlace usando otro camino con lo cual aumenta significativamente la disponibilidad de los enlaces.
- Por tener redundancia de enlaces, posibilita caminos alternativos para la transmisión de datos y en consecuencia aumenta la confiabilidad de la red.
- Como cada estación está unida a todas las demás existe independencia respecto a la anterior.

Desventajas:

- Este tipo de red es la más cara de implementar debido a la gran cantidad de enlaces.
- Tiene baja eficiencia en las conexiones o enlaces, debido a la existencia de enlaces redundantes.

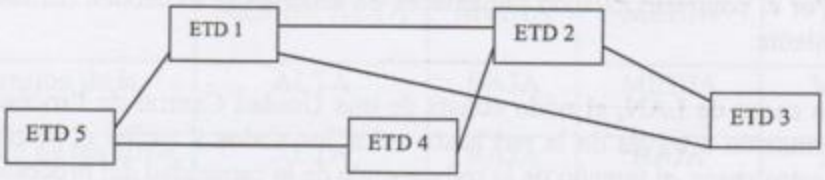
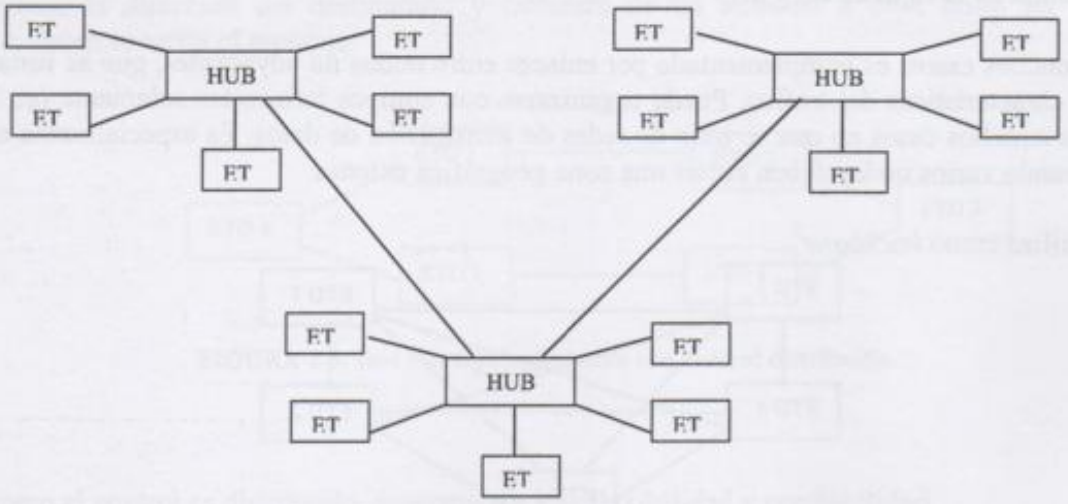


FIGURA 1.9: Red con topología de Malla irregular.

[5] Red principal; instalación de transmisión diseñada para interconectar canales de distribución de baja velocidad o grupos de dispositivos de usuarios dispersos.

1.10.1.5. Estrella Extendida

Es una topología derivada de la estrella. Del nodo central, salen ramas hacia otros nodos que se constituyen a su vez en concentradores de su propia estrella



1.10.1.6. Jerárquica

Es una topología completamente distribuida. Es aquella en la que unos nodos son tributarios de otros de mayor jerarquía. Se tiene como base un equipo de gran soporte, del cual dependen equipos de menor tamaño y equipos terminales. (Ver **figura 1.10**) Representa una red en donde las computadoras alimentan de información a otras computadoras, que a su vez alimentan a otras. Las computadoras que se utilizan como dispositivos remotos pueden tener recursos de procesamiento independiente y recurren a los recursos en niveles superiores e inferiores conforme se requiere información u otros recursos.

En muchos casos y desde el punto de vista exclusivamente topológico, son topologías de características mixtas.

El número de usuarios de cada nodo, dependerá de la disponibilidad que tenga el equipo de conmutación allí situado para manejar equipos terminales.

Es especialmente apta para ser usada cuando los equipos terminales del nodo están ubicados en una zona geográfica concentrada. Se utiliza corrientemente en redes privadas y para las comunicaciones vía satélite. Por el contrario, cuando los enlaces de usuarios se extienden demasiado, esta topología deja de ser conveniente.

En los casos de LAN, el nodo consta de una Unidad Central de Proceso (CPU), que controla el flujo de información a través de la red hasta todos los nodos y recibe el nombre de servidor de la red (Server). En estos casos, el tamaño de la red depende de la capacidad del procesador central.

Esta topología resulta ideal cuando el objetivo consiste en conectar muchos computadores de tipo personal con uno solo, el cual se dedica a controlar los restantes.

En los casos de redes informáticas, los sistemas están basados en un nodo compuesto por un computador central, que está conectado a equipos terminales tradicionales. Estos computadores centrales, actúan como controlador del flujo de información hacia y desde cada dispositivo periférico del sistema.

El computador central interroga selectivamente, en un cierto orden, a cada uno de los dispositivos para determinar si tienen datos para enviar. Solamente cuando éste brinda la autorización, los terminales pueden comenzar a enviar los datos hacia otro terminal o también puede suceder él mismo procese los datos para luego transmitirlos al terminal seleccionado.

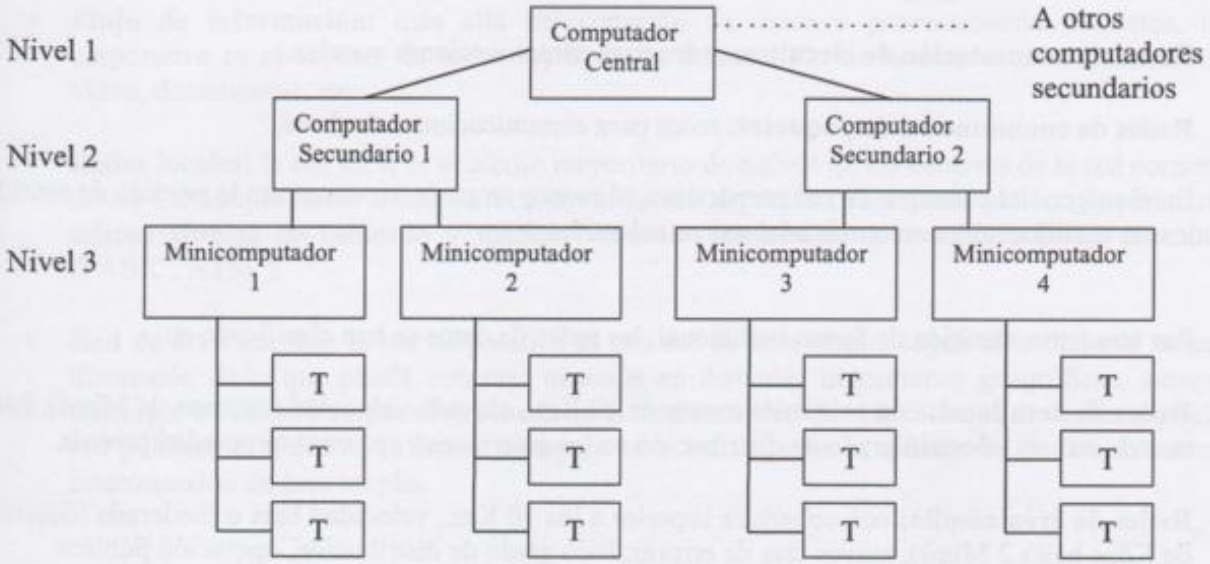


FIGURA 1.10: Red con topología Jerárquica.

1.10.1.7. Cuadro comparativo de las topologías básicas

Características	Estrella	Bus	Anillo	Jerárquica
Número de nodos.	MEDIO /ALTO.	MEDIO	MEDIO	ALTO
Confiabilidad.	MEDIA/ ALTA	MEDIA	MEDIA	ALTA
Facilidad de reconfiguración de la red.	ALTA	BAJA	MEDIA	MEDIA
Facilidad de localización de las fallas.	ALTA	BAJA	BAJA	ALTA
Modularidad	ALTA	MEDIA	BAJA	ALTA

1.11. Red Corporativa

El concepto de red corporativa, como lo vamos a abordar ahora, es relativamente reciente. Este concepto parte de la madurez que en los últimos años han experimentado los distintos tipos de redes de comunicaciones, así como de la capacidad creciente de integración e interoperabilidad entre sistemas hardware y software de proceso y comunicaciones.

Tradicionalmente, las redes de comunicaciones se han clasificado en dos tipos:

- **Redes de conmutación de circuitos:** redes para comunicaciones vocales.
- **Redes de conmutación de paquetes:** redes para comunicaciones de datos.

En el origen del concepto de red corporativa, al menos en parte, se encuentra la pérdida de sentido actual de esta clasificación, como más adelante se aclarará.

Por otra parte, también de forma tradicional, las redes de datos se han clasificado en:

- **Redes de área local:** con cobertura menor de 10 Km., elevada velocidad (decenas de Mbps), baja tasa de errores, elevado grado de distribución en los interfaces y recursos, propiedad privada.
- **Redes de área amplia:** con cobertura superior a los 10 Km., velocidad baja o moderada (decenas de Kbps hasta 2 Mbps), mayor tasa de errores, bajo grado de distribución, operación pública.

De nuevo, debido a los cambios tecnológicos que se han producido tanto en las tradicionalmente conocidas redes locales y redes de área amplia, esta clasificación ha quedado obsoleta, dando lugar a la introducción de una clasificación más realista de las redes en:

- **Redes corporativas:** privadas.
- **Redes públicas:** gestionadas por un operador de red que ofrece servicios públicos de conectividad y transporte de información.

Después de esta pequeña introducción podríamos definir una **red corporativa** como el ***"sistema de comunicaciones y proceso que soporta todo el flujo de información de un grupo de interés o corporación".*** Una red corporativa integrará tanto a las tradicionales redes locales, como a las redes de área amplia, mediante un nuevo concepto: la **interconexión de las redes locales** mediante **servicios de red pública** de tal forma que para el usuario sea transparente, a la hora de acceder a los distintos recursos de la red, la existencia de una red de área amplia, ya que la red corporativa le presenta un interfaz uniforme independientemente de su ubicación.

Analicemos algunos conceptos manejados en las anteriores definiciones:

- **Sistema de comunicaciones:** sin distinguir entre comunicaciones de voz (tradicionalmente soportadas por redes de conmutación de circuitos) y comunicaciones de datos (redes de conmutación de paquetes), porque en la red corporativa se integran ambas.

- **Relación entre proceso y comunicaciones:** ambos conceptos no se pueden manejar de forma separada, porque por una parte los sistemas de comunicaciones actuales tienen una elevada capacidad de proceso, y por otra los elementos de procesos tradicionales (proceso de datos) dependen en gran medida de las comunicaciones, ya que éstas forman parte íntegra del proceso (arquitecturas y aplicaciones *cliente /servidor*).

- **Flujo de información:** más allá del concepto de datos o procesamiento de datos, la red corporativa es el soporte de todos los tipos de información de la corporación: datos, fax, voz, vídeo, documentos, etc.

- **Redes locales:** la red local es el medio mayoritario de acceso de los usuarios de la red corporativa, de tal forma que tanto la red de voz como la red de datos (tradicional red local) comparten el mismo sistema de cableado y muchas veces los elementos de interconexión y conmutación (PABX[6], ATM[7]).

- **Red de área amplia:** la red corporativa es una red de área amplia según el tradicional criterio de dimensión dado que puede conectar usuarios en distantes ubicaciones geográficas, aunque sin embargo, en una red corporativa basada en la interconexión de redes locales mediante servicios de red pública, el objetivo es hacer transparente a los usuarios la existencia de una estructura de interconexión de área amplia.

Un concepto asociado al de red corporativa sería el de **red privada virtual**. Una red privada virtual puede definirse como un tipo de red corporativa, en el que todos los servicios de comunicación de voz y de datos de un usuario son proporcionados por un operador público de interfaz y facturación única. Dicho de otra forma, parte de la red pública es asignada al usuario privado para que haga uso de ella como si **"virtualmente fuera suya"**, aunque la gestión de la misma la realiza el operador público. La ventaja para el cliente es que existe un único punto de facturación y la gestión de las comunicaciones de área amplia se simplifican totalmente porque se deja al operador.

Las redes privadas virtuales ofrecen en general servicios basados en conmutación de circuitos, aptos de forma directa para voz mediante la interconexión de las centralitas de usuario, y que requieren ciertos equipos de adaptación para su utilización por parte del tráfico de datos. En una primera instancia *routers* y de forma avanzada conmutadores y conmutadores ATM. La situación ideal, sólo apta para grandes corporaciones es que el equipo de interfaz entre la red pública y la parte local de la red corporativa sea un conmutador ATM que distribuya tanto los servicios de voz y de datos.

La red corporativa trasciende el concepto tan arraigado de diferenciar el departamento o los servicios de informática de los servicios de telecomunicación de una empresa o entidad. Ambos servicios se deben abordar de forma conjunta y única, con los siguientes objetivos:

---

[6] Centralita privada automática; central telefónica automática de propiedad del usuario, que acomoda la transmisión de llamadas desde y hacia la red telefónica pública.

[7] Modo de transferencia asíncrono.

- Reducción de costos.
- Facilidad de gestión.
- Incremento de la productividad.

Por tanto, el concepto clave para el diseño y gestión de una red corporativa será el de integración: integración de equipos, integración de servicios, integración de aplicaciones e integración de personal técnico.

La red corporativa debe entenderse como una red abierta:

- Formada por elementos independientes del fabricante, con el objetivo de máxima interoperabilidad entre todos los componentes de la red.
- Elementos propios, de tipo abierto y estándar como redes locales, conmutadores, *routers*, centralitas, etc.
- Utilización de servicios públicos (por definición estándar) como líneas alquiladas, RDSI[8], servicios Frame Relay[9], etc.

[8] Red Digital de Servicios Integrados: es un estándar del CCITT para una red que acomoda una variedad de servicios de transmisión digital. En Inglés: ISDN (Integrtated Services Digital Network).
[9] Protocolo de transmisión de paquetes de datos en ráfagas de alta velocidad a través de una red digital.

1.12. Estandarización de redes

Desde hace tiempo los diferentes sectores de la industria, y entre ellos el sector de las telecomunicaciones, han aceptado los estándares como algo necesario para definir las características físicas, mecánicas y de procedimiento de los diferentes equipos y sistemas de telecomunicaciones.

En los siguientes puntos se estudiarán diferentes aspectos relacionados con el tema de la estandarización. En concreto se planteará su necesidad y aspectos relativos a la misma, como por ejemplo los organismos de estandarización, tipos y jurisdicción de los estándares.

1.12.1. Necesidad de la estandarización

La estandarización se hace necesaria desde el mismo momento en que diferentes fabricantes diseñan e implementan equipos que están destinados a realizar las mismas funciones o a interconectarse entre ellos. Tanto los fabricantes como los proveedores de servicios tienen sus propias ideas de cómo llevar a cabo dichas funciones; sin embargo debe existir una cierta coordinación con la finalidad de que la industria de las comunicaciones no se convierta en un caos.

En el pasado los fabricantes de computadores no suscribieron esta política, mientras que los productores de equipos de comunicaciones sí reconocieron la necesidad de facilitar la interconexión y la comunicación con los equipos de otros fabricantes. En el primer caso el objetivo perseguido por los fabricantes de computadores era el de monopolizar sus clientes haciéndoles dependientes de la tecnología, de forma que no pudieran acudir a otros fabricantes. Al aumentar el número de computadores existentes así como de las redes de computadores, dicha situación se convirtió en insostenible y la coordinación, antes reclamada, se hizo necesaria.

La estandarización proporciona una serie de ventajas, entre las que se pueden destacar:

- Asegura un gran mercado para los productos que lo cumplan.
- Potencia la producción masiva, permitiendo de esta manera reducir costos en la fabricación.
- Permite que productos de diferentes suministradores se puedan comunicar entre sí.
- Da una mayor libertad y flexibilidad al usuario que debe seleccionar y adquirir un determinado equipo.
- Protege la inversión del comprador de un equipo de telecomunicaciones

Sin embargo, junto a las características mencionadas anteriormente, se pueden citar los siguientes inconvenientes:

- Los estándares tienden a "congelar" la tecnología, ya que mientras un determinado organismo desarrolla y redacta el documento que avale a un estándar, se habrán desarrollado, posiblemente, técnicas y equipos más eficaces.

- Existen muchos estándares diferentes para realizar las mismas tareas y funciones, ya que existen multitud de organismos de estandarización. Sin embargo, poco a poco la colaboración y coordinación entre ellas va aumentando.

1.12.2. Tipos de Estándares existentes

Las diferentes normas, recomendaciones o estándares han aparecido de diferente forma y por diferentes motivos. Además no todos ellos tienen la misma validez, ni ámbito de aplicabilidad, por ello hay que distinguir:

1.12.2.1. Estándares de Facto

Se caracterizan porque su aparición viene determinada por la cumbre y el uso, y en ningún caso debido a un plan formal. En el campo de las comunicaciones, los dos ejemplos más claros son: el sistema operativo UNIX y el ordenador personal (PC). El primero como un estándar para las estaciones de trabajo, inicialmente en las universidades, y que posteriormente pasó a utilizarse en los entornos empresariales; y el segundo, debido a que una gran cantidad de empresas dedicadas a la fabricación de ordenadores decidieron construir equipos idénticos a los de IBM.

1.12.2.2. Estándares de Jure

Al contrario que los anteriores, sí vienen avalados por alguna entidad u organismo formal o legal que tiene algún tipo de autoridad en el campo de las comunicaciones. Dentro de este tipo de estándares podemos distinguir los de **obligado cumplimiento**, que son emitidos por organismos de estandarización nacidos de acuerdos entre estados, por ejemplo la Unión Internacional de Telecomunicaciones (ITU), y los de **no obligado cumplimiento**, que por el contrario, son emitidos por algún tipo de organización de tipo voluntario, siendo uno de los ejemplos más claros, la organización denominada *International Electrical and Electronics Engineers* (IEEE). Este último tipo de estándares suele tener gran impacto, ya que por lo general los miembros de estos organismos son profesionales del sector de reconocido prestigio.

1.12.3. Quién es quién en el mundo de las Telecomunicaciones

La situación legal de las compañías telefónicas de todo el mundo varía considerablemente de un país a otro. En un extremo está Estados Unidos, con 1500 compañías telefónicas privadas. Antes de que la AT&T se dividiera en 1984 era la corporación más grande del mundo y dominaba completamente la escena; proporcionaba servicio telefónico a cerca del 80% de los teléfonos instalados en Estados Unidos, distribuidos en la mitad de su área geográfica, y todas las demás compañías combinadas daban servicio a los clientes restantes (en su mayoría rurales). Desde su división, AT&T continúa proporcionando servicio de larga distancia, aunque ahora en competencia con otras compañías. Las siete compañías operadoras Bell regionales que se separaron de AT&T y 1500 independientes proporcionan servicio telefónico local y celular. Algunas de estas compañías independientes, como GTE, son muy grandes.

Las compañías estadounidenses, que proporcionan servicios de comunicación al público se llaman **portadoras comunes**. Los precios y servicios de estas empresas están descriptos en un documento llamado **tarifa**, el cual debe ser aprobado por la Comisión Federal de Comunicaciones para el tráfico interestatal e internacional, y por las comisiones de servicios públicos para el tráfico intraestatal.

En el otro extremo se encontraban los países en los que el gobierno nacional tenía un monopolio completo de todas las comunicaciones, incluidos el correo, el telégrafo, el teléfono, y frecuentemente también la radio y la televisión. La mayor parte del mundo pertenecía a esta categoría. En algunos casos, la autoridad de telecomunicaciones es una compañía nacionalizada; en otros, es simplemente una rama del gobierno, usualmente conocida como la PTT (Administración de Correo, Telégrafo y Teléfono.) La tendencia mundial es hacia la liberación y competencia, alejándose del monopolio gubernamental.

Con todos estos proveedores de servicios diferentes, existe una clara necesidad de lograr la compatibilidad a escala mundial para asegurar que las personas (y las computadoras) de un país puedan llamar a sus homólogos en algún otro. En realidad, esta necesidad ha existido desde hace mucho tiempo. En 1865, representantes de muchos gobiernos europeos se reunieron para formar el predecesor de la actual ITU, llamado CCITT (Comité Consultivo Internacional de Telegrafía y Telefonía.) La misión de la CCITT fue estandarizar las telecomunicaciones internacionales, lo que en esos días significaba telegrafía. Aun entonces era claro que si una mitad de los países usaba código Morse y la otra usaba algún otro código, se iba a presentar un problema. Cuando el teléfono se convirtió en un servicio internacional, la ITU emprendió la tarea de estandarizar también la telefonía. En 1947 la ITU llegó a ser una agencia de las Naciones Unidas.

La ITU tiene tres sectores principales:

1. Sector de radiocomunicaciones. **(ITU-R)**

2. Sector de estandarización de telecomunicaciones. **(ITU-T)**

3. Sector de desarrollo. **(ITU-D)**

La **ITU-R** se ocupa de la asignación de frecuencias de radio en todo el mundo a los grupos de interés en competencia. A nosotros nos concierne principalmente la ITU-T, que está relacionada con los sistemas telefónicos y de comunicación de datos. De 1956 a 1993, la ITU-T fue conocida como CCITT por las iniciales de su nombre en francés: *Comité Consultatif International Télégraphique et Téléphonique*. El 1° de Marzo de 1993 se reorganizó el CCITT para hacerlo menos burocrático y cambió de nombre para reflejar su nuevo papel. Tanto la ITU-T como el CCITT emitieron recomendaciones en el área de las comunicaciones telefónicas y de datos. Entre las recomendaciones del CCITT hay una que todavía está en uso; tal es la X.25 de CCITT, aunque desde 1993 las recomendaciones llevan la etiqueta ITU-T.

La **ITU-T** tiene cinco clases de miembros:

1. Administraciones (PTT nacionales).

2. Operadores privados reconocidos (por ejemplo, AT&T, MCI, British Telecom).

3. Organizaciones regionales de telecomunicaciones (por ejemplo, la ETSI europea).

4. Organizaciones comerciales y científicas de telecomunicaciones.

5. Otras organizaciones interesadas (por ejemplo, redes bancarias y de aerolíneas).

La ITU-T tiene cerca de 200 administraciones, 100 operadores privados y varios cientos de miembros más. Únicamente las administraciones pueden votar, pero todos los miembros pueden participar en el trabajo de la ITU-T. Como Estados Unidos no tiene una PTT, alguien más tiene que representarlo en la ITU-T. Esta tarea recayó en el Departamento de Estado, probablemente con la excusa de que ITU-T tenía que ver con países extranjeros, la especialidad del Departamento de Estado.

La tarea de la ITU-T es hacer recomendaciones técnicas acerca de las interfaces de telefonía, telegrafía y comunicación de datos. A menudo estos estándares lograron reconocimiento internacional; por ejemplo, las recomendaciones de la serie V.xx para módem, que especifica la normativa para la interconexión de los terminales DTE con terminales DCE (módems).

Cabe señalar que las recomendaciones de la ITU-T técnicamente sólo son sugerencias que los gobiernos pueden adoptar o ignorar, según lo deseen. En la práctica, un país que desee adoptar un estándar telefónico distinto al del resto del mundo es libre de hacerlo, pero a expensas de aislarse de todos los demás. Esto podría funcionar en Albania, pero en cualquier otro lugar sería un problema real. La ficción de llamar a los estándares de la ITU-T "recomendaciones" fue y es necesaria para mantener apaciguadas a las fuerzas nacionalistas en muchos países.

El trabajo real de la ITU-T se realiza en grupos de estudio, que frecuentemente llegan a incluir 400 personas. Los grupos de estudio se dividen en partidas de trabajo, las cuales a su vez se dividen en equipos de expertos, los que se subdividen en grupos *ad hoc*.

1.12.4. Quién es quién en el mundo de los Estándares Internacionales

La mayoría de los estándares internacionales son producidos por la ISO (Organización Internacional de Estándares), una organización voluntaria, no surgida de un tratado, fundada en 1946.

Esta emite estándares internacionales a nivel mundial en prácticamente cualquier ámbito científico y tecnológico, industrial (infraestructuras, ciencias, seguridad y entorno, electrónica, tecnología de la información, telecomunicaciones, agricultura, tecnología de materias, construcción, tecnologías especiales... también, es la encargada de publicar los números ISBN - International Standard Book Number). Coopera con el IEC e ITU en el ámbito de las telecomunicaciones y el proceso de la información.

Entre sus miembros están los organismos de estandarización nacionales como:

ANSI American National Standards Institute Estados Unidos
DIN Deutsches Institut fuer Normung Alemania
BSI British Standards Institution Reino Unido
AFNOR Association Francaise de Normalisation Francia
UNI Ente Nazionale Italiano de Unificatione Italia
NNI Nederlands Normalisatie-Instituut Países Bajos
SAA Standards Australia Australia
SANZ Standards Association of New Zealand Nueva Zelanda
NSF Norges Standardiseringsforbund Noruega
DS Dansk Standard Dinamarca
AENOR Asociación Española de Normalización España

El peso de cada miembro depende de indicadores económicos como el PIB (producto interior bruto) y el valor de las exportaciones e importaciones, esto es un dato a tener en cuenta, ya que nos está diciendo que son los países ricos los que realmente imponen sus reglas.

La organización interna del ISO dada la cantidad de ámbitos que trata está formada por los cerca de 200 TCs (Technical Committees), cerca de 600 Subcomités (SC) y 2100 grupos de trabajo (Working Groups), estos comités se llaman por orden de creación así el TC 97 se encarga del procesado de información y el SC 16 es el encargado de llevar OSI (Open System Interconection).

El proceso de creación de un estándar ISO es como sigue. Uno de sus miembros, por ejemplo, una organización nacional de estándares, propone la creación de un estándar internacional en un área concreta. En ese momento la ISO crea un nuevo grupo de trabajo que se encarga de desarrollar el primer borrador llamado CD (Committee Draft, borrador del comité). El CD se distribuye al resto de miembros de la ISO, y en un periodo de 6 meses han de dar su opinión, mejoras, críticas sobre el CD. A continuación, se modifica de acuerdo a las modificaciones solicitadas y se somete a votación, si es aprobado entonces el documento pasa a ser un DIS (Draft Internacional Standard) que se difunde de nuevo para recibir comentarios, se modifica y se vota nuevamente. En base a los resultados de esta votación se prepara, aprueba y publica el texto final del IS (International Standard). En áreas muy polémicas un CD o un DIS ha de superar varias versiones antes de conseguir votos suficientes, y el proceso entero puede llevar años.

La ISO ha publicado más de 10.000 estándares algunos de ellos muy famosos como las especificaciones Joliet (estándar de grabación de CDs), ISO 8571 (FTAM), X.21, X.25, X.500, ISO 7498 (OSI Reference Model), las normas de calidad ISO 9000, etc.

En colaboración con el ISO también tenemos al IEC (Comité Electrotécnico Internacional) que desarrollan estándares conjuntos. En el IEC también está organizado en comités (JTC) y subcomités (SC). Desde el punto de vista de las telecomunicaciones el más importante es el JTC-1/SC-6 que ha desarrollado estándares como el ISO/IEC 8824-ASN.1, ISO/IEC 9595[-1-9] (Sistema Directorio) o el ISO/IEC 10021[1-10] (Sistema de mensajería MHS).

En cuestiones de estándares de telecomunicaciones, la ISO y la UIT-T a menudo cooperan para evitar la ironía de tener dos estándares internacionales oficiales y mutuamente incompatibles (la ISO es un miembro de la UIT-T.)

El representante en Estados Unidos de la ISO es el ANSI (Instituto Nacional Estadounidense de Estándares), el cual, a pesar de su nombre, es una organización privada, no gubernamental y no lucrativa. Sus miembros son fabricantes, empresas de telecomunicaciones y otros particulares interesados. La ISO a menudo adopta los estándares ANSI como estándares internacionales.

Otro protagonista importante en el mundo de los estándares es el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), la organización profesional más grande del mundo. Además de publicar revistas y organizar numerosas conferencias cada año, el IEEE tiene un grupo de estandarización que elabora estándares en las áreas de ingeniería eléctrica y computación. el estándar 802 del IEEE para redes de área local es el estándar clave para las LAN, y posteriormente fue adoptado por la ISO como base para el estándar ISO 8802. Los desarrollaremos en profundidad en la unidad 2.

1.12.5. Quién es quién en el mundo de los Estándares de Internet

El amplio mundo de la Internet tiene sus propios mecanismos de estandarización, muy diferentes de los de la ITU-T y la ISO. La diferencia puede resumirse en forma burda diciendo que la gente que asiste a las juntas de estandarización de la ITU o de la ISO usa traje. La gente que asiste a las juntas de estandarización de la Internet usa ya sea jeans o uniformes militares.

Las reuniones de la ITU-T y la ISO están pobladas por oficiales corporativos y burócratas para quienes la estandarización es su trabajo. Ellos consideran la estandarización como algo positivo y dedican sus vidas a ella. Por otro lado, la gente de Internet definitivamente prefiere la anarquía por cuestiones de principios, pero sabe que algunas veces se necesitan acuerdos para lograr que las cosas funcionen. Así pues, los estándares, aunque no debieran existir, son ocasionalmente necesarios.

Cuando se inició la ARPANET, el DoD (Departamento de Defensa) creó un comité informal para supervisarla. En 1983, el comité fue bautizado como IAB (Consejo de Actividades de Internet) y se encomendó la misión un poco más amplia, a saber, mantener a los investigadores que trabajaban con la ARPANET y la Internet apuntando más o menos en la misma dirección. El significado del acrónimo "IAB" se cambió más tarde a Consejo de Arquitectura de Internet.

Cada uno de los aproximadamente 10 miembros del IAB encabezó una fuerza de trabajo sobre algún aspecto de importancia. El IAB se reunía varias veces al año para comentar resultados y realimentar al DoD y a la NSF, quienes proporcionaban la mayor parte de los fondos en esa época. Cuando se necesitaba un estándar (por ejemplo, un algoritmo de ruteo nuevo), los miembros del IAB lo discutían y después anunciaban el cambio para que los estudiantes graduados, quienes eran el corazón de las labores de creación de software, pudieran implementarlo.

La comunicación era a través de una serie de informes técnicos llamados RFC (*Request for Comments*: Petición de Comentarios.) Los RFC se guardan en línea y pueden ser recuperados por cualquier interesado en ellos. Los RFC están numerados en orden cronológico de creación. Son publicadas periódicamente en servidores públicos de Internet. Los RFCs están publicados en formato ASCII. Deben seguir unas pequeñas reglas, que serán revisadas por el RFC Editor. Básicamente son las siguientes:

58 líneas por página
72 Caracteres de ancho incluidas las cabeceras
No está permitido subrayar ni negrita
1 línea de separación por cada párrafo
Nada de Pies de página, ni notas al pie.
Las Referencias no se han de hacer respecto de la página sino respecto de la sección.

Normalmente, en vez de formatearlo a mano se utiliza una herramienta de Unix llamada nroff.

En teoría, para que un protocolo llegara a ser un estándar, lo único que habría que hacer es publicar un borrador, de forma que se hicieran diversas implementaciones del mismo y basándose en estas experiencias, si cumpliera los requisitos mínimos, redactarlo formalmente. Pero esto no es tan sencillo, primero, por las dificultades de redactar un texto técnico de calidad, los intereses económicos y el llegar a un consenso por parte de la comunidad internauta. Los requisitos técnicos que se le piden a un protocolo son, básicamente, los siguientes: a) Qué sea un proyecto abierto (open), es decir, que haya sido desarrollado mediante listas de correo públicas o similares. b) Qué sea flexible y portable para la mayor cantidad de sistemas posibles y ninguno se vea favorecido. c) Qué haya habido una fase exitosa de

pruebas previa. d) Qué desde el punto de vista técnico sea una solución eficiente al problema planteado. e) Que sea imperecedero en la medida de lo posible

Como se puede observar, antes de que un protocolo llegue a ser un estándar tiene que haber varias implementaciones y ser aceptado por la comunidad internauta, es decir, que se la gente lo use. Los estándares reciben un nombre adicional al del número de RFC, STDxxx, donde xxx es el número de estándar. Se ha incluido una lista de los STD en el apéndice, al final de este documento se pueden encontrar las referencias a los ficheros.

En 1989, la Internet había llegado a ser tan grande que este estilo tan informal ya no funcionaba. Para entonces, muchos proveedores ofrecían ya productos TCP/IP y no los querían cambiar sólo porque 10 investigadores habían tenido una mejor idea. En el verano de 1989, el IAB se reorganizó otra vez. Los investigadores pasaron otra vez a la IRTF (Fuerza de Trabajo de Investigación sobre Internet), la cual se hizo subsidiaria de IAB junto con la IETF[10] (Fuerza de Trabajo de Ingeniería de Internet.).

El IAB se pobló con gente que representaba una gama amplia de organizaciones, no sólo la comunidad de investigación. Inicialmente, el IAB fue un grupo que se perpetuaba a sí mismo, pues sus miembros servían por un término de dos años y los nuevos miembros eran designados por los antiguos. Más tarde fue creada la *Internet Society*, formada por gente interesada en la Internet.

Así, La *Internet Society* es en cierto sentido comparable con la ACM o el IEEE; está gobernada por administradores elegidos por quienes designan a los miembros del IAB.

Lo que se buscaba con esta división era tener al IRTF concentrado en investigaciones a largo plazo, mientras que el IETF se encargaba de los problemas de ingeniería a corto plazo. El IETF se dividió en grupos de trabajo, cada uno con un problema específico por resolver. Los presidentes de estos grupos de trabajo inicialmente se reunían como un comité de conducción para dirigir los trabajos de ingeniería. Los temas del grupo de trabajo incluyen nuevas aplicaciones, información de usuarios, integración de OSI, enrutamiento y direccionamiento, seguridad, administración de redes y estándares. Se llegaron a formar tantos grupos de trabajo (más de 70) que fue necesario agruparlos en áreas, y los presidentes de área formaron el comité de conducción.

Adicionalmente, se adoptó un proceso de estandarización más formal a imagen del de la ISO.

Para convertirse en propuesta de estándar, la idea básica se debe explicar completamente en un RFC y debe generar suficiente interés en la comunidad para justificar su consideración. Para avanzar a la etapa de borrador de estándar, debe existir una implementación operante que haya sido probada concienzudamente por al menos dos sitios independientes durante cuatro meses. Si el IAB se convence de que la idea es buena y el software funciona, puede declarar que el RFC es un estándar de Internet.

Algunos estándares de Internet han llegado a ser estándares del DoD (MIL-STD), volviéndose obligatorios para los proveedores del DoD.

Además debemos decir que las direcciones de Internet son asignadas por INTERNIC[11].

---

[10] http//www.ietf.org

[11] Internet Network Information Center.

1.13. Arquitectura de Redes

Las pilas de protocolos (*suites*) constituyen una jerarquía de diversos protocolos que trabajan en forma conjunta para llevar a cabo la transmisión de datos de un host a otro de la red (o de distintas redes). Se asemejan mucho a la estructura burocrática del estado, donde cada oficina, cada departamento cumple con una función y brinda servicios a otra oficina, donde el trámite sigue su curso.

El problema completo de transmisión de datos se organiza en capas o niveles a fin de reducir la complejidad. Cada capa se construye sobre su predecesora, recibe de esta una unidad de datos y sirve a la siguiente. Su propósito es ofrecer ciertos servicios a las capas superiores, liberándolas del conocimiento detallado de cómo se realiza ese servicio.

El número de capas, el nombre y contenido, varían de una a otra arquitectura de red.

Al conjunto de capas y **protocolos** (acuerdo entre las partes que se comunican sobre cómo va a proceder la comunicación) se los denomina **Arquitectura de Red**.

Ésta deberá contener la información necesaria y suficiente que permita construir el *software* y el *hardware* de cada capa, siguiendo el protocolo apropiado. La capa *n* de una máquina dialoga con la capa *n* de otra.

Desde el punto de vista conceptual, los procesos de la capa *n* conciben su comunicación como si fuera horizontal, usando el protocolo de la capa *n*, aun cuando éstos se comuniquen a través de una interfaz, y no con el otro lado.

1.13.1. Modelo de referencia OSI

Es un modelo que está muy difundido y es aceptado como un estándar internacional basado en una propuesta de ISO (Organización de Estándares Internacionales). Se lo denomina Modelo de Referencia OSI (*Open Systems Interconexion*) o también, Modelo para la Interconexión de Sistemas Abiertos.

Los sistemas relacionados con la información y las comunicaciones han tenido problemas importantes cuando han tratado de interconectarse, es decir cuando equipos de fabricantes distintos han tenido que intercambiar datos entre sí. La solución a este problema es la creación de un marco de referencia en el que se fijen todos los fabricantes a la hora de diseñan sus equipos y dispositivos.

La necesidad de estandarización para favorecer la interconexión, llevó a la aparición de un modelo de referencia. El modelo de referencia fue publicado por ISO y posteriormente adoptado por el CCITT (ITU-T). Los sistemas basados en este modelo de referencia se denominan abiertos, debido a que pueden interconectarse con otros sistemas que estén basados en el mismo modelo de referencia.

Consta de siete capas y los principios aplicados para el establecimiento de las capas fueron los siguientes:

- Una capa se creará en situaciones en donde se necesita un nivel diferente de abstracción.

- Cada capa deberá efectuar una función bien definida.
- La función que realiza cada capa deberá seleccionarse tomando en cuenta la minimización del flujo de información a través de la interfaz.
- El número de capas deberá ser lo suficientemente grande para que funciones diferentes no tengan que estar juntas en la misma capa, y además deberán ser lo suficientemente pequeñas para que su arquitectura no llegue a ser muy complicada.

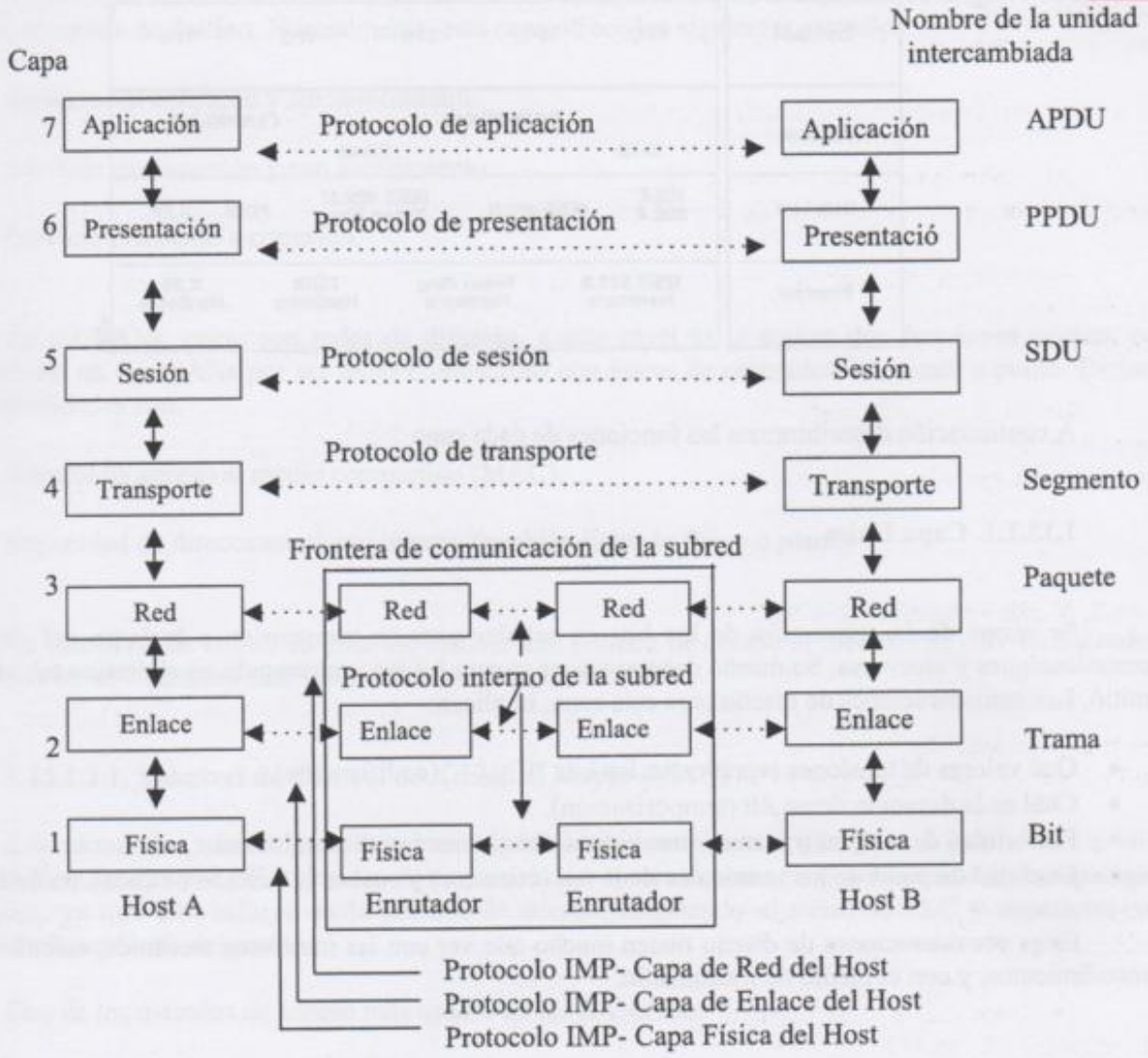
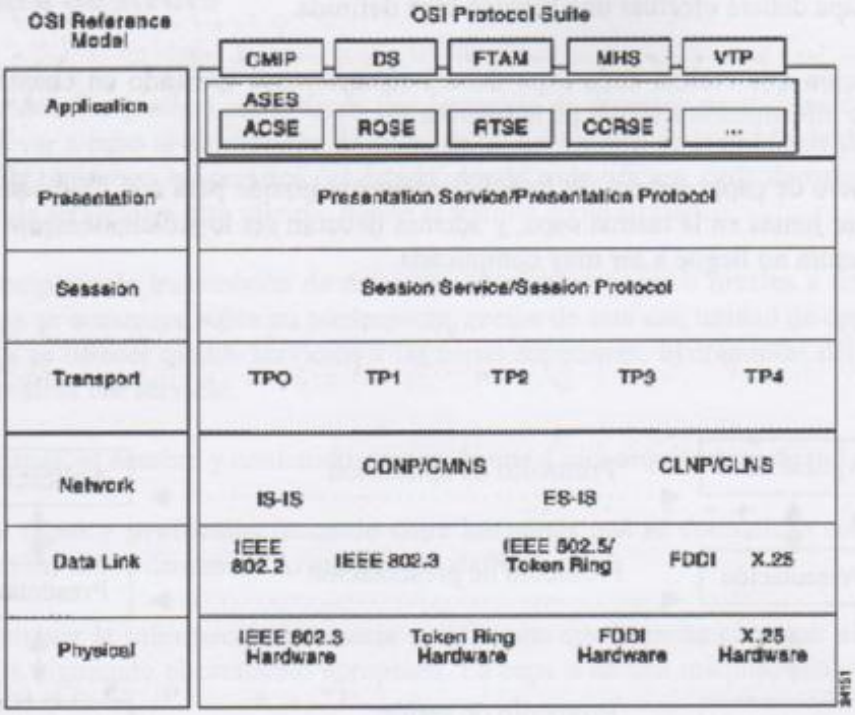


FIGURA 1.17: Capas del Modelo OSI.

Este modelo es una referencia que indica las funciones que debe cumplir cada capa, pero no especifica en forma exacta los servicios y protocolos que se usarían en cada capa en una arquitectura de red determinada. Sin embargo, la ISO ha elaborado normas para todas las capas que se han publicado como estándares (podemos ver algunos de ellos en la siguiente figura):



A continuación describiremos las funciones de cada capa

1.13.1.1. Capa Física

Se ocupa de la conversión de los bits en señales para su transmisión a lo largo del canal de comunicaciones y viceversa. Su diseño debe asegurar que un *bit* sea interpretado en el destino tal como se emitió. Las consideraciones de diseño para esta capa, implican:

- Qué valores de tensiones representan los bits "0"y "1" (codificación).
- Cuál es la duración de un *bit* (temporización).
- Posibilidad de realizar transmisiones bidireccionales en forma simultánea.
- Cantidad de pines de los terminales de la red (conector) y cual es la función de cada uno de ellos.

Estas consideraciones de diseño tienen mucho que ver con las interfaces mecánica, eléctrica y de procedimientos, y con el medio de transmisión.

1.13.1.2. Capa de Enlace

La tarea de esta capa consiste en, a partir de un medio de transmisión común, trasformarlo en una línea sin errores para la capa de red. Esta tarea la realiza trozando los datos en **tramas**, transmitiéndolas en forma secuencial, y procesando las tramas con asentimientos devueltas por el receptor.

Como la capa física transmite un flujo de bits sin tener en cuenta su significado o estructura, recae sobre la capa de enlace la creación y reconocimiento de los límites de la trama. La trama debe poder retransmitirse en caso de destrucción, pero también debe poder distinguirse la duplicación de tramas en el caso de retransmisión por no haberse recibido, por destrucción, del acuse de recibo (ACK).

Un problema que se da, no sólo en esta capa, es la saturación de los canales por diferencia de velocidad entre receptores, para lo cual deben implementarse mecanismos de control de flujo y control de errores. Otro problema a resolver es que en una línea full dúplex, las tramas de asentimiento compiten en el uso de la línea con las tramas de datos.

El principal servicio es el de transferir datos de la capa de red de la máquina de origen a la capa de red de la máquina de destino. Normalmente, esta capa ofrece los siguientes servicios:

- Servicio sin conexión y sin asentimiento.
- Servicio sin conexión y con asentimiento.
- Servicio orientado a conexión.

En las LANs, como son redes de difusión, a este nivel se le suman dos **funciones** nuevas, no consideradas en las WANs por ser redes conmutadas con líneas de comunicación punto a punto. Dichas responsabilidades son:

- Control de acceso al medio compartido (MAC).
- Capacidad de direccionamiento interno (también llamado físico o plano).

En este nivel de enlace se debe especificar una política de acceso al medio. Por ello, en las redes LANs, este nivel 2 (enlace) está subdividido en dos subniveles:

1.13.1.2.1. Subnivel de Control de Acceso al Medio (MAC)

Los protocolos usados para determinar quién sigue en un canal multiacceso pertenecen a este subnivel. Éste facilita al LLC un medio de comunicación aparentemente propio. Depende de la topología del medio, ya que ésta influye en la política de acceso, facilitando al subnivel LLC y superiores un servicio independiente del medio.

Dos de los métodos de acceso más usados en las LANs son:

- El método de acceso **por paso de testigo**.
- El método de acceso **múltiple con detección de actividad**.

1.13.1.2.2. Subnivel de Control de Enlace Lógico (LLC)

Su responsabilidad es transferir la trama (unidad de datos) correspondiente al subnivel de enlace lógico del DTE (equipo terminal de datos) destino con ausencia de error. En caso de recepción errónea del mensaje en destino, se corrige el error con una retransmisión. Es decir que, la capa de red de la máquina transmisora pasa un paquete al LLC usando las primitivas de acceso del LLC. Este subnivel entonces agrega una cabecera LLC que contiene los números de secuencia y acuse.

Este subnivel es independiente del medio físico.

1.13.1.3. Capa de Red

Esta capa se encarga del direccionamiento de los datos: le coloca dirección de origen y de destino de los datos para que estos puedan salir de la red y atravesando distintas redes, lleguen finalmente al destino

Otro punto muy importante en las funciones de esta capa es la determinación de cómo encaminar los mensajes (o paquetes). Las rutas podrían basarse en tablas estáticas que se encuentran cableadas en la red y el cambio no es fácil de realizar. También pueden ser tablas estáticas que se establecen al inicio de cada diálogo. En las redes de difusión, el encaminamiento es simple, por lo tanto esta capa es muy pequeña. Por último, pueden ser de tipo dinámico, determinando la ruta para cada paquete en el momento en que es emitido. El control de congestión, por lo tanto, depende de la capa de red.

La responsabilidad de resolver problemas de interconexión de redes heterogéneas también recae en esta capa.

- La capa de red proporciona servicios a la de transporte.

Cuando la red es operada por un proveedor de servicios portadores, y los *hosts* son operados por los usuarios, el servicio de capa de red se convierte en la interfaz entre el proveedor y los usuarios. Como tal definen las obligaciones y responsabilidades del proveedor y del usuario.

Hay quienes opinan que esta capa debe tener servicio no orientado a conexión. Argumentan que la capa de red sólo debe mover los bits y nada más. Desde este punto de vista, los *hosts* deben aceptar que la red es poco fiable y llevar a cabo ellos mismos el control de errores y de flujo. Otro grupo (representado por las empresas telefónicas) argumenta que esta capa debe proveer un servicio fiable, orientado a conexión.

1.13.1.3.1. Encaminamiento

La función real de la capa de red es la del encaminamiento de paquetes desde el origen hasta el destino. En muchas redes los paquetes necesitan realizar muchos saltos para completar un viaje. La excepción la dan las redes de difusión, pero aun aquí el encaminamiento es interesante cuando el origen y el destino no se encuentran en la misma red.

El **algoritmo de encaminamiento** es aquella parte del *software* (conocido como protocolo de comunicaciones) correspondiente a la capa de red, que es la responsable de decidir sobre qué línea de

salida deberá transmitir un paquete que llega. Cuando se utilizan datagramas, la decisión deberá tomarse con cada paquete que llegue; mientras que en el caso de circuitos virtuales, estas decisiones sólo se tomarán cuando se establezca un nuevo circuito virtual, después los paquetes seguirán la ruta establecida. A esto último se le conoce como "**encaminamiento de sesión**", ya que la ruta permanece durante toda la sesión.

1.13.1.3.2. Congestión

Cuando existen muchos paquetes dentro de la red, el rendimiento se degrada. Esta situación se conoce como **congestión**.

Existen varias estrategias para el control de congestión:

- Que asignen recursos anticipados.
- Que desechen paquetes cuando no se pueden procesar.
- Que se restrinja el número de paquetes en la red.
- Utilizar el control de flujo para evitar la congestión.
- Obstruir la entrada de datos cuando la red está sobrecargada

1.13.1.3.3. Bloqueo

La máxima congestión es el **bloqueo**, también llamado estancamiento. En este caso los nodos no pueden proseguir hasta tanto su vecino no realice una acción, el que a su vez espera de otro nodo y éste del primero, creándose un círculo del cual no podrán salir produciéndose un bloqueo.

Si bien existen varios algoritmos que previenen un bloqueo, todos se basan en la asignación y el control de los recursos de cada nodo, evitando la transmisión si no se asegura la continuidad del camino del paquete.

1.13.1.4. Capa de Transporte

Su función principal consiste en aceptar los datos de la capa de sesión, dividirlos (si es necesario) en unidades más pequeñas, pasarlos a la capa de red y asegurar que todos los pedazos lleguen correctamente al otro extremo. Además debe aislar a la capa de sesión de los cambios de tecnología del *hardware*.

Esta capa es el corazón de la jerarquía de protocolos; sin ella el concepto de protocolo no tiene sentido. Su tarea consiste en asegurar el transporte de los datos de la máquina fuente a la destino, independientemente de la red física en uso.

Así como hay dos tipos de servicios de red, también hay dos tipos de servicios de transporte: **orientado a conexión** y **no orientado a conexión**. Ambos servicios son similares a los de la capa de red. Básicamente podemos decir que la existencia de la capa de transporte hace más confiable el servicio, que el proporcionado por la capa de red. Gracias a esta capa es posible que los programas de aplicación puedan escribirse usando primitivas y hacer que funcionen en una gran variedad de redes, sin preocuparse de tratar con diferentes interfaces de cada red.

Podemos dividir el modelo OSI en dos partes:

- De la capa 1 a la 4 serán **proveedoras** de servicio de transporte.
- De la capa 5 a la 7 serán **usuarios** de servicio de transporte.

Esta diferencia entre proveedor y usuario tiene un impacto considerable sobre el diseño de las capas y coloca a la capa de transporte en una posición clave, ya que constituye la frontera entre suministrador y usuario de un servicio de transmisión de datos seguros.

Otra forma de ver a esta capa es considerando que su función es la de enriquecer la calidad de servicio suministrada por la capa de red. En otras palabras, esta capa está para contribuir y llenar huecos entre lo que los usuarios desean y lo que el servicio de red ofrece.

La capa de transporte determina qué tipos de servicio le brindará a la capa de sesión, y en definitiva a los usuarios.

1.13.1.5. Capa de Sesión

Esta capa permite que los usuarios establezcan sesiones de trabajo entre ellos. Por ejemplo, una sesión podrá permitir al usuario acceder a un sistema de tiempo compartido a distancia, o transferir un archivo entre dos máquinas.

Uno de los servicios de esta capa consiste en gestionar el control de diálogo. Las sesiones controlan el tráfico de los mensajes en ambas direcciones.

La administración del testigo es otro de los servicios en las redes Token Ring[12]. Para algunos protocolos es esencial que ambos lados no traten de realizar la misma operación en el mismo instante. Para manejar esta situación, la capa de sesión proporciona testigos que pueden ser intercambiados, sólo quien tenga el testigo puede realizar la operación crítica.

Otro servicio es la **sincronización**. La capa de sesión sólo proporciona puntos de verificación en el flujo de datos, con objeto de que después de una caída, sólo se repitan los mensajes desde el último punto de verificación.

1.13.1.6. Capa de Presentación

Esta capa se ocupa de los aspectos de sintaxis y semántica de la información que transmite. Un ejemplo típico de esta capa es el relacionado con la codificación de datos conforme a lo acordado previamente. La mayor parte de los programas de aplicación no intercambian cadenas de bits binarios aleatorios, sino estructuras de datos constituidos por varios elementos sencillos. Se pueden tener diferentes códigos (ASCII, EBCDIC) enteros, complemento a uno, dos, etc. Para posibilitar la comunicación de ordenadores con diferentes representaciones, la estructura de los datos a intercambiar puede definirse en forma abstracta. El trabajo de manejar estas estructuras de datos abstractas, y la

[12] Estándar desarrollado por IBM y ratificado como un estándar IEEE 802.5.

conversión de la representación utilizada en el ordenador a la representación normal de la red, se lleva a cabo a través de la capa de presentación.

Así para el caso de tener que intercambiar archivos de imágenes, música, multimedia, etc., esta es la capa que maneja su representación (JPEG, MPEG, WAV, Midi, etc.).

Esta capa está ligada también a otros aspectos de representación de la información. Por ejemplo la **compresión de datos**, que se utilizará para disminuir el tamaño de los mensajes a transmitir. Otro aspecto es el de **criptografía** que se usa por razones de seguridad de la información.

1.13.1.7. Capa de Aplicación

Esta capa contiene una variedad de protocolos necesarios para hacer compatibles los distintos dispositivos de aplicación. Por ejemplo, considérese un editor orientado a pantalla que deba trabajar en una red con diferentes tipos de terminales, cada uno con formatos diferentes de pantalla, secuencias de escape para insertar y eliminar texto, mover el cursor, etc. Una forma de resolver este problema es definir una **terminal virtual de red** abstracta, con la cual los programas pueden ser escritos para tratar con ella. Para transferir funciones de una terminal virtual de una red a una terminal real se debe escribir un *software* que permita el manejo de cada tipo de terminal. Por ejemplo, cuando el editor mueva el cursor del terminal virtual al extremo superior izquierdo, dicho software deberá emitir la secuencia de comandos para que el terminal real ubique al cursor en el sitio indicado. El *software* completo del terminal virtual se encuentra en la capa de aplicación.

Otra función de esta capa es la transferencia de archivos. La transferencia de archivos entre dos sistemas diferentes, requiere de la solución de las incompatibilidades.

En esta capa también funcionan los navegadores de Internet. Estos son los programas de aplicación que permiten visualizar en red las páginas webs, mediante el protocolo http.

1.13.2. Modelo TCP/IP

Este modelo fue el que se usó en la "abuela" de todas las redes de comunicaciones, la Arpanet y es el que se usa en su sucesora, Internet. La primera era una red de investigación patrocinada por el Departamento de Defensa de Estados Unidos. Al final conectó a cientos de universidades e instalaciones del gobierno usando líneas telefónicas rentadas. Cuando más tarde se añadieron redes de satélite y radio, los protocolos existentes tuvieron problemas para interactuar con ellas, de modo que se necesitó una arquitectura de referencia nueva. Así, la capacidad de conectar entre sí múltiples redes fue uno de los principales objetivos de diseño.

Esta arquitectura se popularizó después como el Conjunto de protocolos **TCP/IP**, por las iniciales de sus dos protocolos primarios.

Las cuatro capas del modelo son:

- Nivel 4: **Capa de Aplicación.**
- Nivel 3: **Capa de Transporte.**
- Nivel 2: **Capa de Interred.**
- Nivel 1: **Host a red.**

1.13.2.1. Capa del Host a la Red

El modelo realmente no dice mucho de lo que aquí sucede, fuera de indicar que el nodo se ha de conectar a la red haciendo uso de algún protocolo de modo que pueda enviar por ella paquetes de IP. Este protocolo no está definido y varía de un nodo a otro y de red a red.

Esto es bueno desde el punto de vista que el conjunto de protocolos TCP/IP es absolutamente independiente del método de acceso, de la codificación de señales y demás detalles que se podrían presentar en esta capa. La tecnología avanza y va proponiendo otras formas de acceso a la red; todas proporcionan conectividad a IP

1.13.2.2. Capa de Interred

Esta capa es el eje que mantiene unida toda la arquitectura. Su misión es permitir que los nodos inyecten paquetes en cualquier red y los hagan viajar en forma independiente a su destino (que podría estar en una red diferente).

Define un formato de paquete y protocolo oficial llamado **IP** (**Internet Protocol**, protocolo de interred). El trabajo de esta capa es entregar paquetes a donde se suponen que deben ir. Aquí la consideración más importante es el enrutamiento de los paquetes, y también evitar la congestión. Por lo anterior es razonable decir que la capa de interred TCP/IP es muy parecida a la capa de red OSI.

1.13.2.3. Capa de Transporte

Se diseñó para permitir que las entidades pares en los nodos de origen y destino lleven a cabo una conversación, lo mismo que en la capa de transporte OSI.

Aquí se definieron los protocolos de extremo a extremo. El primero, **TCP (Protocolo de Control de la Transmisión)** es un protocolo confiable orientado a la conexión que permite que una corriente de bytes originada en una máquina se entregue sin errores en cualquier otra máquina de la interred. Este protocolo fragmenta la corriente entrante de bytes en mensajes discretos y pasa cada uno a la capa de interred. En el destino, el proceso TCP receptor reensambla los mensajes recibidos para formar la corriente de salida. El TCP también se encarga del control de flujo para asegurar que un emisor rápido pueda abrumar a un receptor lento con más mensajes de los que puede manejar.

El segundo protocolo de esta capa, el **UDP (Protocolo de Datagrama de Usuario)**, es un protocolo sin conexión, no confiable para aplicaciones que no necesitan la asignación de secuencia ni el control de flujo del TCP y que desean utilizar los suyos propios.

1.13.2.4. Capa de Aplicación

Este modelo no tiene capas de sesión ni de presentación. No se pensó que fueran necesarias. La capa de aplicación contiene todos los protocolos de alto nivel. Entre los protocolos más antiguos están el de **terminal virtual (TELNET)**, el de **transferencia de archivos (FTP)** y el de **correo electrónico (SMTP)**. El primero permite que un usuario en una máquina ingrese en una máquina distante y trabaje ahí. El segundo ofrece un mecanismo para proveer datos de una máquina a otra en forma eficiente. El correo electrónico fue en sus orígenes sólo una transferencia de archivos, pero más adelante se desarrolló para él un protocolo especializado; con los años, se le han añadido muchos otros protocolos, como el HTTP, el protocolo que se usa para recuperar páginas en la World Wide Web.

1.13.3. Comparación entre los Modelos OSI y TCP/IP

En la **figura 1.19**, la definición de **servicio** dice lo que la capa hace, no cómo es que las entidades superiores tienen acceso a ella o cómo funciona la capa. La **interfaz** de una capa le dice a los procesos de arriba cómo acceder a ella; especifica cuáles son los parámetros y qué resultados esperar; nada dice tampoco sobre cómo trabaja la capa por dentro. Los **protocolos** pares que se usan en una capa son asunto de la capa. Ésta puede usar los protocolos que quiera, siempre que consiga que se realice el trabajo (esto es, que se provea los servicios que ofrece). La capa puede también cambiar los protocolos a voluntad sin afectar el *software* de las capas superiores.

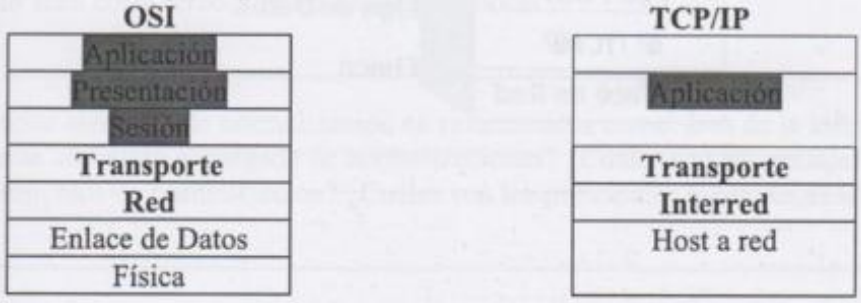
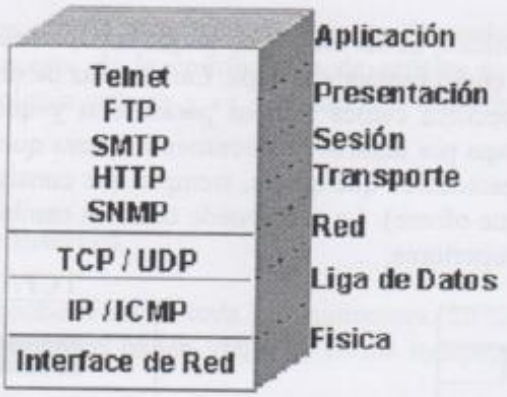


FIGURA 1.18: Comparación de capas entre modelos.

Modelo OSI	Modelo TCP/IP
Se basa en el concepto de un gran número de protocolos independientes.	Se basa en el concepto de un gran número de protocolos independientes.
La funcionalidad de las capas es muy similar a las de TCP/IP.	La funcionalidad de las capas es muy similar a las de OSI.
Tres conceptos (*) son fundamentales: servicios, interfaces y protocolos. Como consecuencia, se ocultan mejor los protocolos y se pueden reemplazar con relativa facilidad al cambiar la tecnología.	Originalmente no distinguía en forma clara entre servicios, interfaz y protocolo, aunque se ha tratado de reajustarlo después a fin de hacerlo más parecido a OSI.
Se desarrolló antes de que se inventaran los protocolos. Este orden significa que el modelo no se orientó hacia un conjunto específico de protocolos, lo cual lo convirtió en algo muy general.	Aquí primero llegaron los protocolos, y el modelo fue sólo una descripción de los protocolos existentes. El único problema fue que el modelo no se ajustaba a ninguna otra pila de protocolos.
Tiene siete capas.	Tiene cuatro capas.
Apoya la comunicación tanto sin conexión como la orientada a la conexión en la capa de red, pero en la capa de transporte donde es más importante lo hace únicamente con la comunicación orientada a la conexión.	Sólo tiene un modo en la capa de red (sin conexión) pero apoya ambos modos en la capa de transporte.

FIGURA 1.19: Comparación entre los dos modelos.

Algunos protocolos definidos en el conjunto de TCP/IP son:



Preguntas de Repaso a la Unidad 1

- 1) Consideremos una red de "N" nodos. Para cada una de las topologías típicas (anillo, estrella, bus, completa) determine:

  a. Cantidad de enlaces total.

  b. Cantidad de enlaces necesarios para agregar un nodo.

  c. Cantidad de interfaces por estación de trabajo

- 2) Si un nivel de una arquitectura de red en capas quiere proveer servicios 100 % confiables de transferencia de archivos, su nivel inmediato inferior debe proveerle:

  a. servicio sin conexión sin reconocimiento.

  b. servicio sin conexión con reconocimiento.

  c. servicio orientado a conexión.

  d. cualquiera de las anteriores.

- 3) Describa las características principales de las siguientes redes y tipos de redes públicas: Red telefónica pública conmutada (RTPC), Red de televisión por cable (CATV), Redes satelitales VSAT, Internet ¿Cuáles de ellas se asemejan en su arquitectura al modelo OSI?

- 4) Explique las diferencias entre las redes WAN, MAN, LAN y PAN.

- 5) Ejemplifique 5 aplicaciones de las redes de computadoras en general. Señale además las desventajas de su implementación en cada caso y proponga métodos para solucionarlas.

- 6) Muestre ejemplos de sistemas de cómputo que interactúen con varios usuarios simultáneamente y que no sean considerados redes de computadoras.

- 6) ¿Conoce ejemplos de normalización no relacionados con el área de la informática? ¿Conoce algún ente argentino encargado de normalizaciones? ¿Cuáles son las ventajas de efectuar estos procedimientos de normalización? ¿Cuáles son los principales inconvenientes para aplicarlos?

- 7) Explique brevemente qué son, para qué se utilizan y/o a qué se refieren cada uno de los siguientes elementos o conceptos:

- red de computadoras:
- equipo monoprocesador/ multiprocesador:
- redes wireless (sin cable):
- configuración punto a punto/ punto a multipunto
- conmutación de circuitos/ de paquetes:
- store and forward:
- multicasting/broadcasting:
- nodo de conmutación:
- enlace:
- host:
- terminal:
- subred de comunicaciones:
- canal o medio de transmisión:
- arquitectura de red:
- control de flujo:
- control de congestión:
- enrutamiento:
- direccionamiento:
- control de errores:
- multiplexación:
- acceso al medio
- comunicación simplex/ dúplex:
- internetwork:
- internet:
- fragmentación de unidades de datos:
- primitivas:
- conexión:
- PDU:
- header:

- 8) Complete el siguiente cuadro referido a las clases de servicios:

	Orientado a conexión	Sin conexión sin reconocimiento	Sin conexión con reconocimiento
Servicio telefónico			
Servicio postal			
Establecimiento de conexión			
Transmisión de PDUs			
Liberación de conexión			
Garantía de secuenciamiento de PDUs			
Garantía de entrega de PDUs			
Entrega de reconocimiento al usuario			
Direccionamiento en fase de conexión			
Direccionamiento en fase de transmisión de PDUs			

- 9) ¿Qué niveles del modelo OSI deben conocer la topología física de la red para trabajar correctamente?

  a. Sólo el 1

  b. 2 y 3.

  c. 3 y 4.

  d. 3.

  e. 4.

  f. Todos los niveles.

  g. Ningún nivel.

- 10) ¿Qué niveles del modelo OSI podrían hacer uso de mecanismos de control de errores en los datos?

  a. 1 y 2.

  b. 1, 2 y 3.

  c. 2 y 4.

  d. 2, 3 y 4.

  e. 2 y 3.

  f. 3 y 4.

  g. 2, 3, 4 y 5.

  h. Todos los niveles.

- 11) ¿Qué niveles del modelo OSI deben preocuparse del control de congestionamiento en una WAN?

  a. 2, 3 y 4.

  b. 1 y 3.

  c. 3.

  d. 3 y 4.

  e. Sólo el 4.

  f. Todos los niveles.

  g. No se realiza.

- 12) ¿Qué protocolos se proponen desde OSI para la capa de Aplicación?

- 13) ¿Qué protocolos se proponen desde la familia TCP para la capa de Aplicación? ¿Son iguales a los propuestos por OSI?

- 14) ¿Qué protocolos se proponen desde la familia TCP para la capa de Transporte? Destaque sus diferencias

- 15) ¿Qué protocolos se proponen desde la familia TCP para la capa de Acceso del host a la red?

- 16) En Telecomunicaciones; un estándar ISO: ¿Es de cumplimiento obligatorio?

- 17) Una recomendación ITU: ¿Es de cumplimiento obligatorio?

- 18) ¿Qué beneficios le reportaría a quien lo cumpla?. Justifique su respuesta

- 19) ¿Qué inconvenientes tendría quien no lo cumpla?. Explique su respuesta

- 20) Explique qué es una RFC. ¿Cuál es el último número disponible?

Bibliografía de la Unidad 1

- **Feit, S.:** *"TCP/IP Arquitectura, protocolos, implementación y seguridad"* Editorial Mc Graw-Hill. 1998
- **Tanenbaum, A. S.**: *"Redes de Computadoras"*. Tercera Edición. Prentice Hall. 2000
- **Tanenbaum, A. S.**: *"Redes de Computadoras"*. Cuarta Edición. PEARSON Prentice Hall. México 2003
- **Esteve Domingo, Manuel y otros.**: *"Redes de Area Local y su interconexión"*.Servicio de Publicaciones de la Universidad Politécnica de Valencia. 2001
- **Halsall, F.** "*Comunicaciones de Datos, Redes de computadores y sistemas abiertos"*. Cuarta Edición. Addison Weslley Longman.
- **Programa de postgrado en Sistemas y Redes de Comunicaciones**. "*Introducción a las Telemática"*. Departamento de Telemática. Febrero/Marzo 1.994. ETSI Telecomunicación. Univ. Politécnica de Madrid.
- **Stalling, William**. "*Comunicaciones y Redes de Computadores"*. Quinta Edición. Prentice Hall. 2001
- **Hellman, Anders**: *"Understanding Telecommunications 1"* Ericsson. Telia. Suecia 1997
- Paginas de Internet.
  - http://www.itu.int/
  - http://www.iso.int/
  - http://www.ietf.org
  - http://www.cisco.com/univercd/cc/lib/
  - http://www.saulo.net/

Unidad 2

Capa de Acceso de Host a Red

Objetivos

- Proporcionar al lector la definición de las características de las redes de área local (LAN).
- Describir los protocolos de acceso al medio y clasificar las redes de área local según el protocolo de acceso al medio utilizado.
- Explicar cada uno de los estándares IEEE de la familia 802
- Describir las variantes de LANs de alta velocidad existentes
- Describir el sistema de cableado estructurado. Explicar la categorización del cableado.
- Definir las redes inalámbricas (WLAN).
- Definir las redes de área metropolitana (MAN). Definir el protocolo FDDI.
- Especificar el concepto de Red de Área Extendida (WAN[13]). Ejemplificar.
- Describir la estructura y el funcionamiento de la Red Telefónica Pública Conmutada (RTPC). Destacar su uso para la transmisión de datos.
- Definir la estructura y los tipos de accesos que existen en la Red Digital de Servicios Integrados[14]. Comprender el concepto de integración de servicios que brinda dicha RDSI
- Definir la estructura y características de las Redes Satelitales con terminales de muy pequeña apertura (VSAT[15]).
- Describir el protocolo Frame Relay.
- Estructurar y describir SONET (Red Óptica Sincrónica). Identificar el estándar internacional SDH (Jerarquía Digital Síncrona).
- Estructurar y describir la tecnología ATM (Modo de Transferencia Asíncrono)

---

[13] En Inglés: Wide Area Network.
[14] RDSI. En Inglés: (ISDN) Integrated Services Digital Network.
[15] En inglés: Very Small Aperture Terminal

2.1. Concepto de Red de Área Local[16]

Una red de área local es una red de comunicaciones que sirve a usuarios dentro de un mismo edificio: Puede ser de datos (LAN), de voz, de video (CCTV), etc.

En lo sucesivo, en este texto cuando hagamos referencia a una Red de Área Local (LAN) lo estaremos haciendo para una red de datos, de cobertura reducida (ambientes de oficinas) y de propiedad privada (empresa, institución, etc.).

2.2. Elementos de una red LAN

Como se vio en el punto **1.9**, una red LAN tiene los siguientes componentes (según la función que cumplen dentro de la LAN):

- Enlace de comunicaciones (cableado y elementos de interconexión).
- Tarjetas de Interfase de Red (NIC)
- Servidores.
- Estaciones de trabajo.
- Sistema operativo de red.

Podemos ver un esquema en la **figura 2.1**.

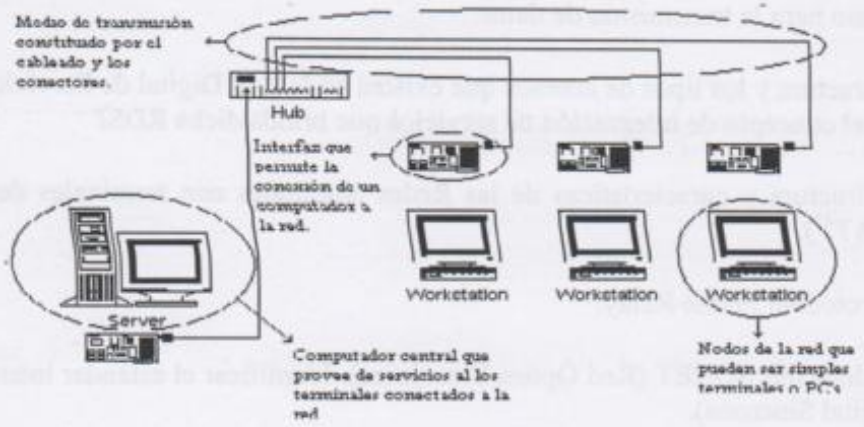


FIGURA 2.1: Red LAN.

[16] En Inglés: Local Area Network.

2.2.1. Enlace de comunicaciones

Lo constituyen el cableado y los otros elementos (hubs, switchs, paneles de conexión, etc.) utilizados para conectar computadoras.

- **Cableado:** la conexión física de computadoras mediante cables entre puestos de trabajo y hubs
- **Hubs:** dispositivos que realizan el bus lógico para el funcionamiento del protocolo de acceso al medio LAN. Funcionan como concentradores de un cableado que sale de ellos en estrella.
- **Switches:** dispositivos especiales para dividir las LANs grandes en segmentos para un manejo más fácil, para minimizar el tráfico innecesario entre segmentos de la red.

2.2.2. Tarjetas de Interfaz (NIC)[17]

FIGURA 2.2: Tarjeta NIC.

Los adaptadores de computadoras para cables son conocidos como NICs.

Éstos conectan a la computadora físicamente al tipo particular de cable que ha sido seleccionado; traducen entre señales bus de PCs locales de bajo poder y señales de medios de red de alto poder para larga distancia más fuertes, y corren programas en su ROM que formatean las señales enviadas por cable.

Es importante notar que ciertos tipos de NICs pueden enviar y recibir datos mucho más rápidamente que otros: hay Token Ring NICs de 4 Mb/s y de 16 Mb/s., Ethernet NICs de 10 Mb/s, de 100 Mb/s y 1000 Mb/s, NICs FDDI de 100 Mb/s, etc.

Con las crecientes necesidades de rapidez en las redes locales, la elección de NICs apropiados para servidores y clientes, es un elemento importante en el diseño de una red. En la **figura 2.2** se muestra una interfaz NIC.

Las tarjetas NIC implementan los niveles 1 y 2 del modelo OSI y en ellas se encuentra el protocolo de acceso al medio.

[17] En Inglés: Network Interfaz Card.

2.2.3. Estructura de una estación de trabajo y un servidor

2.2.3.1. Servidor

El servidor es aquel o aquellas computadoras que van a compartir sus recursos *hardware* y *software* con los demás equipos de la red. Es empleado tanto por su potencia de cálculo, como por la información que gestiona y los recursos que comparte. Las computadoras que toman el papel de estaciones de trabajo aprovechan o tienen a su disposición los recursos que ofrece la red así como los servicios que proporcionan los servidores a los cuales pueden acceder. También se puede pensar en computadoras híbridas, que hacen a la vez de servidores y de estaciones de trabajo.

Existen dos tipos de servidores:

- **Servidores dedicados**: son aquellas computadoras que están exclusivamente a disposición de la red.
- **Servidores no dedicados**: además de tomar el papel de servidores también pueden utilizarse como estaciones de trabajo.

2.2.3.2. Estación de trabajo

Es cualquier estación, terminal, computadora u otro dispositivo en una red de computadoras.

- **Computadoras:** las computadoras "cliente" pequeñas en los escritorios de los trabajadores, y computadoras más grandes "servidores" que proveen servicios especializados y recursos de *hardware* poderosas desde un punto central.
- **Aplicación para clientes y servidores:** programas que proveen funciones de propósito especial para computadoras "cliente y servidor". Las aplicaciones de computadoras cliente modernas cada vez han integrado más funciones de LAN y de Internet. Algunas de las aplicaciones nuevas están siendo desarrolladas de manera modular, para que los componentes pequeños puedan ser bajados de servidores a clientes para uso temporal.

2.2.4. Sistemas Operativos de Red (NOS)[18]

Los sistemas operativos de red son un conjunto de programas y funciones que interactuando en forma conjunta, producen el funcionamiento de un conjunto de máquinas conectadas entre sí por diferentes dispositivos, permitiendo que intercambien informaciones, aplicaciones, etc, y compartan recursos hardware.

Posteriormente desarrollaremos en forma detallada este tema en la Unidad 5.

[18] En Inglés: Network Operating System.

2.3. Métodos de acceso al medio

Los métodos de acceso al medio se encuentran implementados en la NIC de cada máquina; como veremos a continuación son los que posibilitan que un conjunto de máquinas comparta un único medio de comunicación mediante una disciplina para acceder y hacer uso del mismo.

Primero describiremos algunos protocolos muy sencillos como el Aloha y el Alora ranurado que si bien no son los implementados en la actualidad por las placas NIC han dado la base para el desarrollo de los actuales

2.3.1. ALOHA simple

Esta técnica se comenzó a utilizar en un sistema de envío de paquetes a través de enlaces terrestres de radio, pero sus ideas son aplicables a cualquier medio de comunicación. En **ALOHA simple**, todos los usuarios tienen idénticas jerarquías; una estación se pondrá a transmitir cuando tenga datos para enviar.

Como el canal no está dotado de ninguna estructura *primaria /secundaria*, es posible que varios usuarios transmitan simultáneamente. En este caso las señales se interferirán y se producirá una colisión. Cuando se produce una colisión el mensaje se arruina por completo y se deberá retransmitir el paquete.

A grandes rasgos, la idea consiste en escuchar el canal de bajada durante un tiempo igual al de retardo de subida y bajada, después de haber enviado el paquete, ver **figura 2.3.** Si el paquete fue destruido, el nodo emisor después de un tiempo aleatorio de espera vuelve a transmitirlo. En la **figura 2.4** se muestra como las estaciones A y B transmiten a través de un canal. Esto indica que el paquete A1 ha subido y bajado sin problemas, también el B2, no así el A2 que colisiona con el B2

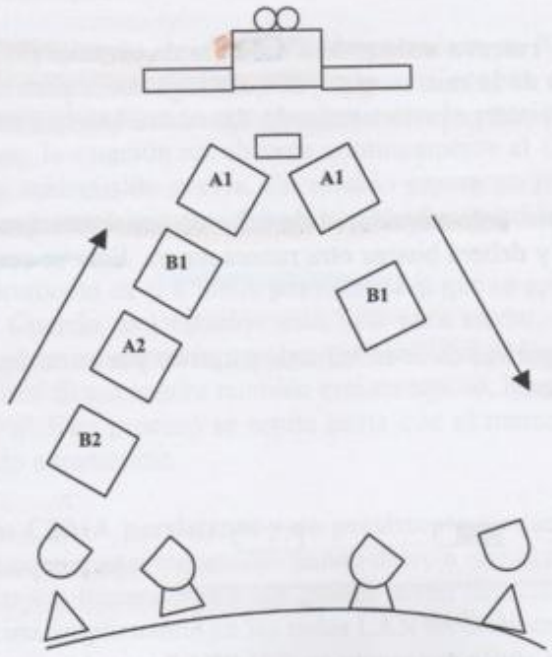


FIGURA 2.3: ALOHA simple.

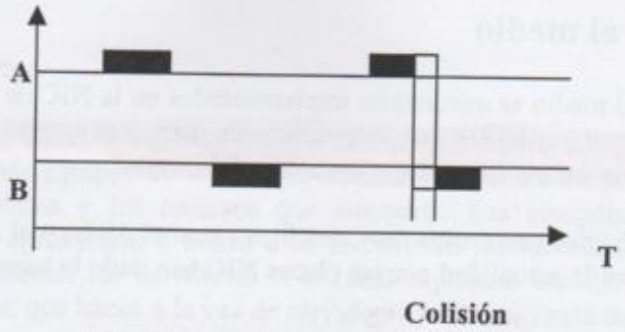


FIGURA 2.4: Colisión de paquetes en el ALOHA simple.

2.3.2. S-ALOHA (ALOHA Ranurado)

Exige el establecimiento de sincronismos a las estaciones terrenas y el satélite. El sincronismo implica enviar un tráfico en períodos concretos (ranuras). Todas las estaciones han de transmitir al comenzar una ranura de tiempo. No puede enviarse un paquete que solape más de una ranura.

ALOHA ranurado produce un aumento significativo del caudal cursado, ya que cuando dos paquetes colisionan, sólo una ranura es afectada.

En el **ALOHA ranurado con captura**, las ranuras de tiempo se combinan dentro de una única trama de ALOHA. Esta trama debe ser igual o mayor que el retardo total de subida y bajada. Por lo tanto un paquete de 1000 bits de 20 *mseg* exige como mínimo 12 ranuras para conformar una trama ALOHA: 12 ranuras por 20 *mseg* es igual a 240 *mseg*. En este método una estación deberá seleccionar una ranura vacía. Las colisiones que aquí se pueden producir es cuando dos estaciones capturan una misma ranura de trama.

En el **ALOHA ranurado con reserva** cada ranura de la trama es propiedad, de un determinado usuario, el que posee el uso exclusivo de la misma, siempre que tenga datos para transmitir. En caso de que renuncie a la misma lo hará con un código predeterminado. La ranura quedará vacía para quien quiera capturarla.

Una vez tomada por otro usuario, éste adquiere el derecho de uso, hasta que el legítimo dueño la reclame. En este caso será expulsado, y deberá buscar otra ranura nueva. Esto se conoce como estructura de igual a igual con prioridad.

En la **figura 2.5** se muestra el gráfico de la emisión de paquetes por parte de las estaciones **A** y **B** donde se observa la colisión de paquetes.

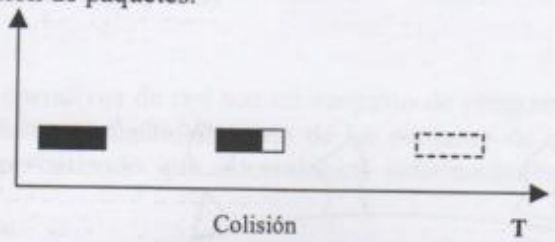


FIGURA 2.5: Colisión de paquetes en el ALOHA Ranurado.

La **figura 2.6** muestra los rendimientos de ALOHA vs. ALOHA ranurado en función de los intentos de transmisión normalizados al tiempo de duración del paquete (G)

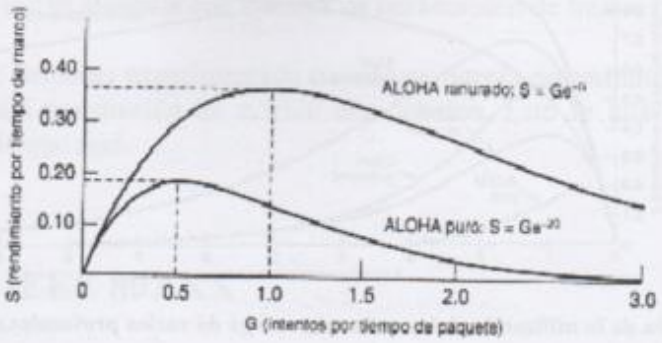


FIGURA 2.6: Rendimiento contra tráfico ofrecido de los sistemas ALOHAS.

2.3.3. CSMA/CD (Acceso múltiple con detección de portadora y detección de colisiones)[19]

Un intento por mejorar el protocolo Aloha consistió en obligar a las estaciones a escuchar el canal antes de transmitir; de esta forma se evitan colisiones. Este protocolo tiene tres variantes:

a) El primer protocolo de detección de portadora se llama **CSMA persistente-1.** Cuando una estación tiene datos por transmitir, primero escucha el canal para ver si otra está transmitiendo en ese momento. Si el canal está ocupado, la estación espera hasta que se desocupa. Cuando la estación detecta un canal en reposo, transmite un marco. Si ocurre una colisión, la estación espera una cantidad aleatoria de tiempo y comienza de nuevo. El protocolo se llama persistente porque la estación transmite con una probabilidad de 1 cuando encuentra un canal en reposo.

b) Un segundo protocolo de detección de portadora se llama **CSMA no persistente.** En este protocolo se hace un intento consistente por ser menos egoísta que el anterior. Antes de enviar, una estación detecta el canal. Si nadie más está transmitiendo, la estación comienza a hacerlo. Sin embargo, si el canal ya está en uso, la estación no observa continuamente el canal a fin de tomarlo de inmediato al detectar el final de la transmisión previa. En cambio espera un período de tiempo aleatorio y repite el algoritmo. Intuitivamente este algoritmo deberá conducir a una utilización mejor del canal.

c) El último protocolo es el **CSMA persistente-p** que se aplica a canales ranurados y funciona de la siguiente manera. Cuando una estación está lista para enviar, escucha el canal. Si el canal está en reposo la estación empieza a transmitir, con una probabilidad p. Con una probabilidad $q = 1 - p$, se espera hasta la siguiente ranura. Si esa ranura también está en reposo, la estación transmite o espera nuevamente, con probabilidad p y q. Este proceso se repite hasta que el marco ha sido transmitido o hasta que otra estación ha comenzado a transmitir.

Los protocolos **CSMA persistente y no persistente** ciertamente son una mejora porque aseguran que ninguna estación comienza a transmitir cuando detecta que el canal esté ocupado. Otra mejora es que las estaciones aborten sus transmisiones tan pronto como detectan una colisión. El protocolo conocido como **CSMA/CD** se usa ampliamente en las redes LAN en la subcapa **MAC**. Ver **figura 2.7.**

[19] En Inglés: Carrier Sense Multiple Access With Collision Detection.

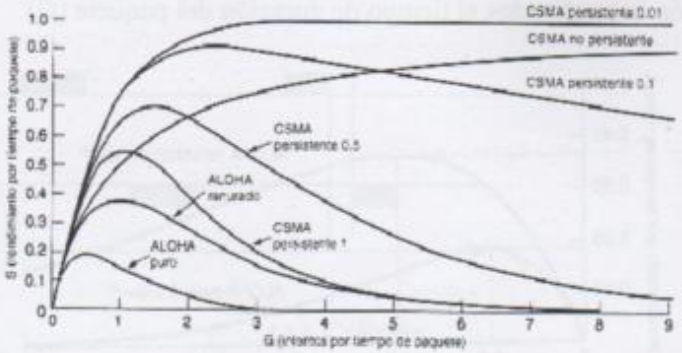


FIGURA 2.7: Comparación de la utilización del canal contra carga de varios protocolos de acceso aleatorio.

CSMA/CD, al igual que muchos protocolos de LAN, utiliza el modelo conceptual de la **figura 2.8**. En el punto marcado t_0, una estación ha terminado de transmitir su marco. Cualquier otra estación que tenga un marco para enviar puede intentar hacerlo. Si dos o más estaciones intentan transmitir simultáneamente, habrá una colisión. Las colisiones pueden detectarse observando el ancho de banda o el ancho del pulso de la señal recibida y comparándola con la señal transmitida.

Una vez que una estación detecta una colisión, aborta la transmisión, y espera un período de tiempo aleatorio e intenta de nuevo, suponiendo que ninguna estación ha comenzado a transmitir durante ese lapso. Por tanto, nuestro modelo CSMA/CD consistirá en períodos alternantes de contención y transmisión, ocurriendo períodos muertos cuando todas las estaciones están calladas.

Sus principales características son:

- **Elevada eficacia**, sobre todo en utilizaciones medias y bajas.
- **La flexibilidad de conexionado y facilidad de adicionar o suprimir estaciones de la red.**
- **Bajo retardo**, aunque no acotable determinísticamente.
- **La ausencia de establecimientos físicos o lógicos al conectarse en red una estación.**

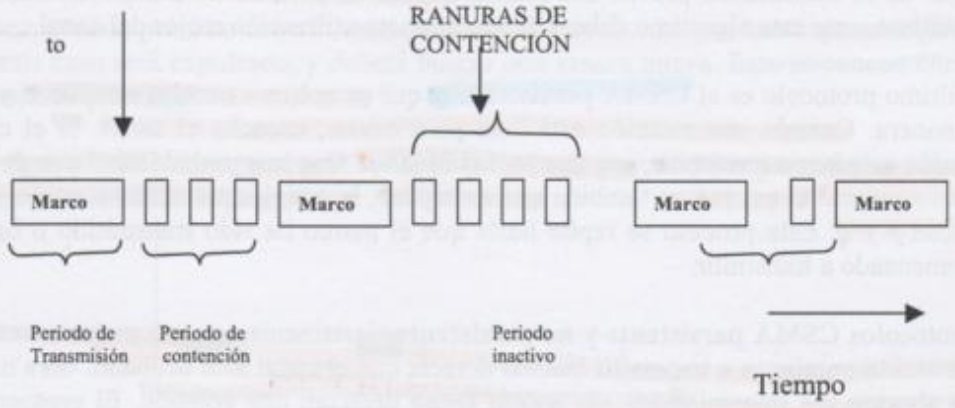


FIGURA 2.8: Funcionamiento de CSMA/CD.

El protocolo CSMA /CD tiene dos inconvenientes:

- Bajo carga pesada, la performance del sistema se degrada severamente. Ocurren cada vez más colisiones y la red es atascada con intentos de retrasmisión de tramas que han sufrido colisiones.
- La cantidad de demoras experimentada cuando se intenta retransmitir una trama es impredecible después que una transmisión ha sufrido una colisión. Esto es una característica indeseable en ambientes de tiempo real.

2.4. Estándares IEEE 802.XX

El Instituto de Ingenieros Electricistas y Electrónicos de USA se ha dedicado a trabajar, desarrollando estándares para las capas Física y de Enlace del modelo OSI, ya que estas se corresponden con la capa de acceso del Host a la Red, que en la familia de protocolos TCP/IP no está especificada.

La familia de estándares, los 802 son para redes LAN y MAN (como podemos observar en la figura 2.8):

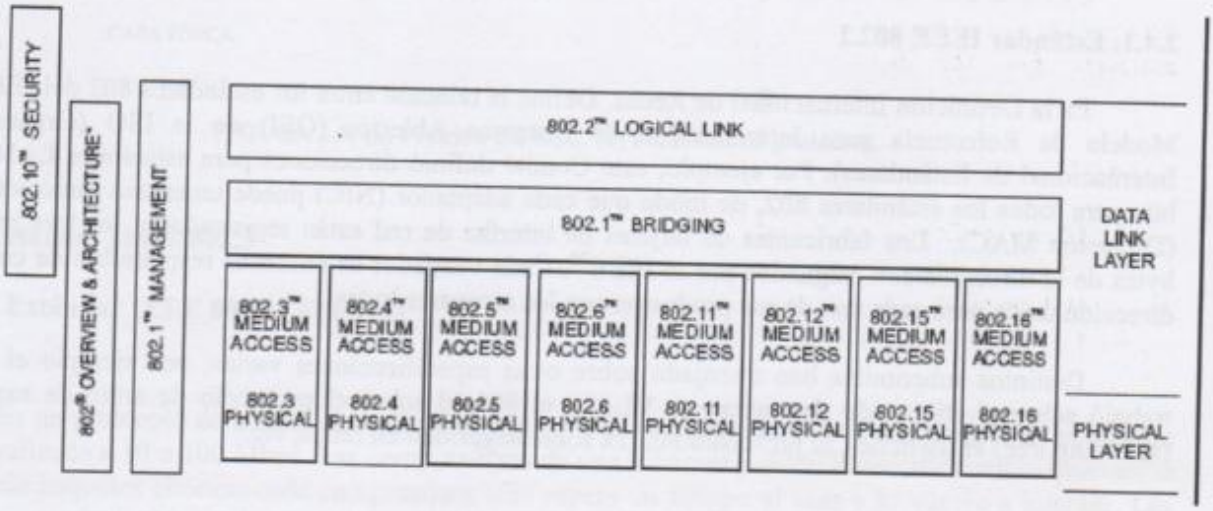


Figura 2.8: Familia de estándares IEEE 802

Estos estándares tienen su correlación con los estándares ISO/IEC. A continuación enumeramos la correspondencia entre algunos de ellos:

- **IEEE 802:** *Overview and Architecture.*
- **IEEE 802.1B** [ISO/IEC 15802-2] *LAN/MAN Management*
- **IEEE 802.1K** [ISO/IEC 15802-2] *LAN/MAN Management*
- **IEEE 802.1D** [ISO/IEC 15802-3] *Media Access Control (MAC) Bridges.*
- **IEEE 802.1Q** *Virtual Bridged Local Area Networks.*
- **IEEE 802.1X** *Port-based network access control*

- **IEEE 802.2** [ISO/IEC 8802-2] *Logical Link Control.*
- **IEEE 802.3** [ISO/IEC 8802-3] *CSMA/CD Access Method and Physical Layer Specifications.*
- **IEEE 802.4** [ISO/IEC 8802-4] *Token Passing Bus Access Method and Physical Layer Specifications.*
- **IEEE 802.5** [ISO/IEC 8802-5] *Token Ring Access Method and Physical Layer Specifications.*
- **IEEE 802.6** [ISO/IEC 8802-6] *Distributed Queue Dual Bus Access Method and Physical Layer Specifications.*
- **IEEE 802.7** *IEEE Recommended Practice for Broadband Local Area Networks.*
- **IEEE 802.10:** *Interoperable LAN/MAN Security.*
- **IEEE 802.11** [ISO/IEC DIS 8802-11] *Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications.*
- **IEEE 802.12** [ISO/IEC 8802-12] *Demand Priority Access Method, Physical Layer and Repeater Specifications.*
- **IEEE 802.15** *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for: Wireless Personal Area Networks.*
- **IEEE 802.16** *Air Interface for Fixed Broadband Wireless Access Systems.*
- **IEEE 802.17** *Resilient Packet Ring*

2.4.1. Estándar IEEE 802.1

Es la Definición Internacional de Redes. Define la relación entre los estándares 802 del IEEE y el Modelo de Referencia para Interconexión de Sistemas Abiertos (OSI) de la ISO (Organización Internacional de Estándares). Por ejemplo, este Comité definió direcciones para estaciones LAN de 48 bits para todos los estándares 802, de modo que cada adaptador (NIC) puede tener una dirección única (Dirección MAC). Los fabricantes de tarjetas de interfaz de red están registrados y los tres primeros bytes de la dirección son asignados por el IEEE[20]. Cada vendedor es entonces responsable de crear una dirección única para cada uno de sus productos con los otros tres bytes.

Distintos subcomités han trabajado sobre otras especificaciones varias; por ejemplo el 802.1q trabajó sobre el etiquetado de tramas en VLAN, el 802.1d sobre el protocolo de árbol de expansión (spanning tree) en switches, el protocolo 802.1x sobre seguridad en redes, etc.

2.4.2. Estándar IEEE 802.2: Control Lógico de Enlace

El IEEE ha definido un protocolo que puede operar por encima de todos los protocolos de LAN y MAN de la familia 802. Además, este protocolo, llamado LLC (Logical Link Control) esconde las diferencias entre los distintos tipos de redes 802, proporcionando un formato único y una interfaz con la capa de red. Este formato, interfaz y protocolo están basados estrechamente en OSI.

El LLC forma la mitad superior de la capa de enlace de datos, con la subcapa de MAC por debajo de él como lo muestra la **figura 2.9**.

El uso típico del LLC es el siguiente: la capa de red de la máquina transmisora pasa un paquete al LLC usando las primitivas de acceso del LLC. La subcapa LLC entonces agrega una cabecera LLC que

[20] Instituto de Ingenieros de Electricidad y Electrónica. En Inglés: *Institute of Electrical and Electronics Engineers.*

contiene los números de secuencia y acuse. La estructura resultante se introduce entonces en el campo de carga útil de un marco 802.x y se transmite. En el receptor ocurre el proceso inverso.

El LLC proporciona tres servicios diferentes:

1. Servicio no confiable de datagramas.
2. Servicio reconocido de datagramas.
3. Servicio confiable orientado a conexión.

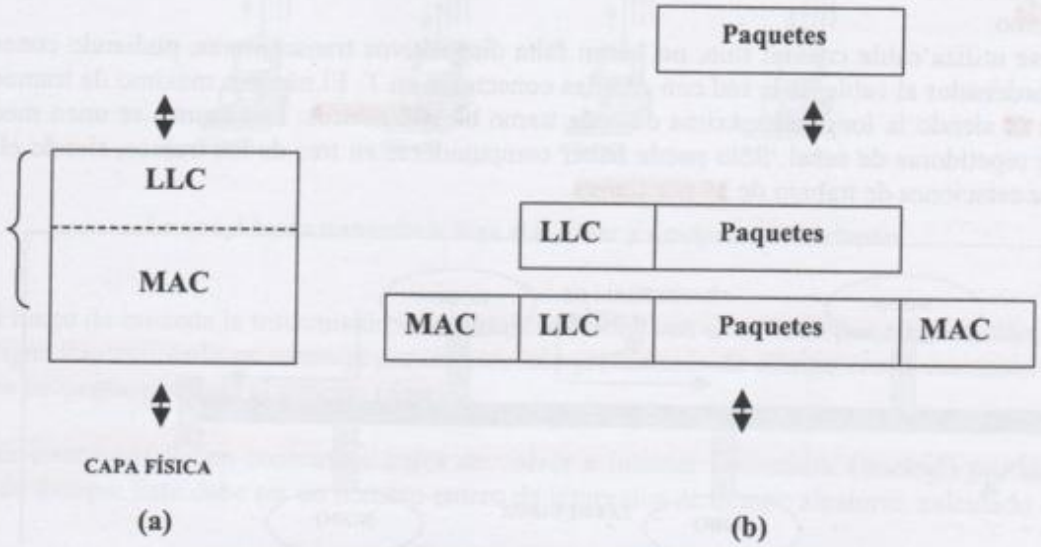


FIGURA 2.9: (a) Posición del LLC. (b) Formatos de protocolo.

2.4.3. Estándar IEEE 802.3

2.4.3.1. Estándar IEEE 802.3: Ethernet [21]

Es un protocolo de acceso al medio pensado para una red basada en bus con control de operación descentralizado a 10 o 100 Mbps. Las computadoras de una Ethernet pueden transmitir cuando quieran; si dos o más paquetes chocan, cada computadora sólo espera un tiempo al azar y lo vuelve a intentar. Las tres razones principales por las que el comité del 802.3 decidió diseñar una LAN. 802.3 fueron:

1. La necesidad de compatibilidad hacia atrás con miles de LAN existentes.
2. El temor a que un protocolo nuevo tuviera problemas imprevistos.
3. El deseo de terminar el trabajo antes de que cambiara la tecnología.

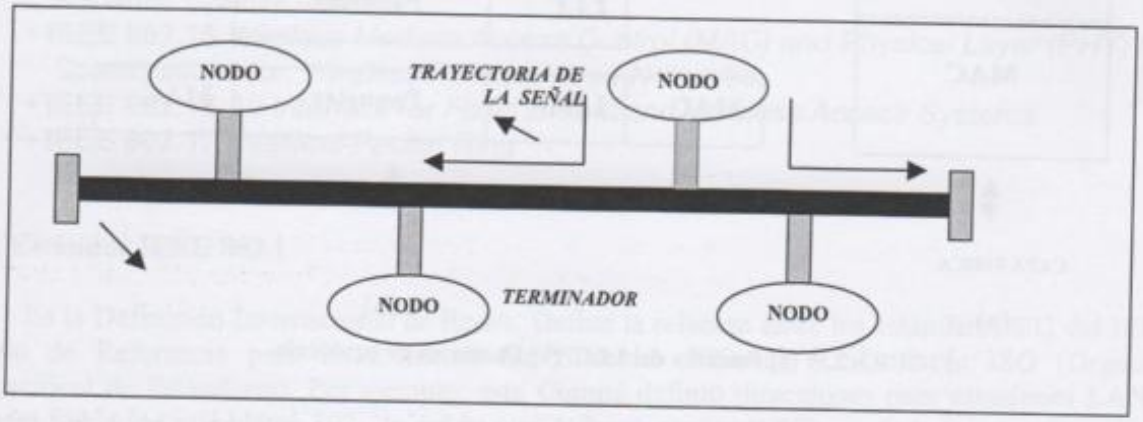
Este estándar fue desarrollado originalmente por *Xerox* y *Dec* como forma de solucionar el problema del cableado de redes. Sus inventores fueron Robert Metcalfe y David Boggs. Según Robert Metcalfe, el nombre Ethernet proviene de la palabra *Ether (éter)*, la cual denomina poéticamente a un material inexistente que, según algunas antiguas teorías, llenaba el espacio y actuaba como soporte para la propagación de la energía a través del universo.

[21] ® Marca registrada de Xerox.

En un principio se pensó en utilizar el cable coaxial (ver **figura 2.10**) para el cableado de este tipo de redes, aunque hoy en día se pueden utilizar otros tipos de cables (ver apartado **2.5. Formas de cableado**) La velocidad de transmisión de la información por el cable es de 10 Mbps.

Si se utiliza cable coaxial grueso, se pueden hacer hasta 4 tramos de cables (unidos con repetidores) de un máximo de 560 metros cada uno. Las computadoras se conectan al cable mediante transceptores, siendo la distancia máxima entre el transceptor y el ordenador de 15 metros. Sólo puede haber computadoras en tres de los cuatro tramos, siendo el número máximo de estaciones de trabajo de 100 por tramo.

Si se utiliza cable coaxial fino, no hacen falta dispositivos transceptores, pudiendo conectarse el cable del ordenador al cable de la red con simples conectores en T. El número máximo de tramos en este caso es de 5, siendo la longitud máxima de cada tramo de 205 metros. Los tramos se unen mediante el empleo de repetidores de señal. Sólo puede haber computadoras en tres de los tramos, siendo el número máximo de estaciones de trabajo de 30 por tramo.



El protocolo CSMA/CD

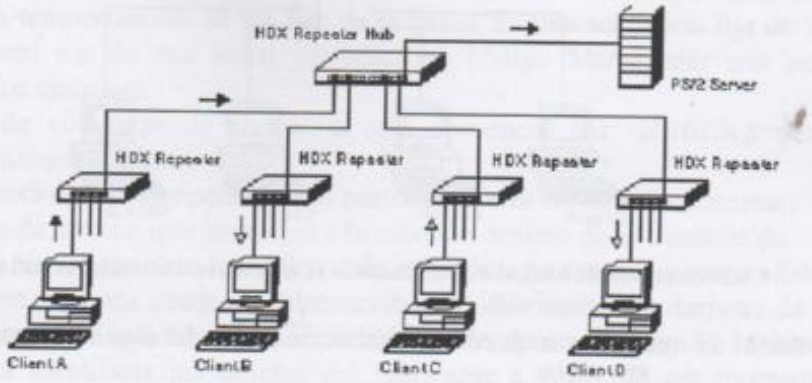
Específicamente el protocolo se refiere tanto al método de acceso al medio que utiliza este tipo de redes conocido como CSMA/CD (***Carrier Sense Multiple Access with Collision Detection***), como a las distintas implementaciones físicas que surgieron del mismo. Es decir que se refiere a las capas 1 (Física) y 2 (Enlace de datos) del Modelo OSI.

El principio de funcionamiento del protocolo lo podemos resumir en los siguientes modos de operación:

Operación en modo half duplex

El método de acceso CSMA/CD es el procedimiento por el cual dos o más estaciones acceden a un medio conductor compartido. En él, la estación que quiere transmitir espera (*defers*) hasta que haya un período libre en el medio conductor, o sea que no haya otra estación transmitiendo.

Recién allí comienza a transmitir en forma serial (bit a bit) el mensaje que tenía esperando. Toda la señal le llega a todos los host conectados al medio conductor compartido.



Lo que el host a transmite le llega al servidor y a todos los otros clientes

Si luego de iniciada la transmisión, el mensaje colisiona con el enviado por otra estación, cada una de ellas sigue transmitiendo un mensaje por un intervalo predefinido de tiempo con la intención de que la colisión se propague por todo el sistema (*Jam*).

Las estaciones deben contenerse antes de volver a intentar transmitir (*backoff*) por un período aleatorio de tiempo. Este debe ser un número entero de intervalos de tiempo aleatorio, calculado como:

$$0 < r < 2^k \quad \text{donde } k = \min(n, 10)$$

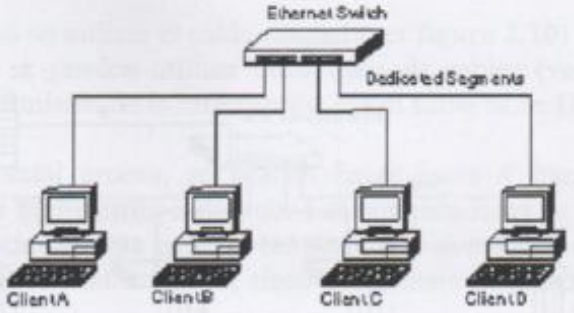
La función que genera este número r debe procurar una correlación mínima entre los tiempos de espera de las demás estaciones que existen en el medio.

Operación en modo full duplex

Este tipo de operación proporciona comunicación simultánea entre dos estaciones a través de un enlace punto a punto (canal dedicado). Así no se requiere que la estación transmisora monitoree el canal, ni se contenga hasta que detecte el canal libre. Este modo sólo puede operar si:

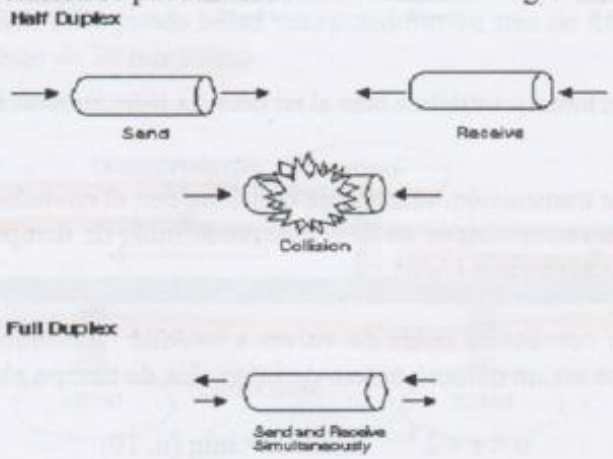
- El medio físico es capaz de transmitir y recibir simultáneamente sin interferencias
- Hay dos estaciones que trabajen exactamente en modo full duplex en los extremos de un enlace punto a punto (no sería necesario el método CSMA/CD).
- Ambas Estaciones deben ser capaces de funcionar en modo full duplex

Esto se logra conectando las estaciones de trabajo a un switch. La tasa de transmisión de bits que se logra es del doble del anterior modo.



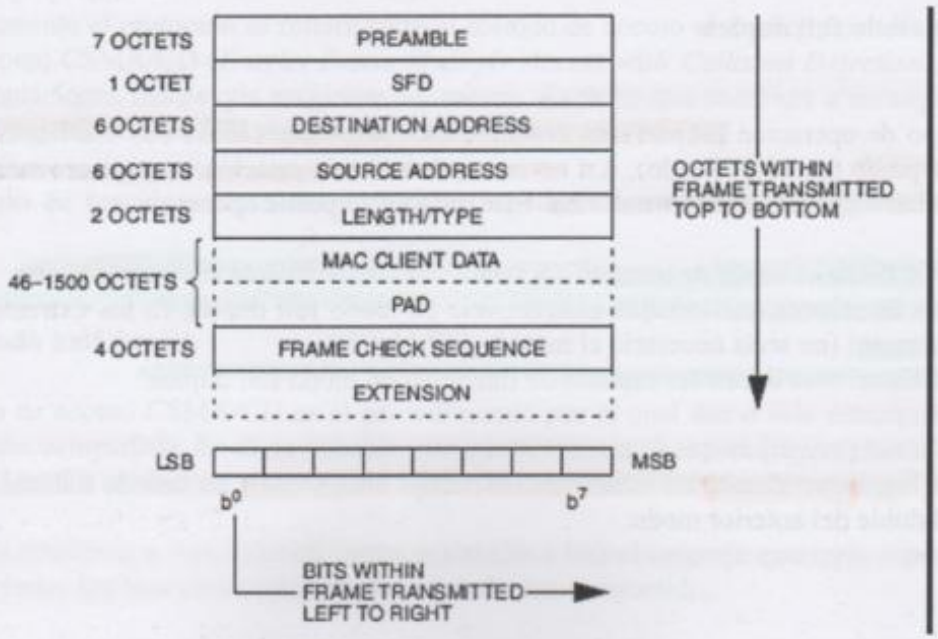
Cada conexión de host al switch constituye un enlace dedicado; es full duplex

Ambos modos de operación se pueden visualizar a través del siguiente gráfico:



Formato de la Trama MAC

Una trama IEEE 802.3 consta de los siguientes campos:



1. El preámbulo tiene la finalidad de sincronizar los circuitos de la capa física de las estaciones receptoras con la temporización de los bits de la trama. Es una secuencia fija de 7 Bytes de 1 y 0 alternados, lo cual me da una señal periódica en código Manchester que permite lograr el sincronismo de los circuitos.
2. El delimitador de comienzo de trama: es una secuencia fija: 10101011 que indica que a continuación comienza la trama.
3. El campo de direcciones se compone de dos partes similares de 48 bits cada una:
   a. Dirección de destino que identifica a la estación destino de la transmisión
   b. Dirección de origen que identifica a la estación que inició la trama. Este campo queda grabado en la placa desde su fabricación. Los fabricantes de tarjetas de interfaz de red (NIC) tienen que solicitar al IEEE la asignación de un número de 24 bits (3 Bytes), que sirve para identificar las tarjetas del fabricante a partir de ese momento. Es el **OUI** ("*Organizationally Unique Identifier*"), tembién conocido como **código de vendedor**. A continuación cada fabricante añade a su OUI otros 24 bits, que forman el número de serie de la NIC, hasta totalizar los 48 bits. Los 6 Bytes de los campos de dirección suelen indicarse en formato hexadecimal, como por ejemplo: 00-10-A4-01-FF-F1.
4. El campo tipo/longitud tiene dos posibles significados dependiendo del valor que contenga:
   a. Si el valor que ese campo contiene es menor o igual que el máximo valor permitido para el tamaño de una trama (*Maximum Transmission Unit* (MTU) 1500 Bytes), entonces el campo indica el tamaño que posee el campo que le sigue (o sea el campo datos).
   b. Si el valor que contiene ese campo es mayor a 1536 en decimal (o 0600 en hexadecimal), entonces el campo indica el protocolo MAC cliente de esa trama.
   Por ejemplo: 0x0600: XNS (Xerox)
   0x0800 IP (Internet Protocol)
   0x6003 DECNET
5. El campo de datos contiene los datos de protocolos de capas superiores y se brinda un servicio totalmente transparente.
   i. Posee un tamaño máximo indicado por la implementación del protocolo en uso de 1500 Bytes
   ii. Posee un mínimo requerido para el correcto funcionamiento del CSMA/CD (de no lograrlo se debe utilizar el siguiente campo que es de relleno)
6. En caso de que el tamaño del campo de datos sea menor que el requerido para el correcto funcionamiento del protocolo MAC, se debe implementar un campo de relleno, al final del campo de datos (y antes del FCS) que será de 46 a 0 Bytes
7. El campo Suma de Comprobación (FCS) consta de 4 Bytes y utiliza un procedimiento de CRC que debe ser similar tanto en el emisor como en el receptor, computable sobre el contenido de todos los campos de la trama (excepto el preámbulo y el SFD).

En total la trama MAC debe tener una longitud igual o mayor a 64 Bytes y menor o igual a 1518 Bytes (sin contar el preámbulo ni el SFD).

Procedimiento de generación del CRC

El último campo de la trama MAC es la Secuencia de Comprobación de Trama (FCS) Matemáticamente se genera con el siguiente polinomio:

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$$

El procedimiento es el siguiente:

a) Los primeros 32 bits de la trama se complementan a dos
b) Los "n" bits de la trama son considerados los coeficientes de un polinomio M(x) de grado (n-1). El primer bit del campo dirección MAC de destino es considerado el coeficiente del término x^{n-1} y el último bit del campo de datos es el coeficiente del término x^0.
c) El polinomio M(x) es multiplicado por x^{32} y dividido por G(x) produciéndose un resto R(x) que será de grado menor a 31
d) Los coeficientes de R(x) son considerados una secuencia de 32 bits
e) Esta secuencia se complementa a dos y es el resultado del CRC, que se coloca en el campo FCS de la trama enviada.

El receptor realiza el mismo procedimiento con la trama que recibe y compara el campo FCS calculado por él con el que llega en la trama. Si son iguales supone que no se han producido errores en la transmisión; si son distintos descarta la trama que le llegó

ERRORES EN LAS TRAMA

Además del ya mencionado problema con el campo FCS, otros pueden ser los motivos que obliguen al receptor a descartar la trama, como:

- La longitud de la trama no concuerda con el contenido del campo longitud de la trama
- La trama que llega no contiene un número entero de Bytes
- La trama que llega está completa pero tiene un tamaño menor a 64 Bytes (512 bits). Se la llama RUNT.
- La trama que llega tiene entre 1518 y 6000 Bytes. Se la llama LONG.
- La trama que llega tiene más de 6000 Bytes. Se la llama GIANT.

Tipos de 802.3

Distintas implementaciones de la arquitectura de este estándar se han llevado a cabo hasta nuestros días. Unas de otras varían en la tasa de bits, en el medio conductor y los conectores utilizados y en la forma de codificación de la señal al enviarla por el medio. Algunas de ellas son:

Comité IEEE 802.3

10BROAD36: IEEE 802.3 Physical Layer specification a 10 Mb/s CSMA/CD LAN sobre cable de banda ancha.

1BASE5: IEEE 802.3 Physical Layer specification a 1 Mb/s CSMA/CD LAN sobre dos pares trenzados de cable telefónico

10BASE2: IEEE 802.3 Physical Layer specification a 10 Mb/s CSMA/CD LAN sobre cable coaxial fino RG 58.

10BASE5: IEEE 802.3 Physical Layer specification a 10 Mb/s CSMA/CD LAN sobre cable coaxial grueso (llamado thicknet).

10BASE-F: IEEE 802.3 Physical Layer specification a 10 Mb/s CSMA/CD LAN sobre cable fibra óptica.

10BASE-T: IEEE 802.3 Physical Layer specification a 10 Mb/s CSMA/CD LAN sobre dos pares trenzados (UTP). Codificación Manchester.

IEEE 802.3u: Fast Ethernet

100BASE-X: IEEE 802.3 Physical Layer specification a 100 Mb/s CSMA/CD LAN que usa el Physical Medium Dependent (PMD) sublayer y Medium Dependent Interface (MDI) del grupo de estándares ISO/IEC 9314.
100BASE-FX: IEEE 802.3 Physical Layer specification a 100 Mb/s CSMA/CD LAN sobre dos fibras ópticas (multimodo 50/125um, 60/125um o monomodo) y 1300nm de longitud óptica. Los conectores pueden ser: SC, Straight Tip (ST) o Media Independent Connector (MIC).
100BASE-T: IEEE 802.3 Physical Layer specification a 100 Mb/s CSMA/CD LAN. Utiliza la Codificación 4B5B
100BASE-T2: IEEE 802.3 specification a 100 Mb/s CSMA/CD LAN sobre dos pares UTP Categoría 3 o mejor, balanceados. Codificación PAM 5X5
100BASE-T4: IEEE 802.3 Physical Layer specification a 100 Mb/s CSMA/CD LAN sobre cuatro pares de cables trenzados Categoría 3, 4, y 5 (UTP). Utiliza la Codificación 8B6T
100BASE-TX: IEEE 802.3 Physical Layer specification a 100 Mb/s CSMA/CD LAN sobre dos pares UTP Categoría 5 o cableado shielded twisted-pair (STP)

IEEE 802.3z: Gigabit Ethernet

1000BASE-CX: 1000BASE-X sobre cable de cobre especialmente blindado y balanceado categoría 5e
1000BASE-LX: 1000BASE-X usa un emisor láser (long wavelength laser de 1300nm) sobre fibra multimodo (62.5/125µm) y monomodo a 1350 nm.
1000BASE-SX: 1000BASE-X usa un emisor láser (short wavelength laser de 850nm) sobre fibra multimodo (62.5/125 µm)
1000BASE-T: IEEE 802.3 Physical Layer specification a 1000 Mb/s CSMA/CD LAN que usa dos pares UTP balanceados Categoría 5. Codificación 4D-PAM5
1000BASE-X: IEEE 802.3 Physical Layer specification a 1000 Mb/s CSMA/CD LAN que usa un nivel Físico derivado de ANSI X3.230-1994. Codificación 8B10B

IEEE 802.3ae: 10Gigabit Ethernet

10GBASE-LX4: IEEE 802.3ae Physical Layer specification a 10 Gb/s CSMA/CD LAN y MAN. Codificación 8B10B
10GBASE-R: IEEE 802.3ae Physical Layer specification a 10 Gb/s CSMA/CD LAN y MAN. Codificación 64B66B. Familia compuesta por: 10GBASE-SR, 10GBASE-LR, y 10GBASE-ER.
10GBASE-W: IEEE 802.3 Physical Layer specification a 10 Gb/s CSMA/CD LAN y MAN. Codificación 64B66B y 50 WIS Wan Interface Sublayer. Familia compuesta por: 10GBASE-SW, 10GBASE-LW, y 10GBASE-EW.

Temporizaciones

El funcionamiento del protocolo CSMA/CD requiere que las estaciones antes de transmitir escuchen el canal libre durante un tiempo determinado: el IFG. Asimismo luego de colisionar deben retraerse un tiempo: el backoff.

Las distintas implementaciones del estándar poseen distintos valores de los parámetros de tiempo:

Parameters	Values	Values	Values
slotTime	512 bit times	512 bit times	4096 bit times
interFrameGap	9.6 μs	0.96 µs	0.096 µs
attemptLimit	16	16	16
backoffLimit	10	10	10
jamSize	32 bits	32 bits	32 bits
maxUntaggedFrameSize	1518 octets	1518 octets	1518 octets
minFrameSize	512 bits (64 octets)	512 bits (64 octets)	512 bits (64 octets)
burstLimit	not applicable	not applicable	65 536 bits

Estos valores de temporizadores hacen que al diseñar una red LAN que use el protocolo 802.3 se deban respetar algunas consideraciones, resumidas en la siguiente regla mnemotécnica:

5 – 4 – 3 – 2 – 1

Se pueden instalar 5 segmentos, unidos por 4 repetidores (hubs); sólo en tres de ellos puede haber estaciones de trabajo, mientras que 2 de ellos deben servir sólo para unir repetidores. Entre todos forman un único dominio de colisión

2.4.3.2. Estándar IEEE 802.3u: Fast Ethernet (Ethernet rápido)

Precisamente como veremos en el siguiente apartado, el estándar IEEE 802.5 (*token ring*) tiene dos ambientes de productos ofrecidos a 4 Mbps y a 16 Mbps. El comité IEEE (Ethernet CSMA/CD), siente la necesidad de una segunda alternativa para la tecnología de la red 10 Mbps.

El concepto principal en que se basa el Ethernet rápido es sencillo: mantener todos los formatos de los paquetes, interfaces y reglas de procedimientos anteriores, y simplemente reducir el tiempo de bit de 100 *nseg* a 10 *nseg*. Técnicamente habría sido posible copiar el 10 Base-5 o el 10 Base-2 y aun detectar colisiones a tiempo con sólo reducir la longitud máxima del cable por el factor de 10. Pero sin embargo, las ventajas del 10 Base-T fueron tan contundentes que el Ethernet rápido se basa completamente en este diseño. Por lo tanto todos los sistemas de Ethernet rápido usan concentradores; no se permiten cables de derivación múltiple con derivaciones vampiro ni conectores BNC.

2.4.3.2.1. Objetivos básicos de Ethernet rápido

- 100 Mbps en el escritorio.
- Preservar la inversión del cableado existente.
- Soporte de redes de campo existentes y futuras.
- Bajo costo.
- Soporte de aplicación multimedia.
- Rápida adopción de mercado.
- Influencia existente del protocolo estándar de control de acceso al medio (MAC).
- Proveer migración a bajo costo.

Algunas variantes en cuanto al cableado y el tipo de codificación empleado en la señal son:

TABLE 13.2 IEEE 802.3 100BASE-T physical layer medium alternatives.

	100BASE-TX		100BASE-FX	100BASE-T4
Transmission medium	2 pair, STP	2 pair, Category 5 UTP	2 optical fibers	4 pair, Category 3, 4, or 5 UTP
Signaling technique	4B5B, NRZI	4B5B, NRZI	4B5B, NRZI	8B6T, NRZ
Data rate	100 Mbps	100 Mbps	100 Mbps	100 Mbps
Maximum segment length	100 m	100 m	100 m	100 m
Network span	200 m	200 m	400 m	200 m

2.4.3.3. Estándar IEEE 802.3z Ethernet a 1 Gbps

También conocida como Gigabit Ethernet, se trata de un tipo de red de área local que fue estandarizada en Junio de 1988. La identificación recibida por el estándar ha sido la de IEEE 802.3z. Básicamente es una evolución de 100 base T pero con velocidad de transmisión en línea de 1 Gbps.

La red mantendría el protocolo CSMA/CD, pero como sucede en el 100 base T la distancia de los canales deberían reducirse en proporción al aumento de la velocidad, si se quiere mantener el tamaño mínimo de trama en 64 bits con el fin de detectar las colisiones, y en este caso la longitud del canal sería de 20 metros, lo que no es muy operativo.

La solución adoptada es incrementar el tamaño de trama mínimo a 512 bytes mediante la inclusión de relleno en las tramas de tamaño menor, aunque con la consiguiente pérdida de eficacia. El problema que podría aparecer con el envío de paquetes pequeños, se resuelve mediante la implementación de una característica denominada "packet bursting" que permite a los servidores conmutadores y otros dispositivos entregar ráfagas de paquetes pequeños.

El uso previsto de este tipo de red será principalmente la conexión de conmutadores, a modo de troncal. En un futuro cercano se plantea la posibilidad de realizar migraciones de los protocolos Ethernet actuales a Gigabit Ethernet, cuatro de los posibles escenarios son:

- Actualización de enlaces entre conmutadores y servidores para obtener enlaces de alta velocidad entre ellos.
- Actualización de enlaces entre conmutadores 10 / 100 / 1000 para conseguir enlaces de 1Gbps entre ellos.
- Actualización de troncales Fast Ethernet conmutadas agregando un conmutador Gigabit Ethernet.
- Actualización de una red troncal FDDI[22] conectando *hubs* FDDI con conmutadores Gigabit Ethernet.

[22] Interface de Distribución de Datos de Fibra. En Inglés: Fiber Disrtibuted Data Interface.

2.4.4. Estándar IEEE 802.4: Token Bus

El estándar 802.4, describe una LAN llamada *token bus* (bus de ficha). Físicamente, es un cable lineal o en forma de árbol al que se conectan las estaciones. Las estaciones están organizadas lógicamente en forma de anillo, donde cada estación conoce la dirección a su "izquierda" y a su "derecha". Cuando sé inicializa el anillo lógico, la estación de número más alto puede enviar el primer marco. Hecho esto, pasa el permiso a su vecino inmediato enviándole un marco de control especial llamado ficha (*token*). La ficha se propaga alrededor del anillo lógico, teniendo permiso de transmitir marcos sólo quien tiene la ficha. Dado que sólo una estación a la vez tiene la ficha, no ocurren colisiones.

Un punto importante a notar es que no es importante el orden físico en que están conectadas las estaciones al cable. Dado que el cable inherentemente es un medio de difusión, todas las estaciones reciben todos los marcos, descartando los que no están dirigidos a ellas. Cuando una estación pasa la ficha, envía un marco de ficha dirigido específicamente a su vecino lógico en el anillo, sin importar la ubicación física de esa estación en el cable.

Esta LAN *(Token Bus)* emplea equipo de televisión por cable altamente confiable, que se puede obtener sin necesidad de pedidos de numerosos proveedores. Es más determinístico que el 802.3, aunque las pérdidas repetidas de la ficha en momentos críticos pueden introducir más incertidumbre de la que están dispuestos a admitir sus partidarios. Esta LAN puede manejar marcos mínimos cortos. Ver **figura 2.12.**

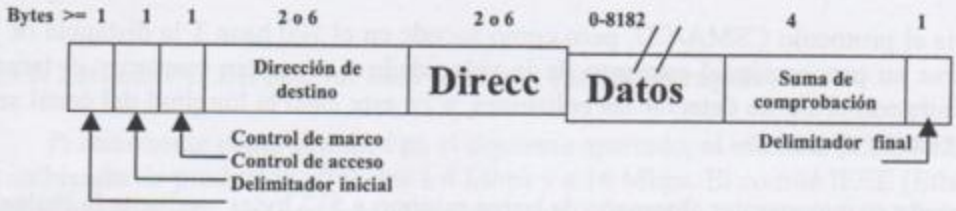


FIGURA 2.12: Formato de marco de 802.4.

El *token bus* también reconoce prioridades y puede configurarse para proporcionar una fracción garantizada del ancho de banda a tráfico con prioridad alta como la voz digitalizada. Esta LAN también tiene rendimiento y eficiencia excelentes con alta carga volviéndose efectivamente TDM[23]. Por último, el cable de banda ancha puede manejar múltiples canales, no sólo de datos sino también de voz y televisión.

Por el lado negativo, los sistemas de banda ancha emplean mucha ingeniería analógica e incluyen módems y amplificadores de banda amplia. El protocolo es extremadamente complicado y tiene un retardo sustancial cuando la carga es baja. Por otra parte, el *token bus* no es idóneo para las implementaciones de fibra óptica y tiene una base instalada de usuarios pequeños.

[23] Multiplexado por División en el Tiempo. En Inglés: time División Multiplex.

2.4.5. Estándar IEEE 802.5: Token Ring

Las redes en anillo no son nada nuevo, pues se han utilizado desde hace mucho para redes locales como de área extendida. Entre sus muchas características atractivas está el que un anillo no es realmente un medio de difusión, ver **figura 2.13** sino un conjunto de enlaces punto a punto individuales que, coincidentemente, forman un círculo. Los enlaces punto a punto implican una tecnología bien entendida y probada en el campo que puede operar un par trenzado, cable coaxial y fibra óptica. La ingeniería de anillos es casi completamente digital. Un anillo también es equitativo y tiene un límite superior conocido de acceso al canal.

Un asunto fundamental en el diseño y análisis de cualquier red de anillos es la longitud física de un bit. Si la tasa de datos del anillo es de *R Mbps,* se emite un bit cada *1/R µseg.* con una velocidad de propagación de señal tópica de unos *200 m/µseg,* cada bit ocupa *200 /R* metros del anillo. Esto significa, por ejemplo, que un anillo de 1 Mbps cuya circunferencia es de 1000 metros puede contener sólo 5 bits a la vez.

En un Token Ring (anillo con fichas), circula un patrón de bit especial, llamado ficha (*token*), (ver **figura 2.14**) alrededor del anillo cuando todas las estaciones están inactivas.

Cuando una estación quiere transmitir un marco, debe tomar la ficha y retirarla del anillo, antes de transmitirla. Esta acción se lleva a cabo invirtiendo un solo bit de la ficha de 3 bytes, lo que instantáneamente la convierte en los tres primeros bytes de un marco MAC[24] de datos normal, ver **figura 2.15**. Debido a que sólo hay una ficha, hay sólo un canal de la misma manera en que lo resuelve el *token bus*.

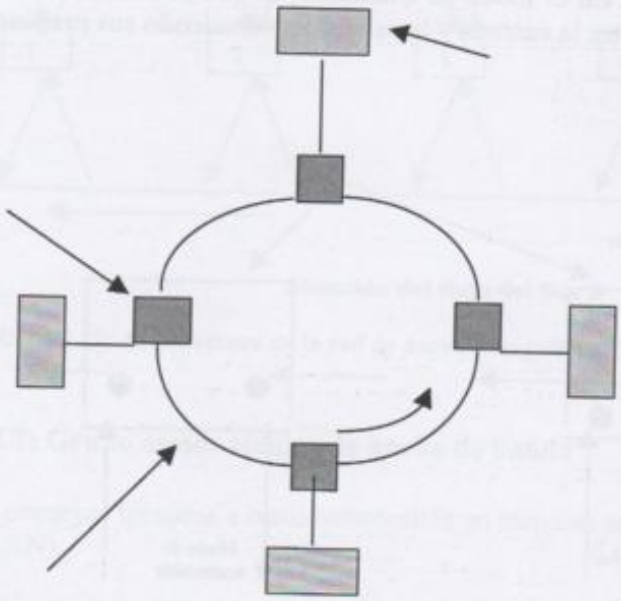


FIGURA 2.13: Token Ring.

[24] Control de Acceso al Medio. En Inglés: Media Access Control.

Una implicación del diseño del *token ring*, es que el anillo mismo debe tener un retardo (*delay*) suficiente para contener una ficha completa que circule cuando todas las estaciones están inactivas. El retardo tiene dos componentes: el retardo de un bit introducido por cada estación y el retardo de propagación de la señal.

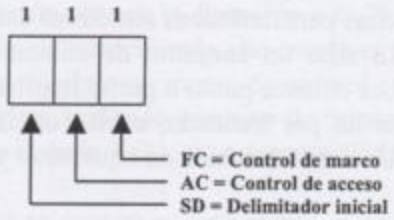


FIGURA 2.14: Formato de marco del testigo.

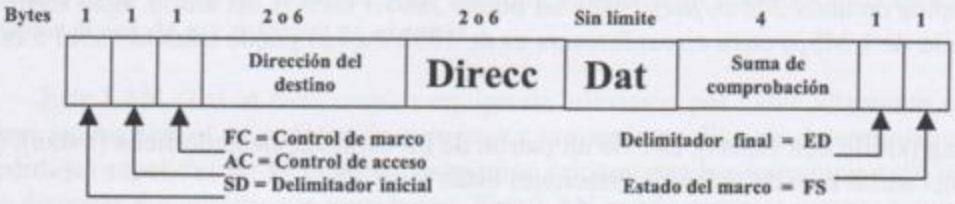


FIGURA 2.15: Formato de marco de 802.5.

Las interfaces del anillo tienen dos modos operativos, escuchar y transmitir. En el modo de escuchar, los bits de entrada simplemente se copian en la salida, con un retardo de un tiempo de bit, como se muestra en la **figura 2.16.** En el modo de transmitir, al que se entra una vez que se tiene la ficha, la interfaz rompe la conexión entre la entrada y la salida, introduciendo sus propios datos en el anillo.

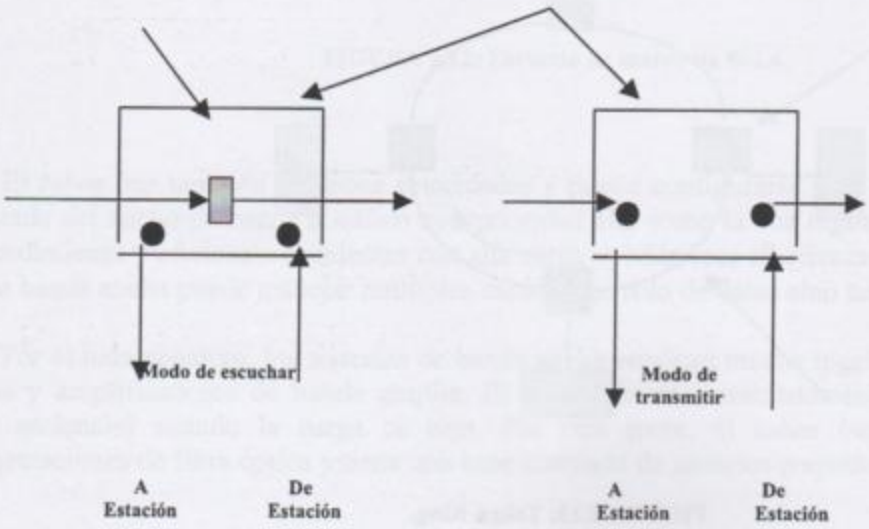


FIGURA 2.16: Modo de Escuchar.

2.4.6. Estándar IEEE 802.6: Bus doble de colas distribuidas

Ninguna de las LAN vistas hasta ahora es adecuada para usarse como MAN[25]. Las limitaciones de longitud del cable y los problemas de desempeño cuando se conectan miles de estaciones, las limitan a áreas de extensión pequeña. Para redes que cubren una ciudad completa, IEEE definió una MAN, llamada **DQDB** (*Distributed Queue Dual Bus*), como el estándar 802.6.

En la **figura 2.17** se ilustra la geometría básica del 802.6. Dos buses unidireccionales paralelos serpentean a través de la ciudad, con estaciones conectadas a ambos buses en paralelo. Cada bus tiene un *head-end*. Cuando la célula llega al final, sale del bus. Cada célula lleva un campo de carga de 44 bytes, haciéndola compatible con algunos modos AAL[26]. Cada célula contiene *dos bits* de protocolo, *ocupado*, que se establece para indicar que la célula está ocupada, y *solicitud*, que puede establecerse cuando una estación quiere hacer una solicitud. Para transmitir una célula, la estación necesita saber si el destino está a la derecha o la izquierda de ella. Si el destino está a la derecha utiliza el *bus A,* sino utiliza el *bus B*. Los datos se introducen en cualquiera de los dos buses usando un circuito *OR* alambrado, de manera que la falla de una estación no desactive la red.

A diferencia de los otros protocolos de LAN 802, EL 802.6 no es ávido. En todos los demás si una estación tiene la oportunidad de enviar, lo hará. Aquí las estaciones se ponen en cola en el orden en que van quedando listas para enviar y transmitir, en orden FIFO[27] (el que entra primero sale primero).

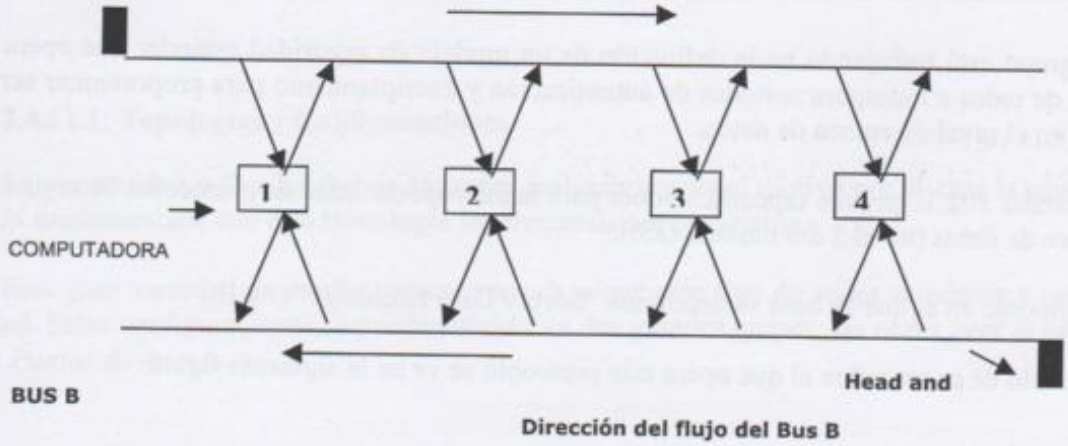


FIGURA 2.17: Arquitectura de la red de área metropolitana DQDB.

2.4.7. Estándar IEEE 802.7: Grupo asesor técnico de ancho de banda

Este comité provee consejos técnicos a otros subcomités en técnicas sobre redes LAN o MAN de banda ancha (Broadband LAN).

[25] Red de Área Extendida. En Inglés: Wide Area Network.
[26] Capa de Adaptación ATM. En Inglés: ATM Adaptation Layer.
[27] En Inglés: First In First Out.

2.4.8. Estándar IEEE 802.8: Grupo asesor técnico de fibra óptica

Provee consejo a otros subcomités en redes por fibra óptica como una alternativa a las redes basadas en cable de cobre. Los estándares propuestos están todavía bajo desarrollo.

2.4.9. Estándar IEEE 802.9: Redes integradas de voz y datos

El grupo de trabajo del IEEE 802.9 trabaja en la integración de tráfico de voz, datos y video para las LAN 802 y Redes Digitales de Servicios Integrados (RDSI[28]). Los nodos definidos en la especificación incluyen teléfonos, computadoras y *codificadores /decodificadores* de video (*codecs*).

La especificación ha sido llamada: Ethernet IsoEnet: IEEE 802.9 IVDLAN (Integrated Video and Data Local Area Network) Datos y Voz Integrados (IVD). El servicio provee un flujo multiplexado que puede llevar canales de información de datos y voz conectando dos estaciones sobre un cable de cobre en par trenzado. Varios tipos diferentes de canales son definidos, incluyendo full duplex de 64 Kb/s sin switcheo, circuito switcheado, o canales de paquete switcheados.

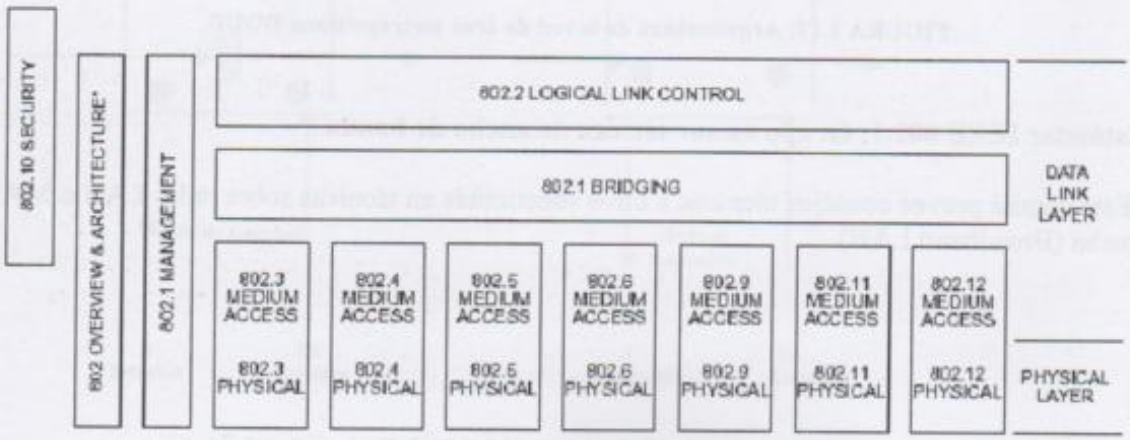
2.4.10. Estándar IEEE 802.10: Grupo asesor técnico de seguridad de redes

Este grupo está trabajando en la definición de un modelo de seguridad estándar que opera sobre una variedad de redes e incorpora métodos de autenticación y encriptamiento para proporcionar servicios de seguridad en el nivel de enlace de datos.

El estándar 802.10 provee especificaciones para la interoperabilidad de protocolos de seguridad a nivel de enlace de datos (nivel 2 del modelo OSI).

El protocolo en el que se basa se denomina "Secure Data Exchange" (SDE).

El modelo de capas sobre el que opera este protocolo se ve en la siguiente figura:



[28] En Inglés: Integrated Services Distributed Network.

2.4.11. Estándar IEEE 802.11: Redes inalámbricas (WLAN)

Este comité está definiendo estándares para redes inalámbricas. Está trabajando en la estandarización de medios como la radio transmisión por espectro ensanchado (DSSS), radio de banda angosta (OFDM), infrarrojo, y transmisión sobre líneas de energía.

La especificación original, conocida como IEEE 802.11 utiliza el método de acceso al medio conocido como CSMA/CA y una técnica de modulación de espectro ensanchado llamada secuencia directa (DSSS). Posteriores versiones del estándar establecieron distintas alternativas para la capa física pero manteniendo el mismo método de acceso al medio.

En el siguiente cuadro podemos ver un resumen de las variantes de WLAN

Especificación	Estatus	Máxima tasa de bits	Frecuencia de operación	Técnica de Modulación
IEEE 802.11	Especificación original adoptada por la mayoría de fabricantes de WLANs	2 Mbps	2.4 GHz	FSSS / DSSS
IEEE 802.11b	Compatible con Wi-Fi	11 Mbps	2.4 GHz	DSSS
IEEE 802.11a	Reducido alcance	24 - 54 Mbps	5.0 GHz	OFDM
IEEE 802.11g	Mayor alcance y menor consumo	24 - 54 Mbps	2.4 GHz	DSSS /OFDM

2.4.11.1: Topologías y Configuraciones

La versatilidad y flexibilidad de las redes inalámbricas es el motivo por el cual la complejidad de una LAN implementada con esta tecnología sea tremendamente variable.

Esta gran variedad de configuraciones ayuda a que este tipo de redes se adapte a casi cualquier necesidad. Estas configuraciones se pueden dividir en dos grandes grupos, las *redes peer to peer* y las que utilizan *Puntos de Acceso*.

2.4.11.1.a: Peer to peer

También conocidas como **redes *ad-hoc***, es la configuración más sencilla, ya que en ella los únicos elementos necesarios son terminales móviles equipados con los correspondientes adaptadores para comunicaciones inalámbricas.

En este tipo de redes, el único requisito deriva del rango de cobertura de la señal, ya que es necesario que los terminales móviles estén dentro de este rango para que la comunicación sea posible. Por otro lado, estas configuraciones son muy sencillas de implementar y no es necesario ningún tipo de gestión administrativa de la red.

Un ejemplo sencillo de esta configuración se muestra en la siguiente ilustración.

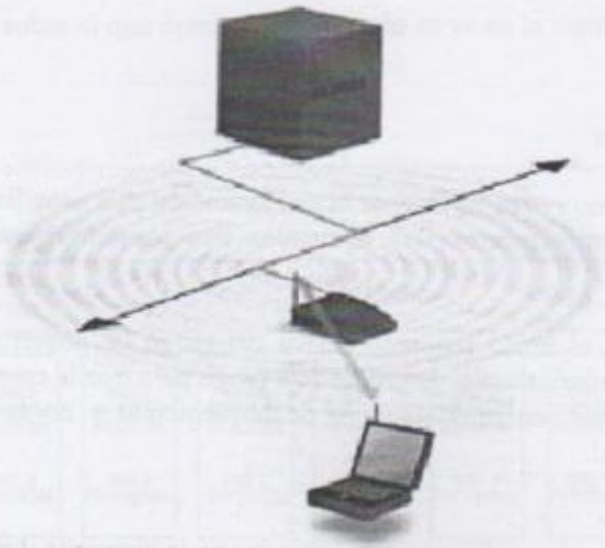
Conexión peer to peer

2.4.11.1.b: Modo infraestructura

Estas configuraciones utilizan el **concepto de celda,** ya utilizado en otras comunicaciones inalámbricas, como la telefonía móvil. Una celda podría entenderse como el área en el que una señal radioeléctrica es efectiva.

A pesar de que en el caso de las redes inalámbricas esta celda suele tener un tamaño reducido, mediante el uso de varias fuentes de emisión es posible combinar las celdas de estas señales para cubrir de forma casi total un área más extensa.

La estrategia empleada para aumentar el número de celdas, y por lo tanto el área cubierta por la red, es la utilización de los llamados ***Puntos de acceso***, que funcionan como repetidores, y por tanto son capaces de doblar el alcance de una red inalámbrica, ya que ahora la distancia máxima permitida no es entre estaciones, sino entre una estación y un punto de acceso.



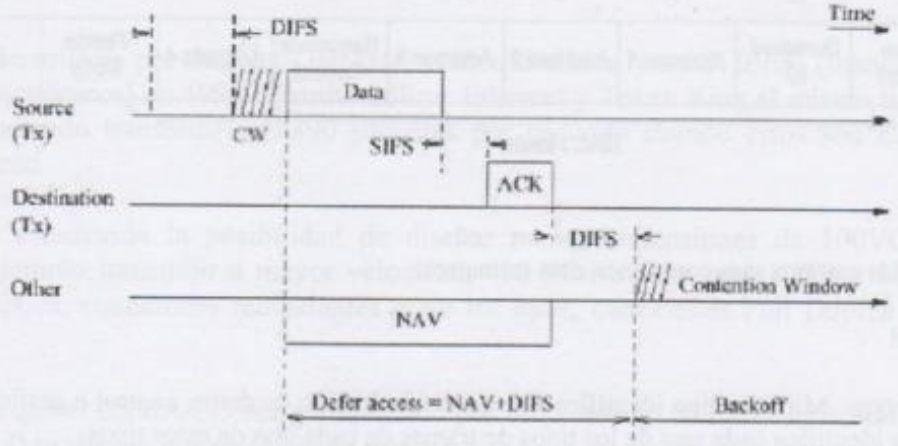
Utilización de un *Punto de acceso*

2.4.11.2: Protocolo CSMA/CA

Dos enfoques para redes inalámbricas se han planeado. En el enfoque distribuido, cada estación de trabajo controla su acceso a la red. En el enfoque de punto de coordinación, un hub central enlazado a una red cableada controla la transmisión de estaciones de trabajo inalámbricas.

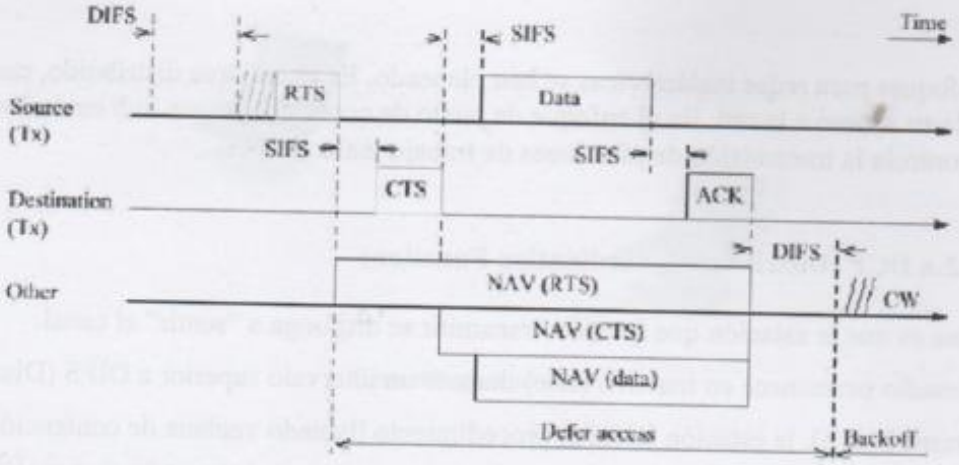
2.4.11.2.a DCF (Distributed Coordination Function)

- La idea es que la estación que necesita transmitir se disponga a "sentir" el canal.
- Si el medio permanece en inactivo (idle) durante un intervalo superior a DIFS (Disrtributed InterFrame Space), la estación inicia el procedimiento llamado ventana de contención (CW)
- Si finalizado su tiempo de CW, el medio aún sigue libre, la estación transmite
- Tras la recepción del paquete por parte de la estación destino, espera otro marco de tiempo denominado SIFS (Short InterFrame Space) y transmite el paquete ACK.
- ACK no es transmitido si hay errores en recepción
- Lógicamente se usa un sistema de detección de errores (CRC)
- Las demás estaciones calculan el vector NAV y liberan el medio



Se puede aumentar aún más la eficiencia de este protocolo si se implementa la función de alertar al destino cuando se le quiere enviar un mensaje, a través de los mensajes de RTS / CLS

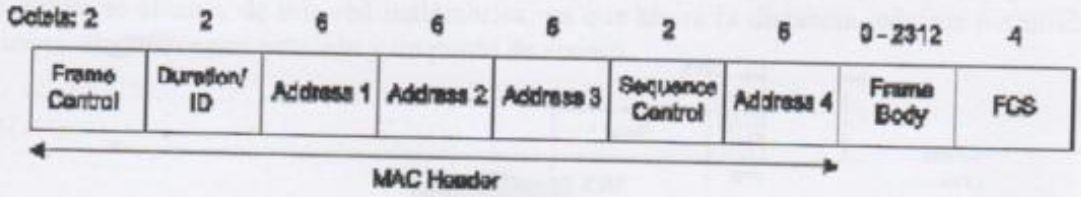
- El emisor manda un paquete RTS
- El receptor lo recibe y "si le parece" manda un paquete CTS
- Cuando el emisor lo recibe, manda la información, para que la reciba el receptor
- Se introduce información de longitud de datos
- Este mecanismo resuelve el problema de las terminales ocultas



2.4.11.2.b Formato de la trama

La trama MAC de este protocolo está definida como sigue:

- 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
- Una secuencia checksum (FCS) que contiene un código de redundancia CRC de 32 bits



En detalle los campos que componen esta trama son:

- Campo de control
  - 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.

- 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.

Las tramas MAC se pueden clasificar según tres tipos:

a) Tramas de datos.
b) Tramas de control. Los ejemplos de tramas de este tipo son los reconocimientos o ACKs, las tramas para multiacceso RTS y CTS, y ls tramas libres de contienda
c) 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.

Las redes inalámbricas o WLAN no deben pensarse como redes aisladas, sino más bien que se pueden pensar como una extensión inalámbrica de otra red LAN cableada ya que se conecta a ella a través de un Access Point

2.4.12. Estándar IEEE 802.12 (100VG Any LAN)

Fue desarrollado por Hewlett Packard y estandarizada por el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) en 1995. Permite utilizar Ethernet y Token Ring al mismo tiempo, transmite a 100 Mbit/s, pudiendo transmitir 109.890 paquetes por segundo cuando éstos son Ethernet con carga completa de la red.

Se está estudiando la posibilidad de diseñar nuevas extensiones de 100VG ANYLAN que permitan por ejemplo transmitir a mayor velocidad, 400 Mbit/s para cable UTP y 1 Gbit/s cuando se utilizan fibra óptica, conexiones redundantes entre los *hubs*, conexiones Full Duplex y transmisión en ráfagas.

Propone que el CSMA/CD sea reemplazado por un protocolo de red descrito como DPP (Demand Priority Protocol) protocolo por demanda de prioridad.

Principio de funcionamiento:

El protocolo de Acceso con prioridad bajo demanda fue desarrollado en 1995. Combina las mejores características de Ethernet (simplicidad, acceso rápido y modularidad) con las mejores de Token Ring (control robusto, sin colisiones, y retardo deterministico).

El control de la prioridad por demanda en la red está centralizado en los repetidores y está basado en el intercambio de requerimientos y o notificaciones entre los repetidores y sus nodos asociados. El acceso a la red es otorgado por el repetidor, el cual va sondeando a los nodos en una secuencia circular (cyclic round robin pool). Este protocolo de "round robin" posee dos niveles de prioridad:

- Prioridad Normal
- Alta prioridad

Dentro de cada nivel de prioridad, la selección de cuál nodo será el próximo a transmitir está determinado más por el sondeo secuencial, que por el pedido de alguno de los nodos.

IEEE 802.12 transporta tanto tramas IEEE 802.3, Ethernet como IEEE 802.5.

Topología

La topología básica es similar a la 10BASET. Cada repetidor tiene puertos locales para conexión de estaciones y puertos opcionales para cascada (esto es para extender la estrella) mediante los cuales se conecta a repetidores de niveles superiores. Esto habla de una topología jerárquica. Una red puede contener hasta 5 niveles de repetidores en cascada.

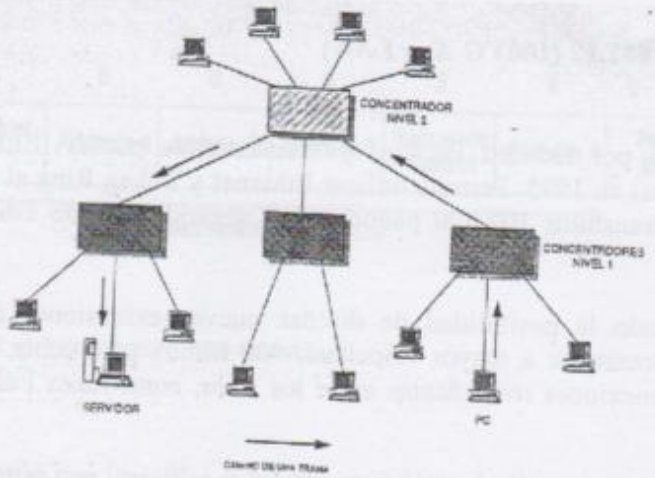


FIGURA 2.18: Red VG-AnyLAN Con niveles de concentradores

No se sabe a ciencia cierta que grado de aceptación en el mercado podrá tener este estándar ya que no es tan modular como lo es Ethernet

2.4.13. Estándar IEEE 802.13

Este estándar no se usa en la actualidad

2.4.14. Estándar IEEE 802.14: Protocolo MAC para redes HFC de CATV

Este protocolo se aplica en las redes residenciales de cable (CATV); en el se identifican tres aspectos importantes de control de acceso al medio (MAC): sincronización, modo de acceso al canal aguas arriba y resolución de colisiones.

Introducción

La tendencia actual nos lleva a considerar las redes híbridas fibra-coaxial (HFC) como las redes que en el futuro harán llegar hasta los hogares de un gran número de personas un amplio abanico de servicios y aplicaciones de telecomunicaciones, entre los que sobresalen: Vídeo por Demanda (VoD), Pago por Ver, Videófonos, servicios Multimedia y la vaca sagrada de los proveedores de servicio: el acceso a Internet a alta velocidad. Tanto los proveedores de servicio telefónico como los de TV por cable tienen un gran interés en proveer estos tipos de servicios y en tal sentido, están apuntando sus baterías hacia allá.

Las operadoras de cable que disponen de grandes redes analógicas con topología de árbol de cable coaxial, observan que con medianas inversiones pueden digitalizar la red ofreciendo no sólo distribución de video analógico, sino también servicios digitales interactivos multimedia de gran ancho de banda.

En 1994, el Grupo de Trabajo IEEE 802.14 fue formado para definir una capa física, además de una capa MAC para transferencia de datos bidireccional sobre una red HFC-CATV. Además, el IEEE 802.14 tiene como objetivo desarrollar normas para el despliegue de todo tipo de servicios de banda ancha a través de las estructuras HFC de cable.

El Grupo de Trabajo ya ha definido varios aspectos generales de lo que será el estándar para la provisión de este tipo de servicio. Debe soportar diversos tipos de tráfico como: CBR (Constant Bit Rate), VBR (Variable Bit Rate), Orientado a Conexión (CO) y No Orientado a Conexión (CL). Fuentes de tráfico en la cabecera dentro de la red deberán proveer transmisión punto a punto, punto-multipunto, multipunto a punto y multipunto-multipunto. Debe ser compatibles con tecnologías emergentes como la compresión de video y el ATM. Debe coexistir perfectamente con el modelo actual de transmisión de video analógico. Así mismo, el estándar debe proveer flexibilidad en la asignación de frecuencias hacia y desde los headend, así como también, obviamente debe permitir flujo de datos tanto simétricos como asimétricos.

Es así como el Grupo de Trabajo IEEE 802.14 ha expuesto un conjunto de criterios que se deben cumplir para lograr el éxito del estándar que quieren desarrollar. Esos criterios son los siguientes:

- Amplio Mercado Potencial: El potencial para las redes interactivas basadas en cables es tan amplio como el de la propia televisión por cable. Hoy la industria despliega un millón de cajas set-top compuestas simplemente de un sintonizador y un descrambler. Sin embargo, en este ambiente tan simple, la industria hoy tiene muchos end-stations incompatibles y técnicas de transmisión distorsionantes, cada vendedor suple sus propios sistemas. Dado la gran variedad de servicios de diferente naturaleza que se pueden prestar a través de este sistema, se hace necesario unificar esfuerzos para crear una tecnología única en la industria, un estándar. El objetivo del Grupo de Trabajo, entonces, es proveer costos balanceados en cada uno de los servicios que se prestarían.
- Arquitectura Compatible con IEEE 802: La idea fundamental de la familia de estándares IEEE 802 es la provisión de protocolos que permitan el uso de un medio común, compartido por muchos usuarios. El propósito del trabajo del grupo CATV se adhiere muy bien a este paradigma ya que la

red de distribución de CATV es un medio compartido. Por razones de fiabilidad, facilidad de mantenimiento y uso inadecuado de medios que de uso compartido ha habido una evolución del campo LAN hacia medios radiados no compartidos, pero seguiría siendo necesaria la presencia del hub. En tal sentido, el estándar propuesto debe estar conformado por arquitectura 802 y debe soportar la provisión de servicios de datos 802.2.

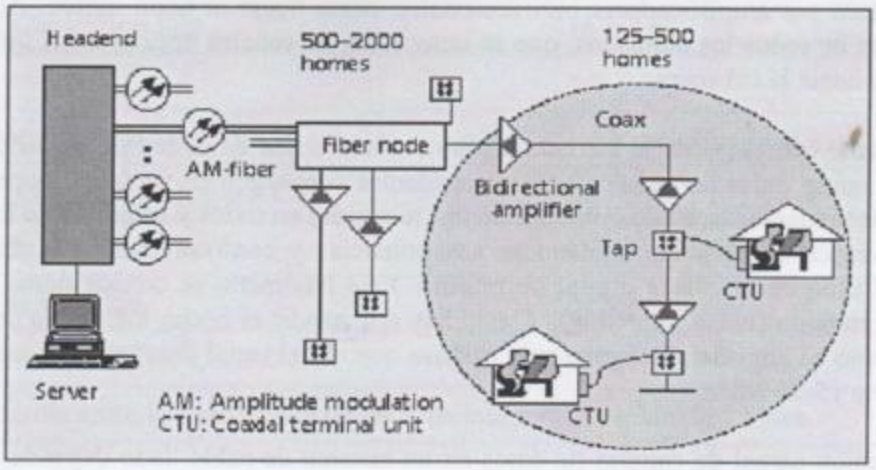
- Marcada Identidad: Cualquier trabajo que provea protocolos optimizados para múltiples servicios sobre sistemas CATV no debe carecer de una marcada identidad. Varios protocolos (802.4, 10Broad36) estaban cerca de ser estandarizados para este tipo de medio físico, pero ellos no trabajan en este ambiente por las siguientes razones:
- Distancia: Las redes de distribución de CATV cubren distancias por encima de los 80 kms.
- Compatibilidad de Servicios: Ninguno de los protocolos existentes soportan ambientes multiservicios (CBR, VBR, tráfico desbordado).
- Equipamiento del Consumidor: Los consumidores podrían cambiar sus equipos frecuentemente rompiendo con los esquemas que asumían que todas las unidades de red deberían estar continuamente encendidas.
- Ambiente: Las redes de distribución de cable existentes están sustancialmente subdivididos en asignación de frecuencias, ruidosidad y tienen ambientes operacionales que no están adecuadamente direccionados por los esquemas existentes.
- Grandes números de estaciones: Algunas plantas de distribución de CATV hoy soportan decenas de miles de usuarios activos simultáneamente. No existen estándares que direccionen tan grandes comunidades como las que se encuentran en esas plantas.
- Factibilidad Técnica: Presentaciones del Grupo de Estudio de Protocolos de CATV, indican que la factibilidad técnica es alcanzable. Mucha de la tecnología necesaria está siendo desarrollada, como la transmisión de material de video comprimido, tasas de transmisión contínuas aguas arriba y aguas abajo en las cuales se han comprobado velocidades de 43 Mbps y 10 Mbps, respectivamente dentro de los 6 Mhz de un canal de Televisión.
- Factibilidad Económica: La convergencia de la industria de la computación con las industrias de la televisión y la telefonía está liderando el desarrollo de cajas set-top con el poder computacional de las mas avanzadas estaciones de trabajo, que son necesarias para tareas de compresión y decompresión de video. Se presume que estos equipos estarán al alcance del consumidor con bajos precios.

Arquitectura de una red de CATV

La arquitectura de Redes Híbridas fibra-coaxial (HFC), en las que las fibras y los cables coaxiales son usados para transportar señales multiplexadas para un grupo de 500 hasta 2000 subscriptores, esta convirtiéndose en el estándar de la industria de CATV y provee alrededor de 800 MHz de ancho de banda a los subscriptores. Esto permite distribuir canales de video que requieren alrededor de 6 MHz de ancho de banda.

La arquitectura HFC está comenzando a considerarse como una infraestructura para transmitir comunicación bidireccional. Por la asignación de frecuencias a los canales de TV (la portadora del canal 2 se sitúa entre 54 y 60 MHz), es que se dispone de un residuo (de unos 50 MHz de ancho de banda), lo cual puede ser aprovechado para enviar y/o recibir datos, entre los usuarios y la cabecera.

Debido a que la arquitectura no contiene elementos conmutadores en la instalación, y únicamente requiere conversores ópticos/eléctricos y eléctricos/ópticos, amplificadores, y fuente de poder, el costo de instalación es relativamente bajo.



Está arquitectura posee las siguientes características:

- Topología de árbol y ramas.
- Canales aguas arriba y aguas abajo asimétricos.
- Distribución de usuarios en torno a un concentrador.

Un grupo de 500 hasta 2000 hogares subscritos son servidos por una fibra que va desde la cabecera a un nodo de fibra. Las señales son distribuidas eléctricamente a los hogares que están dentro del área de servicio de un nodo de fibra. De 125 a 500 subscriptores están adheridos a un segmento de cable coaxil de casi 5 Km (4,82 Km).

Las estaciones están adheridas a transmisores de cable y la recepción de señal de TV se realiza sobre frecuencias separadas de la de datos. Para la señal de TV, existen canales aguas abajo (desde la cabecera a la estación) en frecuencias por encima de los 54 Mhz, hasta la frecuencia límite superior está asignada para la transmisión aguas abajo.

La banda de frecuencias, como por ejemplo, entre 5 y 54 Mhz, está asignada para la transmisión aguas arriba. De nuevo, este ancho de banda es dividido, en canales de (n x 40 Khz), donde n es un número entero. En algunas instalaciones de cable, bandas de frecuencias adicionales para la transmisión aguas arriba son destinadas para uso futuro; a estas se les conoce como división banda media y división banda alta. La banda media abarca desde 5 hasta 108 Mhz. La banda alta cubre un rango entre 5 hasta 174 Mhz. En algunas localizaciones geográficas, la banda original es modificada a 5-42 Mhz, 5-65 Mhz, y 5-48 Mhz en Norte América, Europa y Japón respectivamente.

Canal Aguas Arriba

Este canal ocupa en las redes HFC el espectro comprendido entre 5 y 54 MHz. Este ancho de banda lo comparten todos los hogares servidos por un nodo óptico. Los retornos de distintos nodos llegan a la cabecera por distintas vías o multiplexados a distintas frecuencias y/o longitudes de onda.

Una señal generada por el equipo terminal de un abonado recorre la red de distribución en sentido ascendente, pasando por amplificadores bidireccionales, hasta llegar al nodo óptico. Allí convergen las señales de retorno de todos los abonados, que se convierten en señales ópticas en el láser de retorno, el cual las transmite hacia la cabecera.

Un problema que presenta la estructura arborescente típica de la red de distribución en una red HFC es que, así como todas las señales útiles ascendentes convergen en un único punto (nodo óptico), también las señales indeseadas, ruido e interferencias, recogidas en todos y cada uno de los puntos del bus de coaxial, convergen en el nodo, sumándose sus potencias y contribuyendo a la degradación de la relación señal a ruido en el enlace digital de retorno. Este fenómeno se conoce como acumulación de ruido por efecto embudo (noise funneling). A esto hay que añadir el hecho inevitable de que el espectro del canal de retorno es considerablemente más ruidoso que el del canal descendente, sobre todo su parte más baja, entre 5 y 15-20 MHz

La colocación actual de canales de datos en un sistema de cable dado depende de factores tales como restricción de acceso, asignación de poder, etc., y no deberá ser especificado en el estándar. La transmisión digital se logra modulando la información digital en paquetes sobre la portadora de radio frecuencia analógica (RF) a través de 64-QAM (Modulación en Amplitud en Cuadratura) o 256-QAM en canales aguas abajo y QPSK o 16-QAM en el canal aguas arriba.

64-QAM pueden modular cerca de 36 Mbps en un canal aguas abajo de 6 MHz y la QPSK ofrece fidelidad en medio de una eficiencia espectral, robustez y una implementación fácil para modular a 320 Kbps en un canal aguas arriba de 160 Khz.

Protocolo MAC

El nivel MAC es modular y define varias formas diferentes de acceso al medio físico compartido.

Las estaciones no pueden observar las transmisiones aguas arriba de otras estaciones directamente; por lo tanto ellas son incapaces de detectar colisiones y coordinar sus transmisiones por sí mismas. Con un Protocolo de Control de Acceso al Medio (MAC), las estaciones dentro de una rama pueden compartir el ancho de banda disponible.

Para el canal de aguas abajo, el problema de acceso múltiple no existe por que únicamente la cabecera puede transmitir datos sobre este canal de transmisión. Parte del ancho de banda del canal aguas abajo podría ser usado para la transmisión de señales de control e información de realimentación, tal como sea requerido por el protocolo MAC.

Parámetros	Valores
Números de estaciones activas	200
Distancia desde la estación más distante y la cabecera	80 Km
Rata de transmisión de datos por el canal aguas abajo	30 Mbps
Rata de transmisión de datos por el canal aguas arriba	3 Mbps
Retardo de Propagación	5microseg/Km por coaxial y fibra

Tamaño del Data Slot	64 bytes
Tamaño del Contention Slot	16 bytes
DS/CS	4:1
Ciclo de reservación MAC	1.536ms (36 minislot)
Tamaño de Máxima solicitud por CS	32
Asignación de Ancho de Banda	(12 CS, 6 DS)
Resolución de Colisión	Arbol ternario
Retardo de proceso de la cabecera	0 ms
Banda de guardia entre la transmisión de las estaciones	Duración de 5 bytes.

Parámetros por defecto del MAC

Tres aspectos del protocolo MAC en las redes HFC pueden ser identificados:

- Sincronización.
- Modo de Acceso al canal aguas arriba.
- Resolución de colisiones.

Las redes HFC necesitan dos niveles de sincronización. El nivel físico de sincronización alinea las señales al nivel de bit y el nivel de sincronización MAC alinea una gran cantidad de bit a los niveles de paquetes. Como el retardo de propagación sobre las redes HFC es significativo, el nivel de sincronización MAC no puede ser ignorado, similar a CSMA/CD (Sensor de portadora de Acceso Múltiple con Detección de Colisiones) de Ethernet cuando la transmisión de tramas, una detrás de otra, son deseadas. Cada estación trae una propagación de retardo diferente a la cabecera. Esto implica que cuando la cabecera reserva una ranura de tiempo a la estación b, la estación b tiene que adaptar ese tiempo concedido de transmisión para este retardo de propagación, tal que la trama de transmisión se coloque justo en la ranura de tiempo reservada cuando esta llegue a la cabecera.

Como las estaciones no pueden prestar atención al canal aguas arriba, ellas son incapaces de detectar colisiones por ellas mismas. El choque de transmisiones es abortado, como en el CSMA/CD, y reducir el ancho de banda desperdiciado es imposible. Una practica común para reducir el ancho de banda en conflicto es que la estación envíe una solicitud de trama para informar a la cabecera que necesita enviar una trama de información.

Esto se llama Modo de Acceso Reservado. Existe otro modo llamado Modo de Acceso Isócrono, el cual libera la estación al enviar solicitudes periódicamente para el flujo continuo de trafico.

La colisión puede ocurrir para pocas solicitudes. Para esto se necesita un mecanismo de Resolución de Colisión. Los esquemas P-Persistencia, vía del árbol binario y el árbol n-ary fueron considerados por el Comité. El Comité adopto la resolución del árbol n-ary y el P-Persistencia.

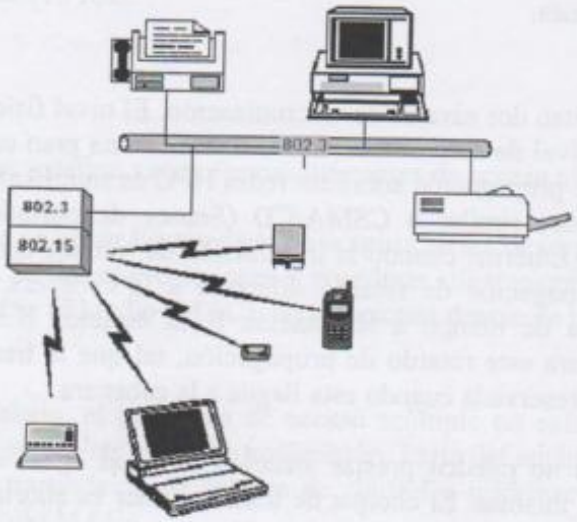
2.4.15. Estándar IEEE 802.15: Acceso inalámbrico para redes de área personal (PAN)

Las Redes de Área Personal (Wireless personal area networks (WPANs)) son usadas para transmitir información sobre distancias cortas, tales como oficinas, hogares, etc. en donde los dispositivos participantes forman un grupo de uso privado. De tal forma proporciona una solución pequeña, económica y eficiente en cuanto al consumo de potencia lo que lo hace aplicable a un amplio rango de dispositivos, tales como teléfonos celulares, PC portátiles, PDAs, micrófonos, sensores, etc.

Esta norma se basa en la especificación **Bluetooth SIG (Special Interest Group)** aparecida en Febrero de 1998, impulsada por las compañías:

–Ericsson
–IBM
–Intel
–Nokia
–Toshiba

En la siguiente figura podemos ver un dispositivo que hace las veces de Bridge adaptando los protocolos 802.3 y 802.5 llamado Gateway de conexión (attachment gateway (AG)



Este estándar está pensado para interoperar con las redes IEEE 802.11, debido a que está implementado físicamente sobre la banda de 2.4 GHz (industrial, scientific, medical (ISM)).

2.4.16. Estándar IEEE 802.16: Acceso inalámbrico fijo de banda ancha (para LAN y MAN)

En enero de 2003 se normalizó este protocolo, que está pensado para brindar acceso inalámbrico a estaciones fijas ubicadas dentro de un área de cobertura metropolitana (distancias de hasta 50 Km.) ya sea que posean o no línea de visión directa con la estación base.

Esta tecnología permite transferencias de hasta 70 Mb/s.

Desde el punto de vista de la conectividad, este protocolo provee una solución equivalente a los accesos cableados, tales como ADSL, o cable modems, o "local loop", "wireless local loop", "middle mile", "WiMAX", PLC (comunicación por línea de energía eléctrica, etc.

Para implementar este protocolo, las tecnologías más usadas son LMDS y MMDS

Esta implementación es conocida también como WiMAX, un acronimo de Worldwide Interoperability for Microwave Access.

Otro estándar es el HIPERMAN (High Performance Radio Metropolitan Area Network) creado por el European Telecommunications Standards Institute (ETSI).

ARQUITECTURAS Y TOPOLOGÍAS

Los sistemas WLL deben optimizar el uso de los canales radio, proporcionando la mayor capacidad posible al máximo numero de abonados,para un ancho de banda dado. Para ello utilizan técnicas de acceso múltiple TDM/TDMA o TDMA/TDMA Desde el punto de vista topológico, presentan un despliegue multicelular que permite el reuso de frecuencia en cada celda, con estructuras punto a multipunto (PMP) o multipunto a multipunto.

Las estructuras punto multipunto se adaptan de modo natural a una colectividad de usuarios distribuidos geográficamente conectada a las redes troncales a través de un nodo de acceso. Este nodo controla la red de acceso y las interfaces de conexión hacia las redes troncales (RPTC, RDSI o IP).

Por razones de fiabilidad se necesitan unidades redundantes, que representan un coste inevitable de abordar desde el primer momento, aun cuando el número de abonados equipados en el sistema sea muy pequeño (situación típica en los primeros meses de despliegue del producto en el campo).

Las estructuras multipunto, aunque con algunas ventajas sobre las anteriores, presentan una complejidad que las ha relegado a un segundo plano. Una de las características más importantes de los sistemas WLL avanzados es la asignación dinámica de los recursos radio en tiempo real, en función de las interferencias presentes en cada momento, lo que facilita en gran medida la planificación de la red a lo largo del ciclo de despliegue del producto.

DIFERENTES ALTERNATIVAS

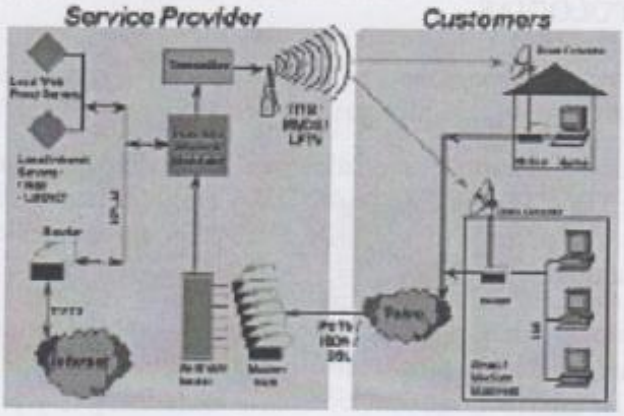
MMDS

La tecnología MMDS (Multichannel Multipoint Distribution Systems) surgió en EE.UU. en los años 80, con la idea de utilizar la banda de 2,5 a 2,686 GHz para la distribución de programas de televisión. La banda, de 186 MHz, se divide en subbandas de 6 MHz, lo que permite la transmisión de 31 canales de televisión analógica NTSC. Este número de canales se puede aumentar utilizando técnicas de compresión y transmisión digital (hasta 5 canales digitales por uno analógico).

Estos sistemas se bautizaron popularmente con el paradójico nombre de "wireless" cable o cable inalámbrico, queriendo significar que equivalían a los conocidos sistemas de distribución de televisión por cable coaxial, pero sin la necesidad de disponer de cable físico. Estaban orientados a entornos rurales o de baja densidad, en donde el tendido de cable convencional para distribución de TV podía resultar antieconómico.

Aunque en EE.UU. tuvieron un desarrollo importante en los años 90, no llegaron a las cifras de mercado esperadas originalmente, por lo que muchos operadores se plantearon nuevas aplica ciones de la tecnología. Un primer paso fue la introducción de un canal de retorno de 12 MHz para proporcionar servicios interactivos como taquilla, vídeo bajo demanda, etc.

Los últimos movimientos en torno a los sistemas MMDS vienen representados por las recientes adquisiciones de empresas poseedoras del espectro por parte de grandes operadores de larga distancia como Sprint y MCI WorldCom, para dar servicios interactivos de voz, datos y acceso a Internet en competencia con los operadores locales. En este caso el concepto de MMDS original se difumina y queda reducido a una porción de espectro que puede ser utilizado por cualquier sistema de acceso múltiple, siempre que se respete la canalización básica de 6 MHz.



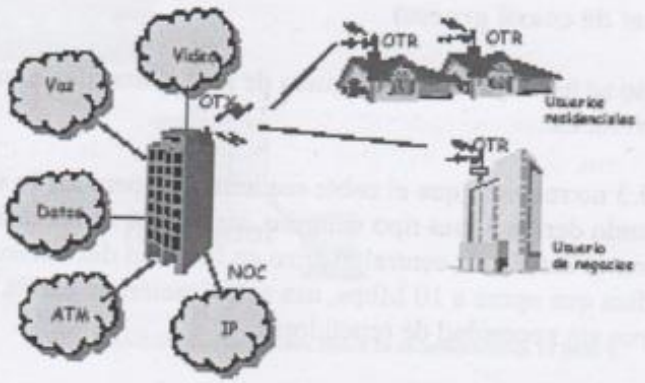
LMDS

Los sistemas LMDS (Local Multipoint Distribution Services) surgieron con una orientación similar a las de MMDS, es decir, aplicaciones de distribución de TV multicanal, si bien, debido a la mayor frecuencia de trabajo (26-28 GHz), las distancias alcanzables eran menores (3-4 km frente a los 15-20 de MMDS). Esto hizo que los sistemas LMDS se vieran desde el principio como una solución urbana, para entornos de alta densidad y concentración de usuarios.

A diferencia de MMDS, los sistemas LMDS no llegaron a desarrollarse en la práctica para la aplicación inicialmente concebida de distribución de TV, viéndose rápidamente su gran potencial como solución de acceso de gran capacidad en aplicaciones de voz y datos. En este sentido, las licencias concedidas en EEUU por la FC C en marzo de 1998 contemplaban la posibilidad no sólo de servicios de TV sino también servicios interactivos de datos y telefonía. Las licencias concedidas recientemente en España en la banda de 26 GHz van básicamente orientadas a servicios interactivos.

Ninguna de las denominaciones MMDS o LMDS responde a un standard específico, por lo que dichos sistemas están basados generalmente en soluciones propietarias de cada fabricante. En el caso de LMDS entendemos por tales a aquellos sistemas de acceso radio fijo de gran capacidad, trabajando en las bandas de 26 ó 28 GHz.

Los sistemas LMDS están orientados fundamentalmente a proporcionar servicios de telecomunicaciones a PYME, por proporcionar grandes capacidades a los usuarios finales (2 Mb/s y superiores en modo circuito), y por ofrecer una amplia gama de servicios tales como telefonía, RDSI (ISDN), líneas alquiladas a n x 64Kb/s y 2 Mb/s, datos en modo paquete, acceso rápido a Internet, etc.



2.4.17 Formas de cableado

Todos los protocolos estudiados hasta aquí se refieren a la capa de enlace de datos o a la capa física, la cual está por encima del medio conductor utilizado para su implementación, así que un mismo protocolo puede tener distintas implementaciones en el cableado

2.4.17.1 10BASE-5 (Ethernet de coaxil grueso)

El cable coaxial grueso se asemeja a una manguera de jardín amarilla, con marcas cada 2.5 metros para indicar los puntos de derivación.

El estándar IEEE 802.3 no requiere que el cable sea amarillo, pero así lo sugiere. Las conexiones a él se hacen generalmente usando derivaciones tipo vampiro, en las que se introduce cuidadosamente una punta hasta hacer contacto con el conductor central macizo en la mitad del núcleo del cable coaxial.
La notación 10 Base-5 significa que opera a 10 Mbps, usa señalización de banda base y puede manejar segmentos de hasta 500 metros sin necesidad de repetidores.

Para lograr abarcar distancias mayores se pueden intercalar hasta cuatro repetidores (esto se conoce como la regla de 5, 4, 3, 2 y 1).

Regla de 5, 4, 3, 2 y 1:

- 5 segmentos de LAN
- 4 repetidores
- segmentos pueden tener conectadas estaciones
- segmentos no deben tener conectadas estaciones
- 1 sólo dominio de colisión

2.4.17.2. 10BASE-2 (Ethernet de coaxil delgado)

A diferencia con el Ethernet grueso, este por ser más delgado se dobla con facilidad, adaptándose mejor a la edificación existente y a la topología de la red. Las conexiones se hacen usando conectores BNC estándar de la industria para formar uniones T, en lugar de usar derivaciones vampiros. Éstas son más fáciles de usar y más confiables. El Ethernet delgado es mucho más barato y más fácil de instalar; sólo tiene el inconveniente de que sólo puede extenderse 200 metros y puede manejar sólo 30 máquinas por segmento de cable.

De ser necesario abarcar una distancia mayor se pueden intercalar hasta cuatro repetidores (también vale la regla de 5, 4, 3, 2 y 1).

2.4.17.3 10BASE-T

Los problemas asociados con la localización de rupturas de cables han empujado a los sistemas a un tipo de patrón de cableado diferente, en las que todas tienen cables que conducen a un concentrador (*hub*) central (topología en estrella). Como vimos en el apartado de topologías, esta es la que posee mayores ventajas sobre todo a la hora de insertar /extraer estaciones con la red en funcionamiento.

Generalmente, estos cables son pares trenzados UTP, ya que la mayoría de los edificios de oficinas ya están alambrados de esta manera y normalmente hay bastante pares extras disponibles. A esto se le llama 10 Base-T. Un ejemplo de esto se ve en la **figura 2.19.**

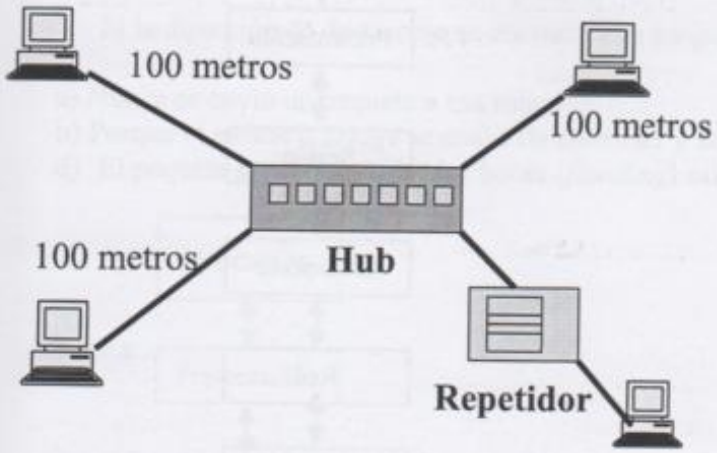


FIGURA 2.19: Configuración típica de concentradores 10 base T.

En el siguiente cuadro comparativo muestra las tres implementaciones.

Nombre	Cable	Segmento máximo	Nodos/segundos	Ventajas
10 BASE - 5	Coaxial grueso	500 m	100	Bueno para backbone
10 BASE – 2	Coaxial fino	200 m	30	Sistema más barato
10 BASE - T	Par trenzado	100 m	1024	Fácil mantenimiento

2.4.18. Dispositivos de Red

2.4.18.1. Hub

Un *hub* como se muestra en la **figura 2.20**, es un dispositivo de interconexión, al cual las estaciones están conectadas directamente, formando la topología de estrella. Ver también la figura 2.21. Cumple funciones en el nivel 1 (físico) del modelo OSI.

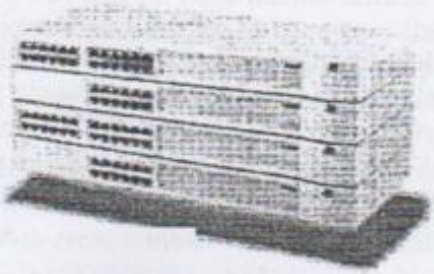


FIGURA 2.20: Hub 10/100 base T.

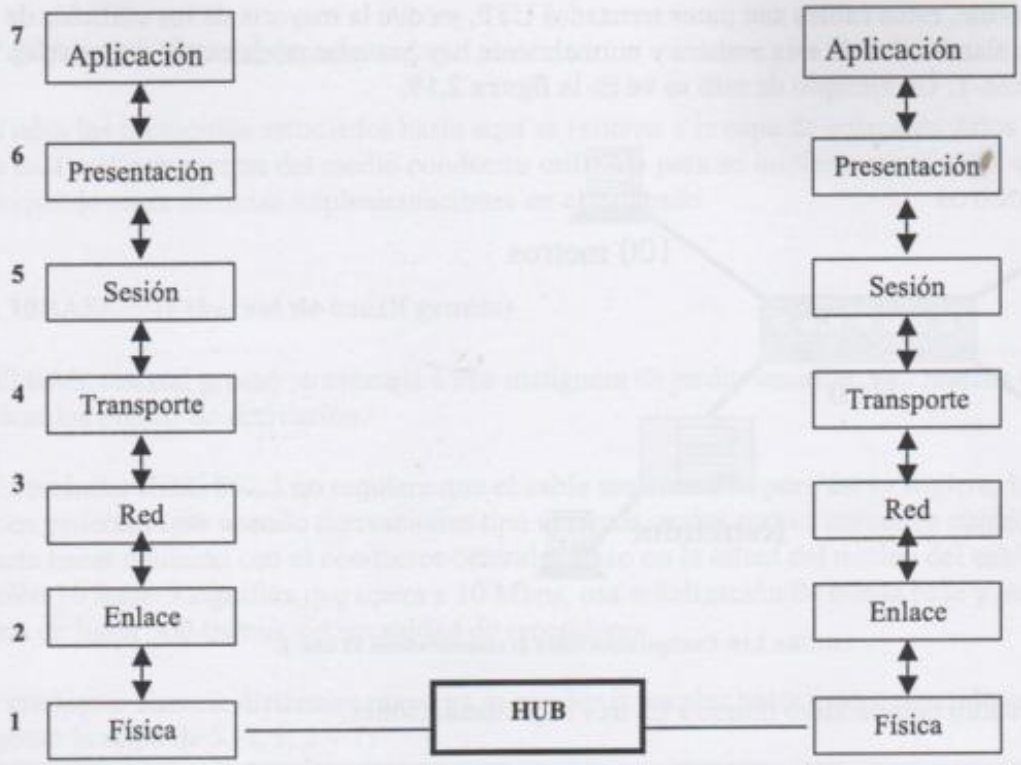


FIGURA 2.21: Diagrama de conexión de un HUB en el modelo OSI.

2.4.18.2. Switch

Se usa de manera similar al hub para interconectar un grupo de estaciones que tienen un segmento de red. Es decir, cuando el tráfico en una LAN se congestiona, ya sea por la existencia de un número excesivo de usuarios o por la creciente demanda de aplicaciones, uno de los recursos con que cuentan los administradores de una red es la segmentación.

El switch es un dispositivo de nivel 2 (enlace de datos) del modelo OSI, y por lo tanto es capaz de dividir la red en segmentos. Así se va partiendo la red en varias redes menores unidos por un elemento de interconexión, el *switch*.

Funcionamiento

Trabaja en la capa 2 del modelo OSI como se observa en la **figura 2.22**, al igual que los *bridges* (puentes). Su funcionamiento es igual que la de los *bridges*: mantienen para cada boca (Interfaz) una tabla de direcciones locales (MAC) y verifican todas las tramas. Si la trama tiene una dirección local no lo reenvían, caso contrario lo hacen al puerto destino. Reciben tramas por los distintos puertos, anota la dirección de quién la envió en su tabla, y las envían de acuerdo a su dirección destino al puerto de salida correspondiente.

Los *switches* arman tablas que contienen la dirección MAC de la estación/es conectadas a cada puerto (*switches* pueden tener más de una estación en cada boca), a medida que van recibiendo tramas en dicho puerto.

Si la dirección de destino no se encuentra en ninguna tabla:

a) Nunca se envió un paquete a esa estación.
b) Porque el *switch* o *bridge* se acaba de encender y las tablas están vacías.
d) El paquete se envía a todas las bocas (*flooding*) salvo al puerto por donde entró.

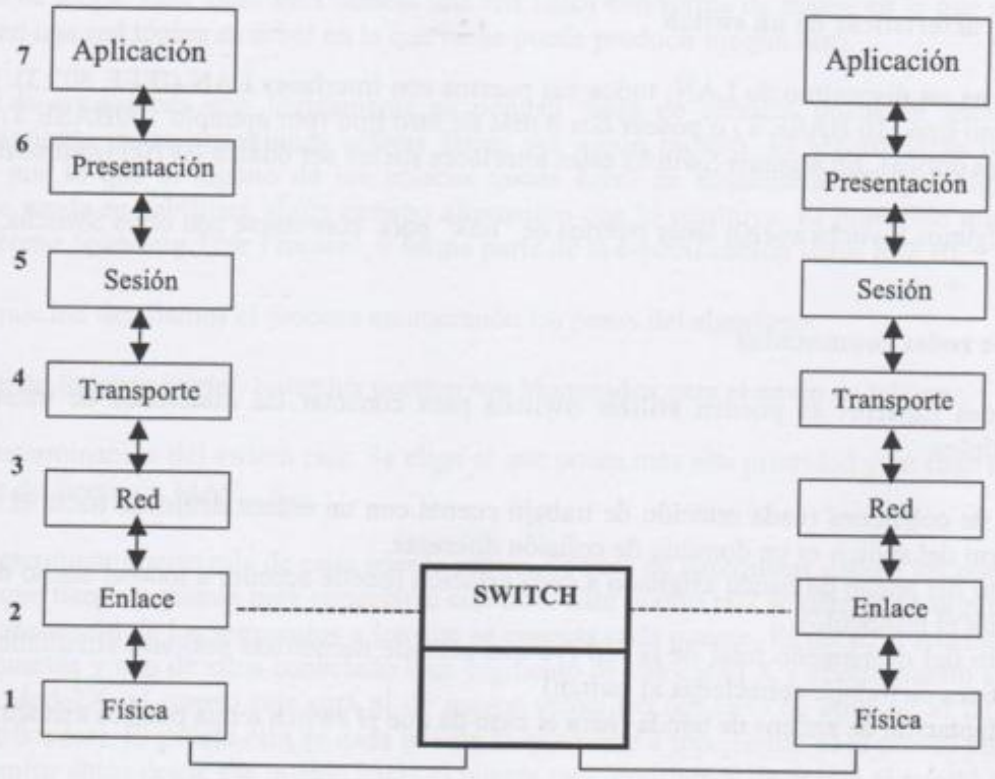


FIGURA 2.22: Diagrama de conexión de un Switch en el modelo OSI.

Tipos de switch

a) **Store and forward** (guardar y enviar): es el más antiguo y deriva de los *bridges*. Recibe toda la trama LAN, verifica (mediante el FCS) que no haya habido errores de transmisión y la envía al puerto destino. Debido a que tiene que esperar para recibir el paquete y luego trasmitirlo, agrega retardos a la red. Este tipo de funcionamiento es el único posible cuando los paquetes viajan entre segmentos de distintas velocidades. Por ejemplo: Ethernet 10 BaseT a Ethernet 100 BaseT.

b) **Cut-through** (cortar y pasar): sin recibir todo el paquete completo y contando con la dirección destino, envía el paquete al puerto destino. Así disminuye el retardo que existe en el otro nodo: pero al no revisar los tramos, puede trasmitirlos erróneamente; se ve imposibilitado a unir segmentos de distintas velocidades.

Estrategias de funcionamiento

Para aumentar el rendimiento de una LAN podemos usar un switch en alguna de estas formas:

- **Segment switching:** Cuando a la boca de un *switch* se conecta un segmento usualmente de pocos usuarios unidos a un hub (*switch* de segmentos).

- **Switched LAN:** Si se conecta un solo usuario a la boca LAN del *switch.*

Características de un switch

Un switch es un dispositvo de LAN; todos sus puertos son interfaces LAN (IEEE 802.3). Pueden ser todas del mismo tipo (10 BASE T) o poseer dos o más de otro tipo (por ejemplo 100BASE T, o 1000 BASE T o de Fibra óptica). En algunos Switchs estas interfaces suelen ser duales 10/100 (*autosensing*).

Además algunos Switchs suelen tener puertos de "link" para conectarse con otros Switchs.

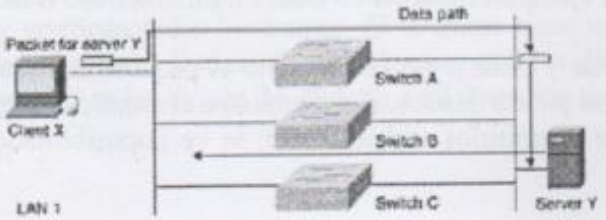
Configuración de redes conmutadas

En las redes Ethernet se pueden utilizar Switchs para conectar las estaciones de trabajo. Las ventajas son múltiples:

- Ausencia de colisiones (cada estación de trabajo cuenta con un enlace dedicado hacia el switch). Cada puerto del switch es un dominio de colisión diferente.
- Incremento del ancho de banda asignado a cada estación (puede acceder a todo el ancho de banda que permita el protocolo)
- Incremento del desempeño total de la red (ya que permite numerosas sesiones simultáneas entre las estaciones de trabajo conectadas al switch)
- Provee adaptación de anchos de banda (para el caso de que el switch tenga puertos asimétricos)

Protocolo Spanning Tree (IEEE 802.1d)

El problema de los switch es que si reciben una trama con una dirección desconocida (que no figura en su tabla) como podría ser un mensaje de broadcast, inundan los demás puertos con dicha trama. Si uno de esos puertos (por ejemplo el de link) está conectado a otro switch, también recibirá la trama y probablemente si no la tiene en su tabla, también inunde a sus otros puertos, de tal forma que la trama le vuelve al switch que la envió en primer lugar; y esta secuencia se vuelve a repetir indefinidamente, produciéndose una **"tormenta de broadcast"**.



Para evitar este problema existe un mecanismo que permite a los switches comunicarse entre sí, pasándose información sobre la topología de las conexiones existentes. Los Switchs/ bridges se comunican mediante *Bridge Protocol Data Units* (B.P.D.U's).

El bridge con la prioridad más alta (el número más bajo de dirección MAC) se constituye en la raíz del árbol de expansión. Este bridge raíz establece el camino de menor coste para todas las redes; cada puerto tiene un parámetro configurable: el Span path cost. Todos los demás caminos son bloqueados para propósitos de envío de tráfico. Una vez conocida la topología los switches desactivarán las conexiones redundantes para garantizar que haya un único camino uniendo todas las redes, de forma que se evite la creación de loops. Este algoritmo cambia una red física con forma de malla, en la que se pueden formar bucles, en una red lógica en árbol en la que no se puede producir ningún lazo.

Las conexiones que lógicamente se pongan fuera de servicio quedarán listas para entrar en funcionamiento si las conexiones activas fallan por algún motivo. El algoritmo se repite cada cierto tiempo, por lo que si alguno de los enlaces queda fuera de funcionamiento por algún motivo en la siguiente ronda se habilitará algún camino alternativo que lo sustituya. El protocolo que permite esto se conoce como Spanning Tree Protocol, y forma parte de la especificación IEEE 802.1d.

A continuación detallamos el proceso enumerando los pasos del algoritmo.

1) En un instante inicial, todos los puertos son bloqueados para el envío de tráfico

2) Determinación del switch raíz. Se elige el que posee más alta prioridad y en caso de empate menor valor de dirección MAC.

3) Determinar puerto raíz de cada puente activo. Se trata de determinar uno de los puertos de los dos o más que tiene un puente para conectarse con otro. Este puerto raíz se determina según las velocidades de transmisión de los segmentos a los que se conecta cada puente. Es decir, si tenemos un puente con dos puertos y uno de ellos conectado a un segmento de velocidad X y el otro puerto a un segmento de velocidad 2X, el puerto raíz será el de mayor velocidad (en caso de empate; el de menor valor de identificador). El puerto raíz de cada puente lo que viene a representar es el puerto por donde se van a transmitir datos desde ese puente hacia el puente raíz. Podríamos decir que el puerto raíz es aquel que nos da el mínimo tiempo posible para ir al puente raíz, con lo que parece lógico quedarse con aquel camino de menor coste.

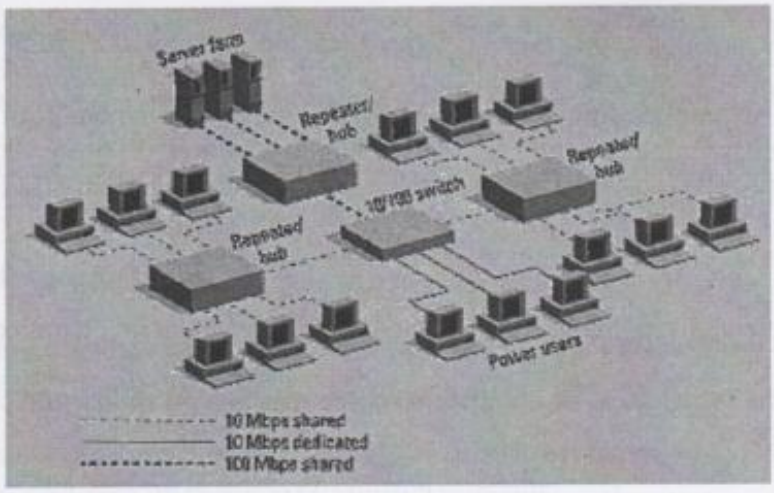
4) Determinar puerto designado de cada segmento. Físicamente el puente tiene dos o más puertos, el puente se comunica a través del puerto a otro segmento. El puerto designado de un segmento será de todos los puertos que se encuentran conectados a ese segmento aquel que dé un valor menor en una función de coste, si coincide elegimos el puerto del puente de menor valor de identificador. De este modo, designamos un único puente para transmitir o recibir datos desde o hacia el puente raíz y designamos un único segmento para transmitir o recibir datos desde o hacia el puente raíz; todo esto con la intención de determinar un único camino para llegar a este puente raíz.

5) Finalmente se establece el estado de cada puerto de cada uno de los puentes en transmisión o bloqueo. Inicialmente, la totalidad de los puertos del puente raíz son puertos designados y por tanto, se establecen en estado de transmisión. Para el resto de los puentes, sólo los puertos raíces y los designados se configuran en estado de transmisión, y el resto en bloqueo.

LAN Virtuales (VLANs)

Los grupos de trabajo en una red han sido creados por la asociación física de los usuarios en un mismo segmento de la red, o en un mismo dispositivo (hub). Como consecuencia directa, estos grupos de trabajo comparten el ancho de banda disponible y los dominios de "broadcast", y con la dificultad de gestión cuando se producen cambios en los miembros del grupo.

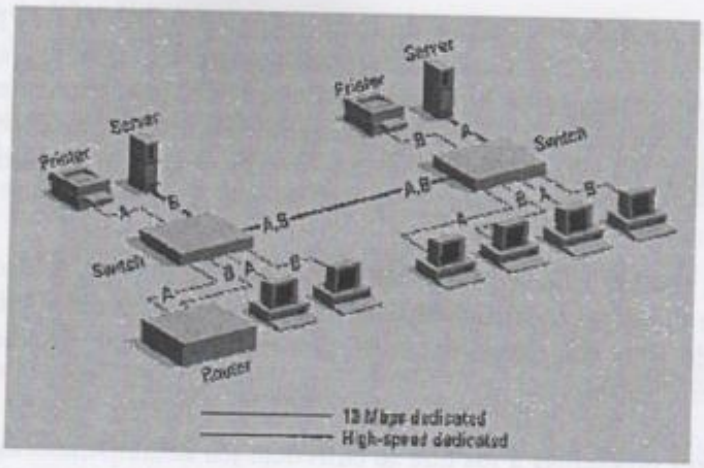
Más aún, la limitación geográfica que supone que los miembros de un determinado grupo deben de estar situados adyacentemente, por su conexión al mismo concentrador o segmento de la red.



Una Virtual LAN es un grupo de dispositivos en una o más LANs que son configurados (utilizando software de administración; existe un estándar IEEE 802.1q) de tal manera que se pueden comunicar como si ellos estuvieran conectados al mismo cable, cuando en realidad están localizados en un segmento diferente de LAN. Esto es porque VLANs están basadas en las conexiones lógicas en lugar de las físicas y es por eso que son extremadamente flexibles.

Los esquemas VLAN (Virtual LAN o red virtual), proporcionan los medios adecuados para solucionar esta problemática, por medio de la agrupación realizada de una forma lógica en lugar de física.

Sin embargo, las redes virtuales siguen compartiendo las características de los grupos de trabajo físicos, en el sentido de que todos los usuarios tienen conectividad entre ellos y comparten sus recursos y sus dominios de "broadcast".



Los puertos de cada switch son configurados como miembros ya sea de la VLAN A o la VLAN B.

Si la estación final transmite tráfico de broadcast o multicast, el tráfico es reenviado a todos los puertos miembros. El tráfico que fluye entre las dos VLANs es controlado y reenviado por el router, dando así seguridad y manejo del tráfico

La principal diferencia con la agrupación física, como se ha mencionado, es que los usuarios de las redes virtuales pueden ser distribuidos a través de una red LAN, incluso situándose en diferentes ubicaciones geográficas y conectándose a distintos hubs de la misma.

Los usuarios pueden, así, "moverse" a través de la red, manteniendo su pertenencia al grupo de trabajo lógico. Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, se logra, como consecuencia directa, el incremento del ancho de banda en dicho grupo de usuarios. Además, al poder distribuir a los usuarios en diferentes segmentos de la red, es posible situar puentes y encaminadores entre ellos, separando segmentos con diferentes topologías y protocolos. Así por ejemplo, es posible mantener diferentes usuarios del mismo grupo, unos con FDDI y otros con Ethernet, en función tanto de las instalaciones existentes como del ancho de banda que cada uno precise, por su función específica dentro del grupo.

Todo ello, por supuesto, manteniendo la seguridad deseada en cada configuración por el administrador de la red: Se puede permitir o no que el tráfico de una VLAN entre y salga desde o hacia otras redes.

Pero aún se puede llegar más lejos. Las redes virtuales permiten que la ubicuidad geográfica no se limite a diferentes concentradores o plantas de un mismo edificio, sino a diferentes oficinas intercomunicadas mediante redes WAN o MAN, a lo largo de países y continentes, sin limitación ninguna más que la impuesta por el administrador de dichas redes.

Prestaciones de las VLAN

Los dispositivos con funciones VLAN ofrecen unas prestaciones de "valor añadido", suplementarias a las funciones específicas de las redes virtuales, aunque algunas de ellas son casi tan fundamentales como los principios mismos de las VLAN.

Al igual que en el caso de los grupos de trabajo "físicos", las VLAN permiten a un grupo de trabajo lógico compartir un dominio de broadcast. Ello significa que los sistemas dentro de una determinada VLAN reciben mensajes de broadcast desde el resto, independientemente de que residan o no en la misma red física. Por ello, las aplicaciones que requieren tráfico broadcast siguen funcionando en este tipo de redes virtuales. Al mismo tiempo, estos broadcast no son recibidos por otras estaciones situadas en otras VLAN.

Las VLAN no se limitan solo a un conmutador, sino que pueden extenderse a través de varios, estén o no físicamente en la misma localización geográfica. Además las redes virtuales pueden solaparse, permitiendo que varias de ellas compartan determinados recursos, como backbones (troncales) de altas prestaciones o conexiones a servidores.

Uno de los mayores problemas a los que se enfrentan los administradores de las redes actuales, es la administración de las redes y subredes. Las VLAN tienen la habilidad de usar el mismo número de red en varios segmentos, lo que supone un práctico mecanismo para incrementar rápidamente el ancho de banda de nuevos segmentos de la red sin preocuparse de colisiones de direcciones.
Las soluciones tradicionales de internetworking, empleando concentradores y routers, requieren que cada segmento sea una única subred; por el contrario, en un dispositivo con facilidades VLAN, una subred puede expandirse a través de múltiples segmentos físicos, y un solo segmento físico puede soportar varias subredes.

Asimismo, hay que tener en cuenta que los modelos más avanzados de conmutadores con funciones VLAN, soportan filtros muy sofisticados, definidos por el usuario o administrador de la red, que nos permiten determinar con gran precisión las características del tráfico y de la seguridad que deseamos en cada dominio, segmento, red o conjunto de redes. Todo ello se realiza en función de algoritmos de bridging, y routing multiprotocolo.

Ventajas de las VLANs

- Movilidad: Como hemos visto, el punto fundamental de las redes virtuales es el permitir la movilidad física de los usuarios dentro de los grupos de trabajo.
- Dominios lógicos: Los grupos de trabajo pueden definirse a través de uno o varios segmentos físicos, o en otras palabras, los grupos de trabajo son independientes de sus conexiones físicas, ya que están constituidos como dominios lógicos.
- Control y conservación del ancho de banda: Las redes virtuales pueden restringir los broadcast a los dominios lógicos donde han sido generados. Además, añadir usuarios a un determinado dominio o grupo de trabajo no reduce el ancho de banda disponible para el mismo, ni para otros.
- Conectividad: Los modelos con funciones de routing nos permiten interconectar diferentes conmutadores y expandir las redes virtuales a través de ellos, incluso aunque estén situados en lugares geográficos diversos.
- Seguridad: Los accesos desde y hacia los dominios lógicos, pueden ser restringidos, en función de las necesidades específicas de cada red, proporcionando un alto grado de seguridad.
- Protección de la inversión: Las capacidades VLAN están, por lo general, incluidas en el precio de los conmutadores que las ofrecen, y su uso no requiere cambios en la estructura de la red o cableado, sino más bien los evitan, facilitando las reconfigura-iones de la red sin costes adicionales.

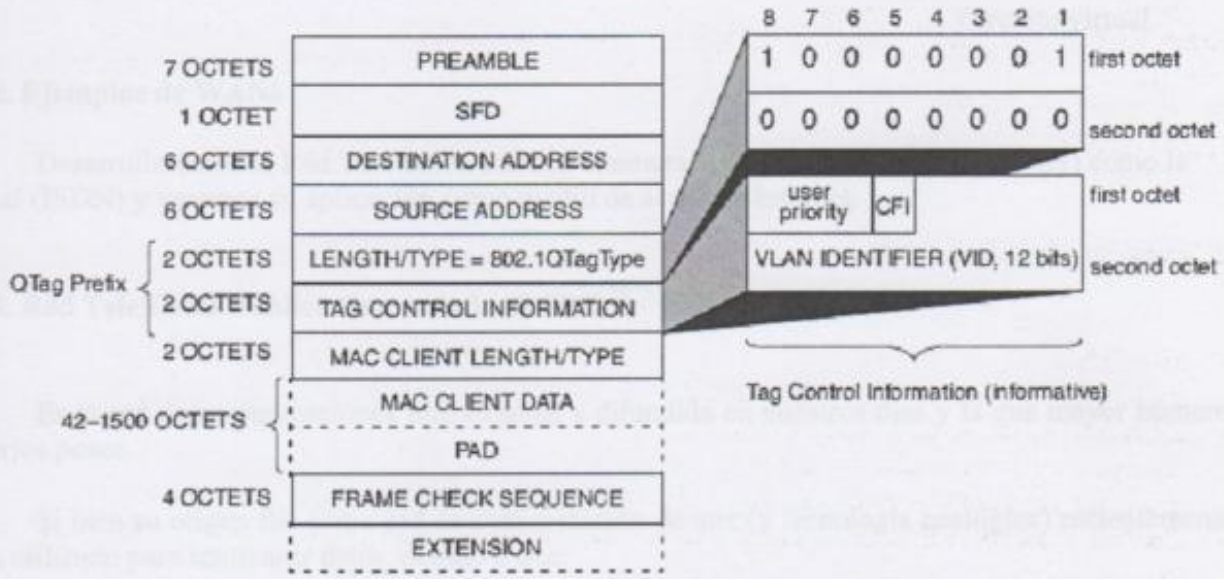
IEEE 802.1q: Protocolo de VLAN

El IEEE normalizó un protocolo para la creación, configuraciónb y administración de VLANs en los switchs. Se basa en el agregado de una etiqueta a la trama IEEE 802.3 para que sea leída por todos los switchs de la LAN y que se retira antes de entregarla a la estación de trabajo destino.

Trama MAC etiquetada

Dentro de la trama MAC se puede incluir una etiqueta de 4 Bytes, divididos en dos pares:

- El primer par es fijo (0x8100) y coincide con la interpretación que se le daría al campo Longitud / Tipo y se destina a indicar que la trama viene con una etiqueta compatible con IEEE 802.1Q: estándar que especifica la arquitectura, los servicios y los protocolos involucrados en las Virtual Bridged LAN.
- El segundo par de Bytes se destina a información de control de etiquetado:
  - Identificador de prioridad (3 bits)
  - El identificador canónico (*Canonical Format Indicador* CFI) (1 bit)
  - VLAN (12 bits)



Las utilidades de esta etiqueta serían:

- La posibilidad de diferenciar tiempos de respuesta para soportar transmisiones en tiempo real o informaciones críticas para el funcionamiento de la red.
- El uso de señalización de prioridades para distintas clases de tráfico previamente identificadas.
- La provisión de servicios de filtrado de tráfico en forma dinámica y el establecimiento de grupos de usuarios dentro del entorno de la LAN, tales que el tráfico dirigido a un determinado grupo, sólo sea encaminado hacia el segmento donde haya integrantes de ese grupo

La siguiente Tabla muestra un resumen de la organización e interconexión de LANs usando los distintos equipos de nivel físico y de enlace vistos hasta el momento, y su relación con los dominios de colisión y de broadcast.

Tabla: Relación entre los equipos de comunicación LAN y los dominios de colisión y broadcast

Equipo	Nivel de Trabajo	Nº Puertos	Dominios Colisión	Dominios Broadcast
Repetidor	Físico	n	1	1
Hub	Físico	n	1	1
Bridge	Enlace	n	n	1
Switch	Enlace	n	n	1
Switch VLAN	Enlace y sup.	n	n	m

2.5. Redes Área Extendida (WAN)

Son redes de área extensa, cruzan fronteras interurbanas, incluso interprovinciales o internacionales. Los enlaces se realizan con servicios privados y/o públicos de telecomunicaciones utilizando principalmente sistemas de comunicaciones ópticos y enlaces satelitales y de microondas. Generalmente prestan servicios de extremo a extremo (teleservicios) o se utilizan para interconectar redes locales o privadas.

2.5.1 Clasificación de las WANs

Según la tecnología que utilicen para trasladar la información hasta el destino se pueden clasificar en:

- WAN → Difusión
- WAN → Conmutadas → Conmutación de Circuitos
- Conmutadas → Conmutación de Paquetes → Datagrama
- Conmutación de Paquetes → Circuito virtual

2.5.2. Ejemplos de WANs

Desarrollaremos la Red Telefónica Pública conmutada (tanto la tradicional (POTN) como la digital (ISDN) y veremos su aplicación como medio de acceso a Internet.

2.5.3. Red Telefónica Pública Conmutada (RTPC)[29]

Es la red de comunicaciones más extensa y difundida en nuestros días y la que mayor número de usuarios posee.

Si bien su origen fue como red de comunicación de voz (y tecnología analógica) recientemente se la ha utilizado para transmitir datos, debido a que:

- El servicio telefónico está disponible en la mayor parte del mundo.
- El costo de una red privada, para un sistema geográficamente remoto, es normalmente muy elevado.
- Es un servicio que está normalizado internacionalmente, hecho éste que permite diseñar equipos informáticos e interfaces con los equipos terminales de datos muy rápidamente y producir la necesaria adaptación de ambos servicios.
- Es un sistema de costos muy aceptable, en función a la inversión que requiere para este tipo de tráfico.

[29] En Inglés: (PSTN) Public Switched Telephone Network.

2.5.3.1. Servicio Telefónico

Definición:

"Servicio destinado a establecer comunicación de voz entre dos individuos que acceden a la red por medio del aparato telefónico".

Esta definición tiene que ver con el origen del sistema telefónico (siglo pasado) y con la limitación impuesta por la legislación actual sobre telecomunicaciones, ya que la red telefónica está capacitada para transportar otro tipo de servicios.

Debido a la larga historia del servicio telefónico y a la importancia estratégica del mismo para el desarrollo de un país, el mismo posee características que lo distinguen de otro tipo de servicios de comunicaciones.

A dichas características las podemos analizar desde dos puntos de vista:

A) Requerimientos de los Usuarios

- Formalidad, puntualidad, integridad (*Reliability*).
- Facilidad de acceso a cualquier usuario.
- Rapidez en el establecimiento de las llamadas.
- Buena calidad de transmisión.
- Bajo costo de la llamada.
- Privacidad de la comunicación.

B) Requerimientos de la Red

- Cobertura geográfica.
- Buena disponibilidad (GOS[30]).
- Funcionamiento en caso de catástrofe.

A su vez la red requiere de sus equipos:

- Larga vida de los equipos.
- Renovables en etapas.

[30] En Inglés: Grade of Service.

- Tener suficiente capacidad para soportar crecimientos de tráfico.
- Uso eficiente del equipamiento.
- Simple de mantener y de reparar (o reemplazar).
- Provisión de repuestos por 10 años.
- Capacidad de redundancia para hacer frente a fallas.
- Normalización internacional: compatibilidad entre equipos de distintos fabricantes.

2.5.3.2. Estructura de la Red Telefónica

Hoy en día el sistema telefónico se organiza como una red jerárquica altamente redundante, de múltiples niveles. La siguiente descripción está sumamente simplificada, pero da la idea esencial. (Ver **figura 5.1**) Cada teléfono tiene dos alambres de cobre (par telefónico) que salen de él y que van directamente a la **central local** más cercana a la compañía de teléfonos (también llamada **oficina local** o **central urbana**). Por lo general, la distancia es de 1 a 5 km, y en las ciudades es menor que en las áreas rurales.

Las conexiones de dos hilos (par) entre el teléfono de cada abonado y la central local se conocen como **líneas de abonado** (también llamadas **lazos locales**).

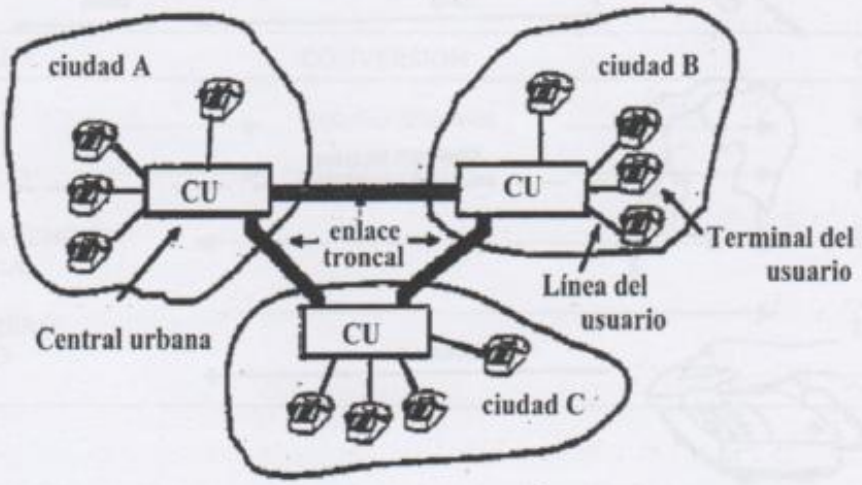


FIGURA 2.5.1: Ejemplo de una red telefónica urbana de tres centrales.

Si un suscriptor conectado a una central local determinada llama a otro suscriptor conectado a la misma central local, el mecanismo de conmutación dentro de la central establece una conexión eléctrica directa entre las dos líneas de abonado (conmutación de

circuitos). Esta conexión permanece intacta mientras dura la llamada, y debe ser liberada una vez que finaliza la misma.

2.5.3.3. Principio de Funcionamiento

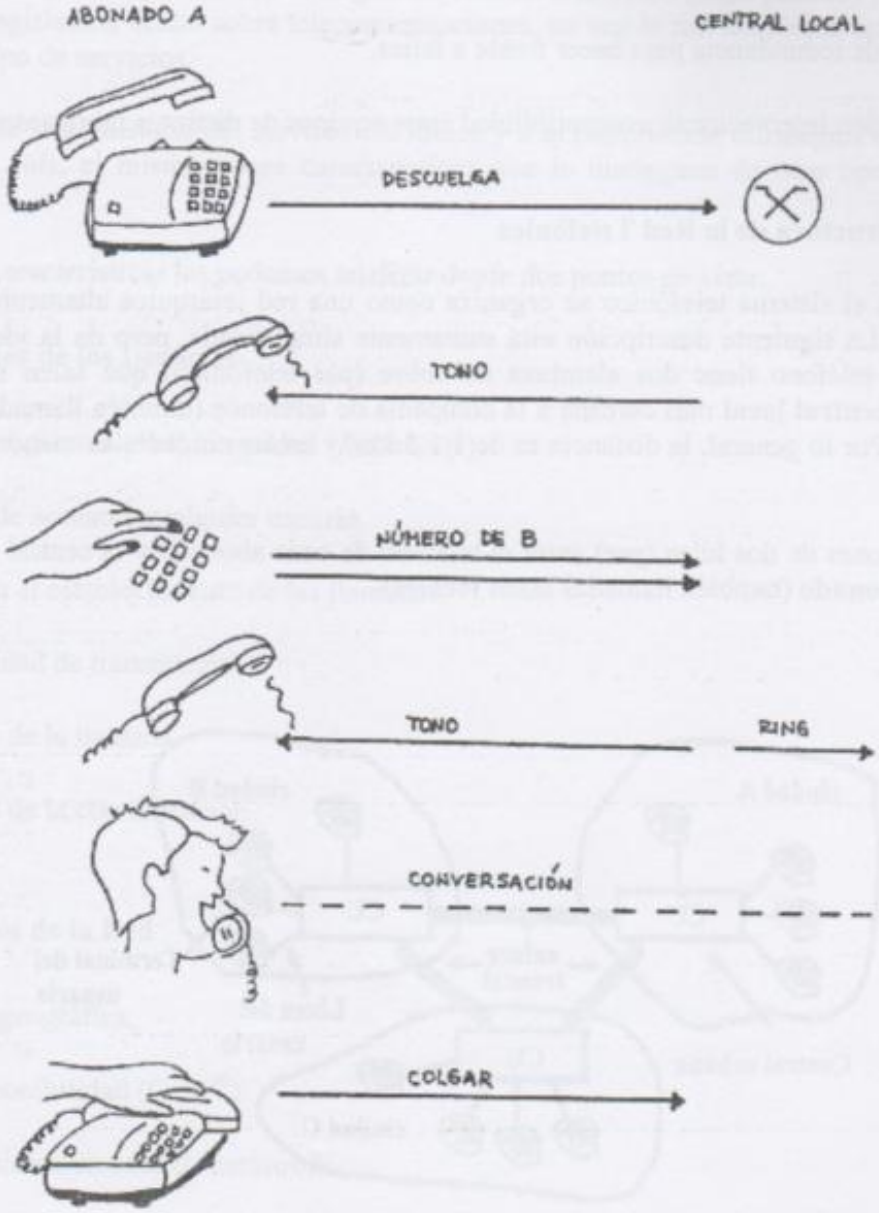


FIGURA 2.5.2: Funciones que realiza el terminal telefónico para que sea posible la comunicación duplex.

El aparato telefónico es el equipo de que dispone el usuario para acceder a la red telefónica. Podemos resumir sus funciones principales en las siguientes:

- Atraer la atención de la central.
- Recibir confirmación de ella.
- Enviar el número del abonado con el cual nos queremos comunicar.
- Alertarnos de que alguien quiere comunicarse con nosotros.
- Convertir nuestra voz en señal eléctrica; y viceversa.
- Avisar a la central cuando la conversación ha finalizado.

En la **figura 2.5.2** se ilustran dichas funciones.

En el mercado podemos encontrar muchas realizaciones tecnológicas del aparato telefónico, las cuales pueden incluir además funciones de rellamada, memorias de números muy usados, etc.; en todos los casos serán variaciones más o menos sofisticadas de estos principios.

Para poder llevar a cabo una conversación telefónica y otras funciones referidas al diálogo con la central local, el terminal debe realizar una conversión electro-acústica de la señal. Esta conversión de la voz (acústica) a señal eléctrica la realiza el micrófono; la inversa, de eléctrica a audible la realiza el parlante. Estos dos elementos están contenidos en el microteléfono (*handset*).

El intercambio de información de señalización con la central la realizan las otras partes del aparato telefónico, como la horquilla y el dial. De este último encontramos dos realizaciones: el disco y el teclado multifrecuencia. Estos conceptos están resumidos en la **figura 2.5.3**.

SEÑAL	CONVERSIÓN	DISPOSITIVO
VOZ →	Acústica /Eléctrica →	MICRÓFONO
SONIDO →	Eléctrica /Acústica →	PARLANTE
ATRAER LA ATENCIÓN DE LA CENTRAL ←	→	HORQUILLA
ENVIAR NÚMERO DE ABONADO →	→	DIAL

FIGURA 2.5.3: Esquema en el que se visualizan las conversiones realizadas en el aparato telefónico.

Si el teléfono al que se llama está conectado a otra central local, se tiene que usar un procedimiento diferente. Cada central local tiene varias líneas salientes a uno o más centros de conmutación cercanos, llamadas **centrales de tránsito** (también llamadas **oficias de cargo**; o, si están dentro de la misma área local, **oficinas tándem**). Estas líneas se llaman **troncales de conexión con cargo**. Si sucede que tanto la central local como la de quien es llamado tienen un troncal de conexión a la

misma central de tránsito (algo muy probable si no están muy alejadas), la conexión se puede establecer dentro de la central de tránsito. (Ver **figura 2.5.4**)

Si el que llama y el que es llamado no tienen una central de tránsito en común, la trayectoria se deberá establecer en un nivel más alto de la jerarquía. Hay centrales primarias y regionales que forman una red que conecta a las centrales de tránsito. Las centrales de tránsito, primarias y regionales, se comunican entre sí mediante **troncales** de gran ancho de banda (también llamados **troncales interoficinas**). La conmutación entre ciudades diferentes se establece a través de nodos de conmutación denominados **Centros Automáticos Interurbanos (CAI)**.

Estos nodos están conectados entre sí de una manera jerárquica, de forma tal, que los hay de diferentes categorías según se encuentren ubicados cerca de la periferia de la red o en los principales centros de concentración de abonados. La cantidad de tipos diferentes de centros de conmutación y su topología varían de país a país dependiendo de su densidad telefónica.

Para telecomunicaciones se usan diversos medios de transmisión. En nuestros días, las líneas de abonado se implementan principalmente con dos tipos de tecnologías: *pares trenzados* y *acceso inalámbrico*. Entre las oficinas o nodos de conmutación se usan ampliamente *cables coaxiales, microondas,* y en especial *fibra óptica.*

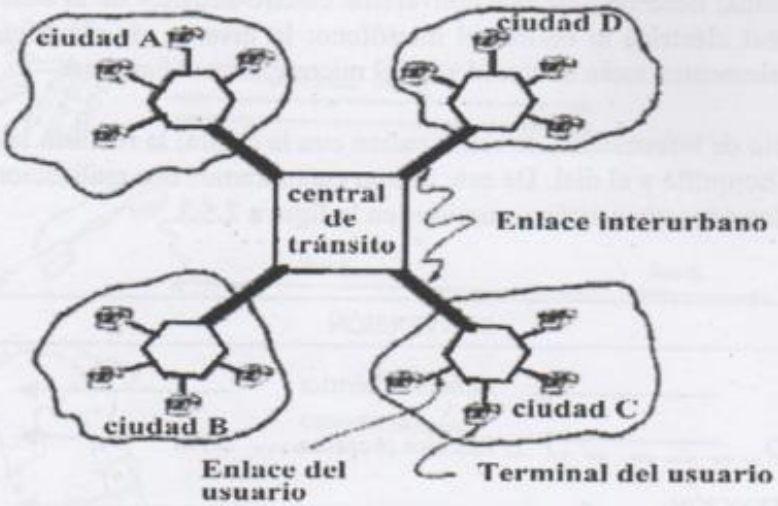


FIGURA 2.5.4: Ejemplo de una red telefónica urbana de cinco centrales conectadas a través de una central de tránsito.

En el pasado, la señal en todo el sistema telefónico era analógica, con la señal de voz real transmitida como voltaje eléctrico del origen al destino. Con el advenimiento de la electrónica digital y las computadoras, se ha hecho posible la conversión del sistema telefónico para transporte señal digital. Debido a las ventajas de ésta respecto de la analógica, todas las troncales de larga distancia dentro del sistema telefónico se convierten a la tecnología digital.

2.5.3.3.1. Funciones de la Central Local

Todo aparato telefónico de abonado está conectado en primera instancia a una central local (a través de lo que se conoce como bucle de abonado), que será la que le suministrará la alimentación de energía necesaria para cumplir con sus funciones.

La central local es un ente complejo que posee organismos específicamente dedicados a la comunicación con los usuarios y otros para el mantenimiento del funcionamiento en sí de la central.

2.5.3.3.1.1. Funciones de Comunicación

A) Establecimiento de la llamada

Para ello la central local debe establecer un diálogo con el terminal de abonado; este proceso se denomina señalización, y puede comprender alguna de las siguientes secciones:

- Detectar un pedido de llamada, por parte de un abonado; esto lo realiza el circuito de línea de abonado, analizando el estado de la horquilla del aparato telefónico.
- Reconocer de qué abonado se trata (abonado A).
- Recibir el número de abonado llamado (abonado B) y almacenarlo.
- Ser capaz de analizar dicho número para seleccionar la mejor ruta disponible a través de la central hacia el enlace correcto.
- Determinar si el teléfono del abonado solicitado (B) está ocupado, y enviar el correspondiente tono de ocupado a A.

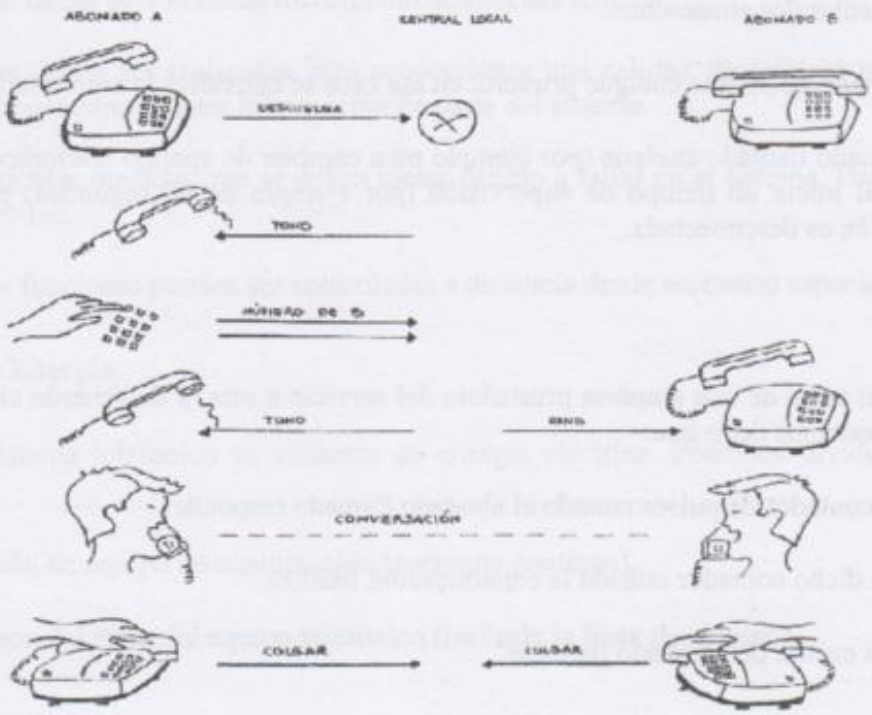


FIGURA 2. 5.5: Operaciones de señalización entre terminales de abonado y central local.

- Conectar las líneas de los abonados llamantes (A) y llamado (B) ("conmutación").

- Enviar la señal de alerta al abonado llamado (B) y devolver el correspondiente tono al que llama (A).

- Detectar cuando el abonado llamado (B) contesta y cortar el tono que devolvía al llamante.

Podemos ver un esquema de este proceso de señalización en la **figura 5.5**.

B) Mantenimiento de la llamada

Debe procurar que los recursos asignados (circuito) a los abonados puestos en comunicación, no sean usurpados por otros abonados que quieren entrar en comunicación, ni que se interrumpa dicho circuito por otro motivo.

C) Desconexión de la llamada

Las horquillas de los dos teléfonos que se encuentran en comunicación son constantemente vigiladas para detectar rápidamente cuál de los dos cuelga el microteléfono y determinar si debe procederse a la desconexión de la llamada o no.

Se pueden presentar dos situaciones:

- Que el abonado que llama cuelgue primero: en ese caso se considera la conversación terminada.

- Que el abonado llamado cuelgue (por ejemplo para cambiar de aparato telefónico); en ese caso la central local inicia un tiempo de supervisión (por ejemplo de 90 segundos) pasado el cual la comunicación es desconectada.

D) Tarifación

Esta función varía de una empresa prestadora del servicio a otra, y de acuerdo al tipo de llamada. Para nuestro país podemos decir que:

- Conecta el contador de pulsos cuando el abonado llamado responde.

- Desconecta dicho contador cuando la comunicación finaliza.

- Actualiza la cuenta del abonado llamado.

E) Conversión Analógica-Digital

El bucle de abonado sigue manejando señales analógicas; por lo tanto en alguna etapa de la transmisión telefónica debe hacerse la conversión de señal analógica a digital (ya que el procesamiento de

dicha señal dentro de la central es de esa naturaleza); y viceversa. Esta conversión se realiza en el denominado circuito de abonado, el cual se puede encontrar dentro del propio edificio de la central.

F) Función de control

Esta función es realizada por un Programa de Control Almacenado (SPC). Esto significa que es una computadora (mediante varios programas) la que lleva a cabo el trabajo del control de la central:

- Detecta y analiza eventos en la conmutación.
- Decide las mediciones a realizar.
- Toma decisiones (por ejemplo en el control de las llamadas).

2.5.3.3.1.2. Funciones Extras

A) Operación y Mantenimiento

Operación: tareas para el desenvolvimiento normal del sistema.

Estas tareas deben ser realizadas para proporcionar una calidad de servicio adecuada al menor costo posible. La operación requiere información de parte del sistema.

Mantenimiento: medidas que se deben tomar debido a fallas en el sistema. Puede ser correctivo, preventivo o predictivo.

Todas estas funciones pueden ser controladas a distancia desde un centro especial de O&M.

B) Suministro de Energía

Todo el sistema telefónico se alimenta de energía eléctrica. Podemos dividir la necesidad de alimentación en:

- Alimentación de equipo de conmutación (corriente continua).
- Alimentación del resto del equipo telefónico (incluida la línea de abonado).

C) Funciones Remotas

En orden a simplificar funciones, reducir costos de instalaciones, acercarse digitalmente lo más posible al abonado, etc., es que se pueden extraer de la central algunas de las funciones, y ubicarlas en lo que se denomina Unidad Remota de Abonado (URA).

2.5.3.4. Componentes de la Red Telefónica

En síntesis, el sistema telefónico consiste en tres componentes principales:

- **Lazos de abonado.**
- **Troncales.**
- **Oficinas o nodos de conmutación.**

2.5.3.4.1. Lazos de Abonado

Por bucle o lazo de abonado (*suscriber loop*) entendemos el equipamiento de la red telefónica que constituye una línea (circuito) exclusivamente dedicada a un abonado; por lo tanto estos recursos no son compartidos con los demás abonados de la red.

Este bucle comprende el tramo que va desde el circuito de línea de abonado (que puede estar en la central local o en una etapa remota) hasta las instalaciones domiciliarias del usuario. Es el medio conductor por el cual se transmiten todas las señales hacia y desde el terminal de abonado (analógico) incluyendo la comunicación en sí.

Por lo tanto es el tramo de la red telefónica que aún se conserva analógico.

Debido a la gran difusión del servicio telefónico este bucle tiene características especiales. Podemos destacar las más importantes en la siguiente numeración:

- Es responsable de más del 50% de la inversión total de una nueva línea.
- La distribución geográfica y la concentración de abonados es muy variable, como así también el proceso de altas y bajas en las conexiones.
- Diferencias en el tipo de abonados (*residencial /comercial*).
- La mayor distancia de un abonado a la central local no debería ser motivo de mayores costos para éste (aunque lo sea para la compañía telefónica).
- En este bucle es donde se pueden producir la mayoría de las interferencias e interrupciones en el servicio.

Alternativas de realización

A) Cable de pares de cobre

Es la realización convencional para cuando el abonado está cerca de la central local (aproximadamente 10 kms.); típicamente utilizado para abonados urbanos. Debe entenderse que este par de cobre llega hasta alguna etapa *concentradora/conversora*, y que de allí hasta la central puede reemplazarse por algún otro tipo de conductor (cable multipar, coaxil, fibra óptica o radioenlace).

B) Conexión vía radio

Es la mejor relación *beneficio/costo* para abonados alejados de la central local (rurales), y es la única posible para abonados que requieran movilidad.

Es una opción más rápida de instalar y que soluciona el problema de acceso de abonados en lugares en donde la red de pares ya está saturada.

Redes Primaria y Secundaria

El bucle de abonado, en su parte exterior a la central es llamado también "red de acceso". Ésta debe ser suficientemente flexible para permitir el crecimiento del número de abonados conectados a la central.

Por lo tanto habrá que organizar muy bien el tendido y la cantidad de los conductores de los cuales va a constar esta red de acceso.

Para ello se la divide en tres partes, las cuales pueden verse en la **figura 5.6**.

A) Red Primaria

Comprende desde el repartidor general (ubicado dentro de la misma central local) hasta los armarios o subrepartidores. Está soportada por cables multipares, coaxiles, conductores de fibras ópticas o radioenlaces.

B) Red Secundaria

Comprende desde los armarios hasta los puntos de distribución. Casi exclusivamente se usan cables multipares.

C) Red de Dispersión

Es la última etapa hasta el abonado. Su realización más difundida es la de cables de pares de cobre; hoy se está intentando con acceso inalámbrico (también llamado RRL, o *Radio in the local Loop*).

2.5.3.4.1.3. Elementos en el Lazo de Abonado

El lazo o bucle de abonado puede contener diversos elementos dependiendo de la realización tecnológica y de la distancia del abonado a la central local, según pudo verse en la **figura 2.5.6**.

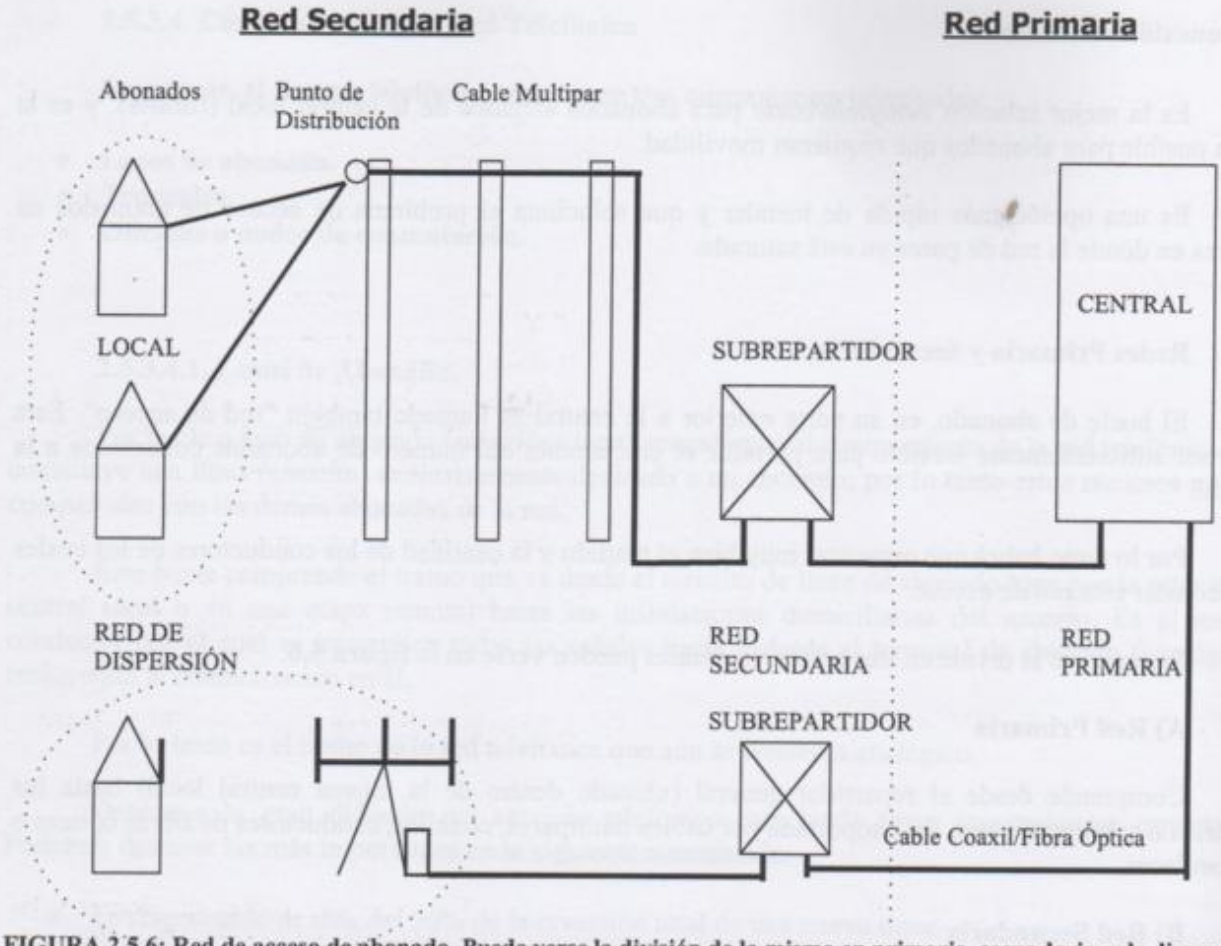


FIGURA 2.5.6: Red de acceso de abonado. Puede verse la división de la misma en primaria, secundaria y de dispersión. La red de dispersión puede estar realizada con conductores de pares de cobre o con acceso inalámbrico (fijo).

A) Punto de Distribución

Generalmente conocido como caja de distribución o caja terminal en donde hay espacio para 10 conexiones de abonados. A ella llegan los pares de cobre de abonado y sale un cable multipar de nx10 pares. (Ver **Figura 2.5.7**)

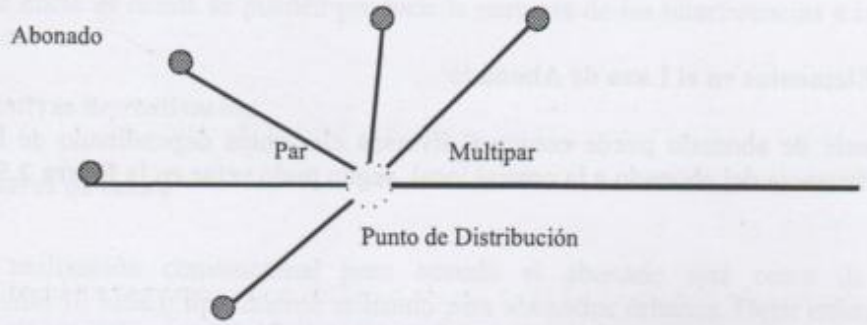


FIGURA 2.5.7: Esquema del Punto de Distribución. Se observa que la salida se implementa sobre un multipar.

B) Subrepartidor

Cumple funciones de reconfiguración de los lazos e interfaz entre distintos tipos de cables; a él llegan los cables trayendo 10 pares y pueden salir cables con, por ejemplo, 50 pares, o incluso cambiar de tipo de cable (a coaxil). (Ver **figura 2.5.8**) Puede ser que en una red muy densa existan varios niveles de subrepetidores.

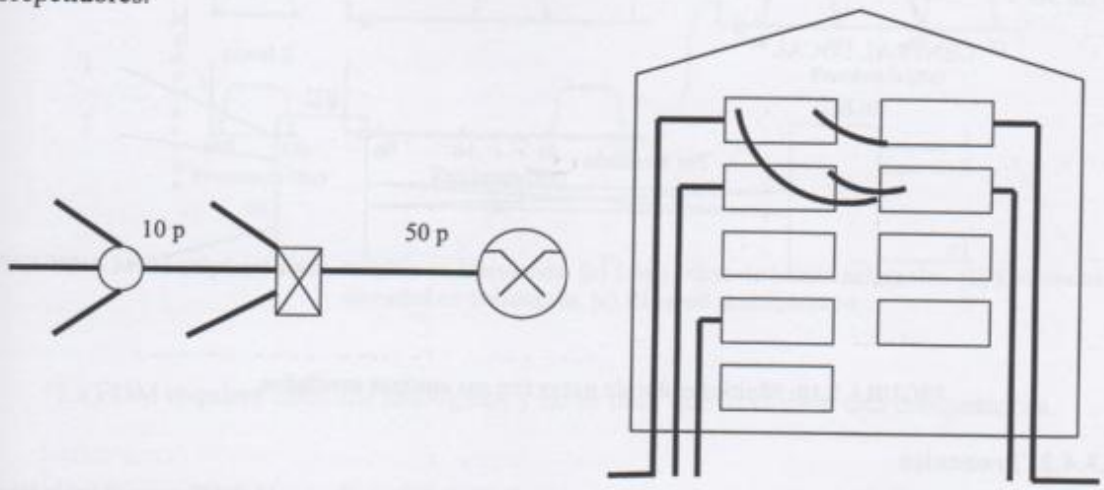


FIGURA 2.5.8: (a) Esquema en cascada donde se ven los puntos de distribución asociados a un subrepartidor. (b) Gabinete para subrepartidor ubicado en la calle.

C) Multiplexor

Es un equipo que "junta" (multiplexa) las señales que le llegan por los cables multipares y las transmite por algún otro medio físico. Si tiene "m" circuitos de entrada, deberá tener "m" circuitos de salida. En él se realiza además la conversión de señal analógica a digital. (Ver **figura 5.9**)

D) Concentrador

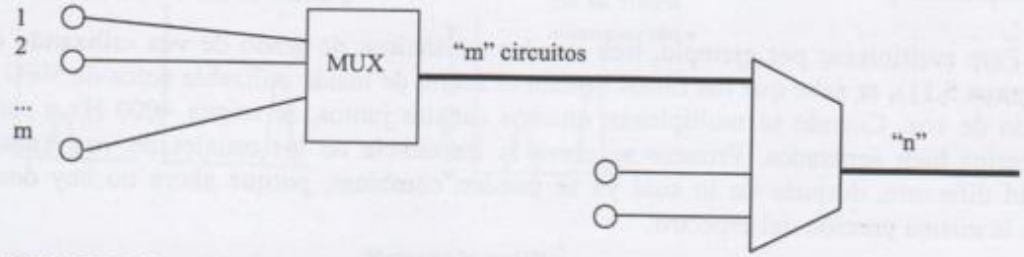


FIGURA 2.5.9: Vemos cómo los multiplexores pueden funcionar en conjunto con los concentradores. Tiene "n" circuitos de salida para "m" circuitos de entrada, siendo m > n. Relaciones de concentración usuales son 4:1 y 8:1.

E) Multiplicador de Pares

Permiten la transmisión simultánea de 2/4 circuitos telefónicos por un par de hilos de cobre (par de abonado). Por eso se lo llama también Sistema de Ganancia de Pares (PGS).

Cada sistema multiplicador de pares está compuesto por dos equipos (Ver **figura 5.10**):

- Unidad del lado de la central local (EU).
- Unidad del lado del abonado (RU).

Este último y los 2, 4 o hasta 12 aparatos telefónicos son telealimentados desde el equipo EU con una tensión de 90 V.

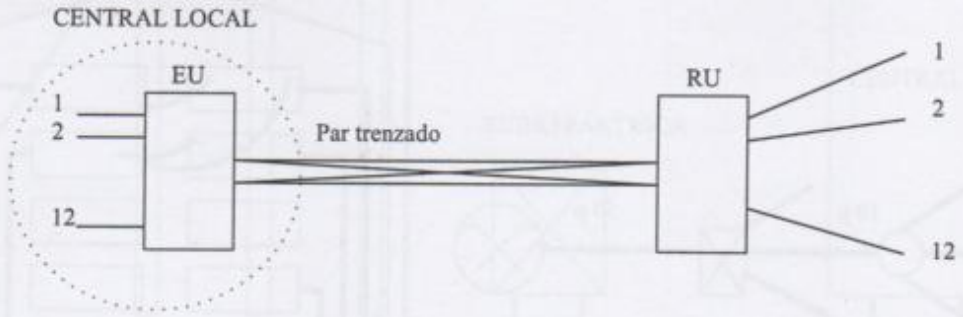


FIGURA 5.10: Multiplicador de pares con sus equipos asociados.

2.5.3.4.2. Troncales

Las compañías de teléfonos han desarrollado esquemas elaborados para multiplexar muchas conversaciones en un solo troncal físico. Estos **esquemas de multiplexión** se pueden dividir en dos categorías:

- **Multiplexión por división en frecuencia (FDM).**
- **Multiplexión por división en tiempo (TDM).**

A) Multiplexión por División en Frecuencia

Para multiplexar por ejemplo, tres canales telefónicos de grado de voz utilizando este esquema (Ver **figura 5.11**), se sabe que los filtros limitan el ancho de banda utilizable cerca de 3000 Hz por canal de grado de voz. Cuando se multiplexan muchos canales juntos, se asigna 4000 Hz a cada canal para mantenerlos bien separados. Primero se eleva la frecuencia de los canales de voz, cada uno en una cantidad diferente, después de lo cual ya se pueden combinar, porque ahora no hay dos canales que ocupen la misma porción del espectro.

Los esquemas de FDM que se emplean en el mundo están normalizados hasta cierto punto. Un estándar muy difundido es el de 12 canales de voz a 4000 Hz multiplexados dentro de una banda de 60 a 108 kHz. Esta unidad se llama **grupo**. La banda de 12 a 60 kHz a veces se usa para otro grupo. Muchas portadoras ofrecen un servicio de líneas alquiladas de 48 a 56 kbps que se basan en este grupo. Se pueden multiplexar cinco grupos (60 canales de voz) para formar un **supergrupo**. La siguiente unidad es el **grupo maestro**, que se compone de cinco supergrupos (en el estándar del CCITT) o de 10 supergrupos (en el sistema Bell).

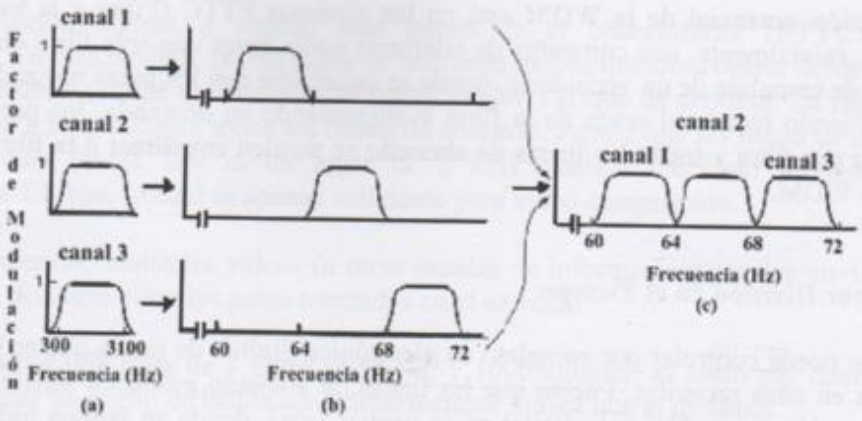


FIGURA 5.11: Multiplexión por división en frecuencia. (a) Los anchos de banda originales. (b) Los anchos de banda elevados en frecuencia. (c) El canal multiplexado.

La FDM requiere circuitos analógicos y no es fácil que lo efectúe una computadora.

Multiplexión por División en Longitud de Onda

Para los canales de fibra óptica se utiliza una variante de la multiplexión por división en frecuencia, llamada **WDM (Multiplexión por división en longitud de onda)**. Dos fibras llegan juntas a un prisma (rejilla de difracción), cada una con su energía en una banda diferente. Los dos haces pasan a través del prisma o rejilla, y se combinan en una misma fibra compartida para ser transmitidos a un destino distante, donde se dividirán de nuevo. (Ver **figura 5.12**)

La única diferencia respecto a la FDM eléctrica es que un sistema óptico que usa una rejilla de difracción es totalmente pasivo y, por ello, altamente confiable.

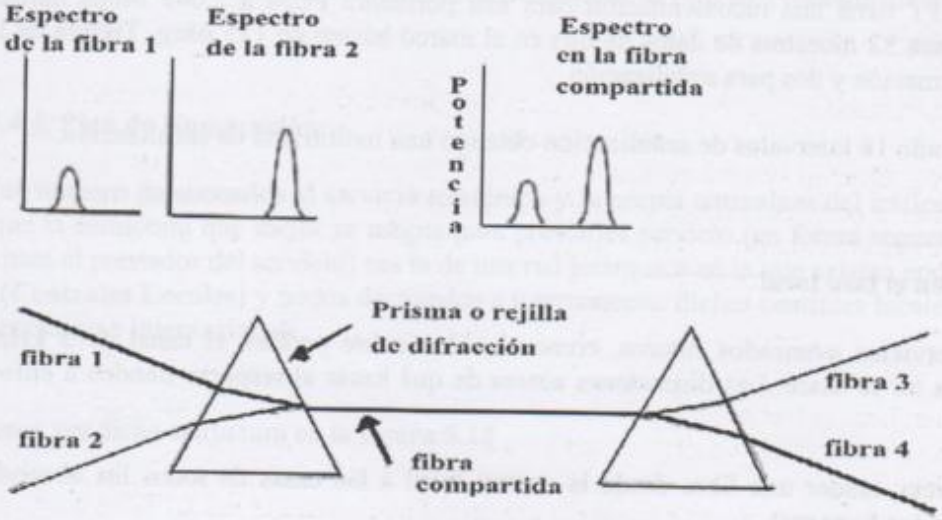


FIGURA 5.12: Multiplexión por división en longitud de onda.

Una aplicación potencial de la WDM está en los sistemas FTTC (Fibra a la banqueta) que se describieron antes. Inicialmente, una compañía de teléfonos podía tener una sola fibra desde una central local hasta la caja de empalme de un vecindario, donde se conectaba con los pares trenzados de las casas. Años después, habiendo bajado el costo de la fibra y aumentando su demanda, los pares trenzados se pueden reemplazar por fibra y todos las líneas de abonado se pueden empalmar a la fibra que llega a la central empleando WDM.

B) Multiplexión por División en el Tiempo

La TDM se puede controlar por completo en electrónica digital, de modo que se ha extendido en forma más amplia en años recientes. Puesto que las líneas de abonado producen señales analógicas, se requiere una conversión de analógico a digital en la central local, donde se reúnen todas las líneas de abonado individuales para combinarse en troncales de salida.

Las señales analógicas se digitalizan en la central local con un dispositivo llamado **codec** (codificador-decodificador), con lo que se producen números de 7 u 8 bits. El codec toma 8000 muestras por segundo (125 µseg/muestra) porque el teorema de Nyquist dice que esto es suficiente para capturar toda la información del ancho de banda de 4 kHz del canal telefónico. Esta técnica se llama **PCM (Modulación de código de pulso)**. La PCM es el corazón del sistema telefónico moderno. En consecuencia, virtualmente todos los intervalos de tiempo dentro del sistema telefónico son múltiplos de 125 µseg.

Cuando la transmisión digital empezó a surgir como una tecnología factible, el CCITT fue incapaz de lograr un acuerdo respecto al estándar internacional para la PCM. En consecuencia, ahora se usan diversos esquemas incompatibles en diferentes países alrededor del mundo.

Un método muy utilizado en Estados Unidos y Japón es el de la portadora T1, la cual tiene 24 canales y nos da una tasa de 1,5 Mb/s.

El CCITT tiene una recomendación para una portadora PCM a 2,048 Mbps llamada **E1**. Esta portadora empaca 32 muestras de datos de bits en el marco básico de 125 µseg. Treinta de los cuales se usan para información y dos para señalización.

Agrupando 16 intervalos de señalización obtengo una multitrama de señalización.

Fibra Óptica en el lazo local

Para servicios avanzados futuros, como el video sobre pedido, el canal de 3 kHz que se usa actualmente ya no se usará. Las discusiones acerca de qué hacer al respecto tienden a enfocarse en dos soluciones.

La directa, tender una fibra desde la central local a las casas de todos los abonados, se llama **FTTH (fibra a los hogares)**.

Esta solución se ajusta bien al sistema actual pero en lo económico no será viable durante décadas; simplemente será muy costosa.

Una solución alterna y mucho más barata es el concentrador (**FTTC: fibra hasta el concentrador**). En este modelo, la compañía de teléfonos instala una fibra óptica desde cada central local hasta cada vecindario (donde se encuentra el concentrador) al que da servicio. La fibra termina en una caja de empalme a la que llegan todos las líneas de abonado. Puesto que las líneas de abonado son ahora mucho más cortas (quizá 100 m en lugar de 3 km), pueden funcionar a velocidades mayores, probablemente a 1 Mbps, lo cual es apenas suficiente para video comprimido.

De esta manera, múltiples videos (u otros canales de información) pueden enviarse por la fibra a alta velocidad y dividirse entre los pares trenzados en el extremo.

Al compartir una fibra de 1 Gbps entre 100 y 1000 clientes, el costo por cliente se reduce y se puede proporcionar un ancho de banda considerablemente mayor que el de ahora.

Las velocidades mayores de 1 Mbps no pueden mantenerse a largas distancias con los pares trenzados existentes, así que, a largo plazo, todos los pares trenzados se tendrán que reemplazar por fibra.

2.5.3.4.3. Oficinas o Nodos de Conmutación

Son centrales de conmutación de una red de telecomunicaciones. Se tiene:

- **Central Local:** central en la que terminan las líneas de los abonados.
- **Central de Tránsito:** central que permite establecer conexiones entre centrales locales.
- **Centros Interurbanos:** central que permite establecer conexiones entre ciudades.
- **Central Internacional:** central (situada en uno de los extremos de un circuito telefónico internacional) que conmuta una comunicación precedente de otro país o destinada a él.

2.5.3.4.4. Plan de Numeración

El gran número de abonados al servicio telefónico y la propia naturaleza del tráfico generado por éstos, hace que la estructura que mejor se adapta para prestarles servicio (en forma segura, eficaz y a la vez rentable para el prestador del servicio) sea la de una red jerárquica en la que existen nodos próximos a los usuarios (**Centrales Locales**) y nodos destinados a interconectar dichas centrales locales (**Centros de Tránsito** interurbano e internacional).

Podemos ver dicha estructura en la **figura 5.13**

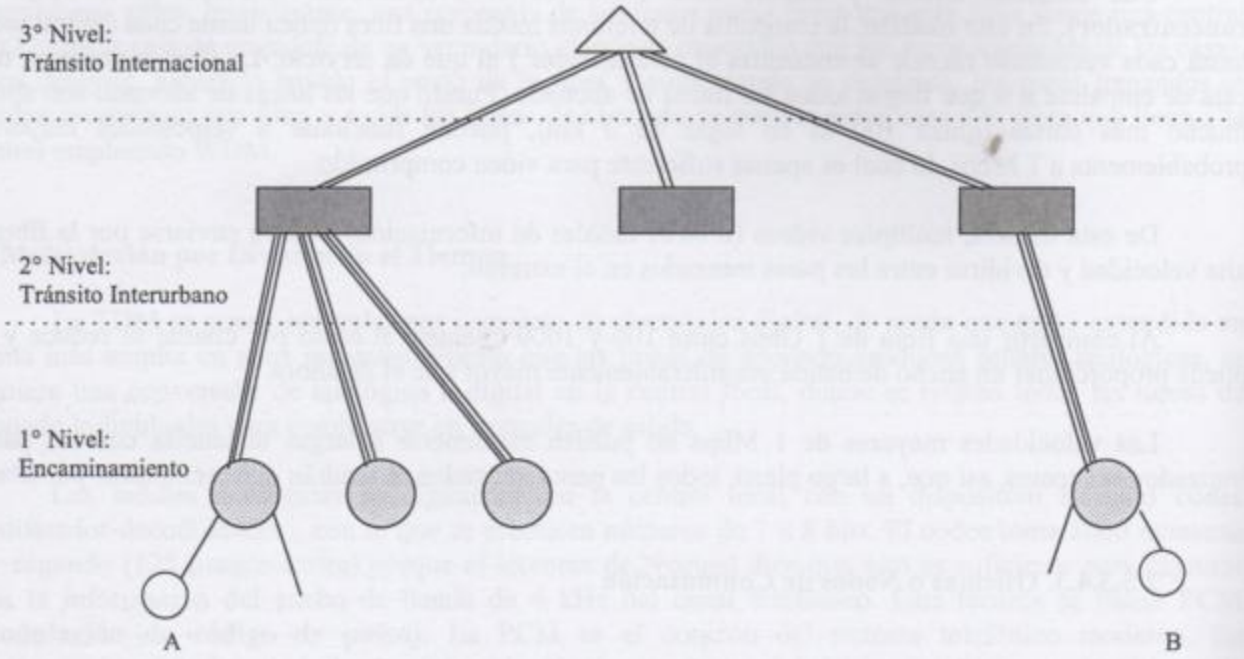


FIGURA 5.13: Estructura Jerárquica de la red telefónica.

La red telefónica funciona estableciendo una conexión por conmutación de circuitos entre el abonado que llama (A) y el abonado llamado (B). Estos pueden pertenecer a centrales locales diferentes, incluso muy distantes una de otra.

Para el encaminamiento de la llamada la Central Local a la cual está conectado el abonado A recibe de éste los números correspondientes al abonado llamado B y debe establecer la ruta más conveniente hacia ese destino.

El número de abonado consta de varias partes que identifica de manera unívoca a dicho abonado B, a la Central Local a la cual pertenece dicho abonado y al área geográfica donde está ubicada dicha central. Para comprender mejor las partes de que está compuesto el número de B analizaremos tres casos.

5.3.4.4.1. Llamada Urbana

Todo abonado al servicio telefónico es reconocido por su propia central local, de entre los 10.000 abonados a los que atiende, por cuatro dígitos agrupados en una estructura conocida como:

M C D U

Donde M: unidad de **M**il
C: **C**entena
D: **D**ecena
U: **U**nidad

A su vez la central origen debe identificar a qué central pertenece B. Esto lo lleva a cabo gracias a los dígitos que identifican a la central local. Para ello se pueden usar uno, dos y hasta tres dígitos según la cantidad de centrales que haya que identificar.

$4(X_1 X_2) X_3$	MCDU
Número de Central	Número de B

Además de ello hay que agregarle el número **"4"** que identificará al abonado como perteneciente a la red fija.

2.5.3.4.4.2. Llamada Interurbana

Para llamadas interurbanas nuestro país ha adoptado el sistema **"numeración cerrado"**, lo cual implica que todos los números de comunicaciones interurbanas deben contener la misma cantidad de dígitos (once).

El mismo debe comenzar con el prefijo de larga distancia (**"0"**) seguido por el **"código de área"** de la central local a la que pertenece el abonado B; este número constará de dos, tres o cuatro cifras, para acomodar la longitud del número de abonado a las exigencias del plan de numeración cerrado.

Supongamos tres ejemplos:

Localidad pequeña: 0 | 3543 | 4 X_3 MCDU

Ciudad: 0 | 351 | 4 $X_2 X_3$ MCDU

Gran centro urbano: 0 | 11 | 4 $X_1 X_2 X_3$ MCDU

La misma estructura deberán seguir los números de servicios de red inteligente:

Cobro revertido: 0 800 888 MCDU

Telefonía celular: 0 351 (15) 676 MCDU

2.5.3.4.4.3. Llamada Internacional

Se debe anteponer el prefijo de comunicaciones interurbanas **("00")** y a continuación el código identificador de país, para lo cual se utilizará uno, dos o tres dígitos, y luego el número de abonado llamado, el cual tendrá una estructura que dependerá del plan de numeración adoptado en dicho país.

00 34 ----------

La recomendación de ITU es que el número de abonado internacional no posea más de doce (12) dígitos.

2.5.3.5. Uso de la Red Telefónica para transmisión de datos

Éste puede hacerse de varias formas diferentes:

- Mediante el uso directo de la red telefónica conmutada **(circuitos conmutados (*dial-up*))**.
- Mediante el uso de líneas dedicadas **(circuitos arrendados punto a punto)**.
- Mediante el incremento del ancho de banda de la línea de abonado **(líneas digitalizadas de banda ancha:** HDSL, ADSL, etc)

2.5.3.5.1. Circuitos Conmutados[31]

El uso de estos circuitos representa uno de los usos más extendidos, para hacer efectiva una comunicación de datos. (Ver **figura 5.14**)

[31] En Inglés: Dial Up.

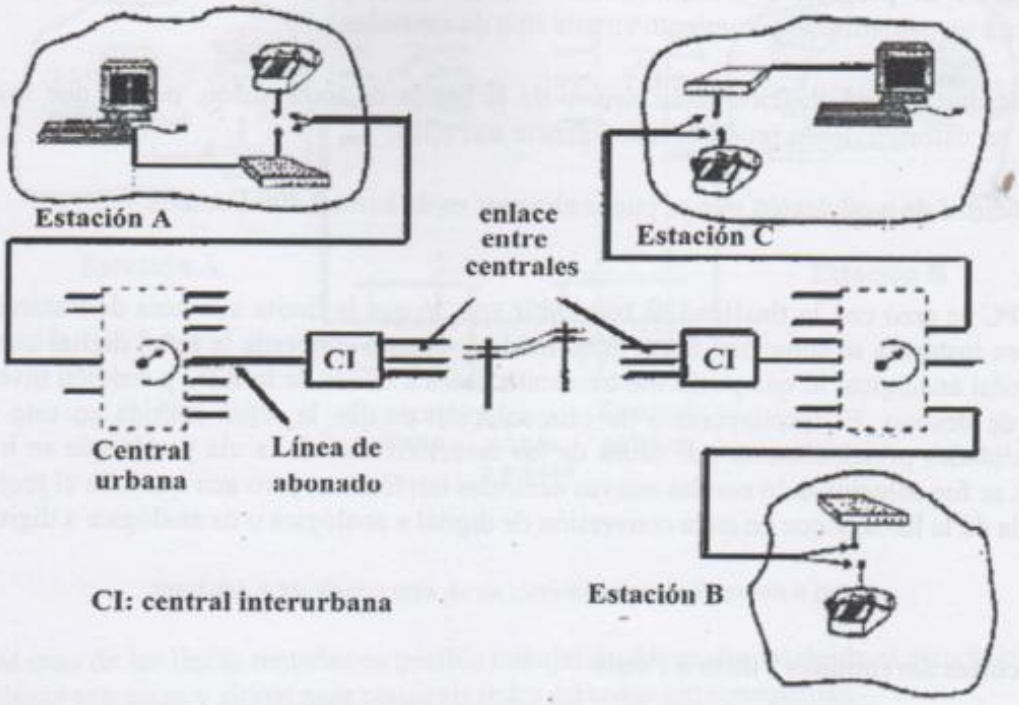


FIGURA 5.14: Estructura de un circuito conmutado.

Si bien los troncales de larga distancia ya son digitales, los lazos locales todavía son analógicos y es probable que permanezcan así por lo menos un tiempo, debido al enorme costo de convertirlos. En consecuencia, cuando una computadora desea enviar datos digitales por una línea de discado, los datos se deben convertir primero a la forma analógica mediante un **módem** para transmitirse por el lazo troncal o la línea de abonado, luego convertirse a la forma digital para transmitirse por los troncales de largo alcance, después reconvertirse a analógico en el lazo local del extremo receptor y, por último, a digitales con otro módem para almacenarse en la computadora de destino.

Precisamente su flexibilidad radica en la posibilidad de establecer, a partir de un punto sobre la red en donde está instalado el equipo terminal de datos (DTE: terminal o computadora), circuitos diferentes de acuerdo a los requerimientos que solicite cada usuario.

Características especiales:

- Esta transmisión no puede ser preacondicionada por cuanto los circuitos que se usan y el enrutamiento, podrán cambiar en cada comunicación que se establezca (se ignora el camino que seguirán).
- El enlace se desconecta una vez que se termina la comunicación.
- Las líneas llegan hasta los abonados a dos hilos, por lo que pueden existir en su recorrido intercaladas bobinas híbridas. Este hecho es una de las razones por las cuales estos circuitos tienen poca calidad en comparación con los circuitos arrendados punto a punto.
- Existe a menudo ruido impulsivo, el cual será tanto mayor, como mayor sea el número de centrales de tecnología electromecánica que están incluidas en el enrutamiento del circuito

establecido. El progresivo reemplazo de estas centrales, por otras de tecnología electrónica, producirá un paulatino mejoramiento en este tipo de centrales.

- Los sistemas de señalización están dentro de la banda de transmisión, por lo que los equipos usados en datos no deben producir interferencia con ellos.

- La velocidad de modulación que se puede alcanzar es de hasta 2.400 Baudios.

La RTPC se creó con la finalidad de transmitir voz, lo que la limita a la hora de transmitir datos. Esto en primera instancia se solucionó a través de módem, el cual convertía la señal digital que emite el ordenador a señal analógica, lo que posibilita transmitir datos a través de la RTC y función inversa hacia el ordenador de destino. El inconveniente de esta solución es que la señal emitida en este viaje iba perdiendo cualidades principalmente por causa de las características de la vía por la que se transmitía. Este problema se fue solucionando con las nuevas centrales telefónicas, pero aun quedaba el problema del ancho de banda de la línea, y que en cada conversión de digital a analógica o de analógica a digital, pierde calidad.

2.5.3.5.2. Circuitos arrendados Punto a Punto

El uso de éstos sobre la red telefónica, representa uno de los usos más extendidos, para hacer efectiva una comunicación de datos, entre dos puntos geográficos. (Ver **figura 5.15**) Dado que no resulta necesario tener facilidades de conmutación, hace a estos circuitos muy convenientes por cuanto a través de ellos, se puede obtener mejor calidad de transmisión.

Características especiales:

- Estas líneas también reciben el nombre de **circuitos dedicados**, **permanentes** o **privados**.

- Están a disposición del usuario las 24 hs.

- Están conectadas a través de centrales locales a las que tributan las líneas de abonado de las estaciones que están conectadas entre sí. Pero las mismas no pasan por sus dispositivos de conmutación. Por esta razón no están afectadas por ruido impulsivo como en el caso de las líneas conmutadas.
- En muchos casos, poseen dispositivos especiales que disminuyen las perturbaciones y la distorsión.

- Al seleccionar el enrutamiento, se busca obtener las menores pérdidas, buscando el par de abonado y/o troncal (también llamado oficina) entre los mejores disponibles, de la misma manera con los circuitos interurbanos, etc.

- Se pueden obtener mejores velocidades de modulación que en las líneas conmutadas. Éstas dependen de que si las líneas son de a dos o a cuatro hilos y a la norma de calidad que cumplen.

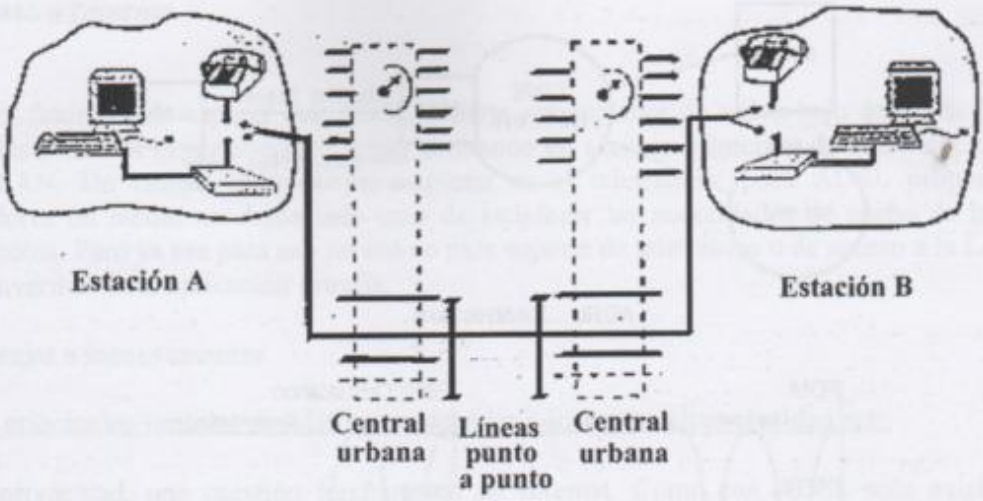


FIGURA 5.15: Estructura de un circuito arrendado punto a punto.

En el caso de las líneas rentadas es posible trabajar en forma digital desde el principio hasta el fin, pero estas líneas son caras y sirven para construir redes privadas intracompañías.

2.5.3.5.3. Líneas digitales de banda ancha (HDSL)

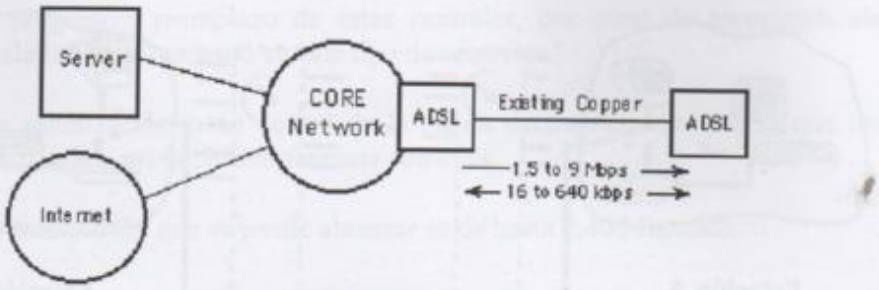
Se puede incrementar notablemente la capacidad de las líneas telefónicas existentes utilizando técnicas de modulación apropiada que aumenten la tasa efectiva de bits enviadas por una línea telefónica existente. Para ello hay que colocar en ambos extremos de la línea (tanto en la central telefónica como en la casa del abonado) unos equipos especiales (llamados modems HDSL) que realizarían esta función de modulación.

Según que el ancho de banda sea el mismo, o distinto para el enlace de subida que el de bajada, el servicio tiene variantes; la más común es el ADSL, que describiremos a continuación

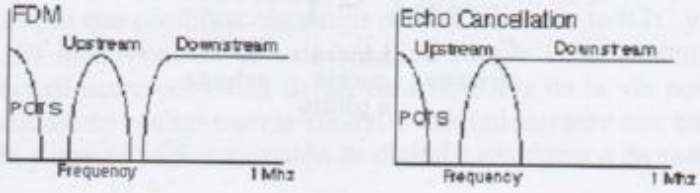
ADSL utiliza técnicas de codificación digital que permiten ampliar el rendimiento del canal telefónico cuyo ancho de banda puede llegar a 1,1 MHz, utilizando el cableado telefónico actual. Para conseguir estas tasas de transmisión de datos, la tecnología ADSL establece tres canales independientes sobre la línea telefónica estándar:

- Dos canales de alta velocidad (uno de recepción de datos y otro de envío de datos). Y un tercer canal para la comunicación normal de voz (servicio telefónico básico).
- Los dos canales de datos son asimétricos, es decir, no tienen la misma velocidad de transmisión de datos. El canal de recepción de datos tiene mayor velocidad que el canal de envío de datos.

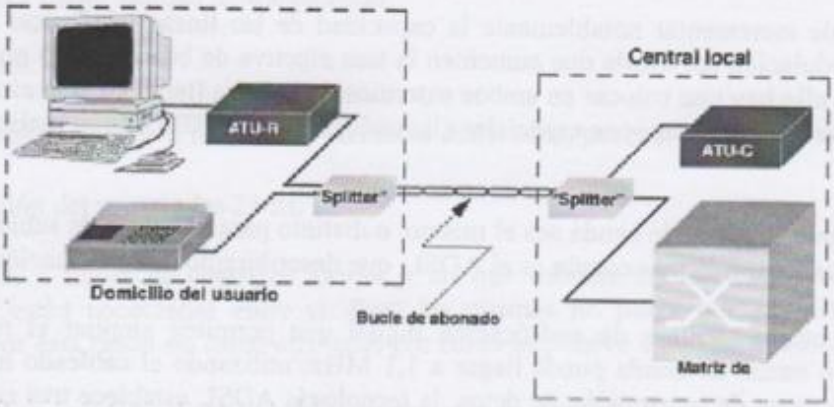
Esta asimetría, característica de ADSL, permite alcanzar mayores velocidades en el sentido red - usuario, lo cual se adapta perfectamente a los servicios de acceso a información (ej. Internet) en los que normalmente, el volumen de información recibido es mucho mayor que el enviado.

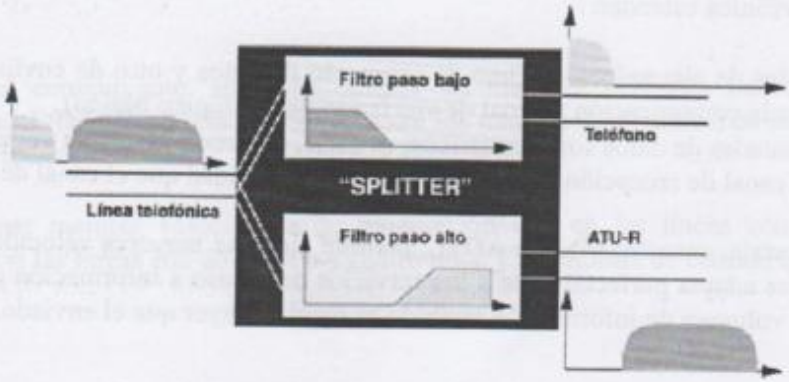


ADSL Connection



En el servicio ADSL, el envío y recepción de datos se establece desde el ordenador del usuario a través de un módem ADSL. Estos datos pasan por un filtro (splitter), que permite la utilización simultánea del servicio telefónico básico (RTC) y del servicio ADSL. Es decir, el usuario puede hablar por teléfono a la vez que esta navegando por Internet.





Acceso a Internet

En el futuro es de esperar que ADSL soporte aplicaciones de vídeo bajo demanda (VoD), en la actualidad las primeras experiencias se están centrando en accesos a Internet de alta velocidad y acceso remoto a LAN. Un campo también por explotar es el teletrabajo, pues ADSL proporciona a los administradores un medio no demasiado caro de satisfacer las necesidades de ancho de banda de sus accesos remotos. Pero ya sea para uso privado o para soporte de teletrabajo o de acceso a la LAN, Internet ya se ha convertido en la aplicación estrella.

Ventajas e inconvenientes

Las principales ventajas de ADSL para acceder a Internet a alta velocidad son:

- La privacidad, una cuestión fundamental en Internet. Como con ADSL sólo existe una única conexión punto a punto entre cada cliente y la red, nadie podrá ver los datos ajenos. Y, aunque no es imposible, resulta muy difícil piratearlos deliberadamente dada la compleja naturaleza de la tecnología de las señales ADSL.

- La calidad del servicio ADSL. Puesto que cada conexión es punto a punto, la calidad es constante para cada usuario.

- Las alianzas que los operadores están creando con las más destacadas firmas de software. Eso ha ocurrido entre GTE y Microsoft a fin de lanzar una experiencia precomercial conjunta. El punto central del acuerdo reside en el protocolo PPTP (Point-to-Point Tunneling Protocol) que Microsoft desarrolló con otras firmas. Con este protocolo el tráfico del cliente remoto se encapsula en tramas PPTP seguras para ser transmitidas por Internet. Y como las tramas PPTP sólo pueden ser decodificadas por el servidor de accesos corporativos apropiado, es posible configurar redes privadas virtuales sobre Internet.

Los principales inconvenientes son los siguientes:

- La tecnología ADSL no contribuirá a eliminar los cuellos de botella causados por los actuales módems.

- Tienen una velocidad inferior a los módems de cable que operan en un rango de velocidades de 10 a 30 Mbps. Además esta tecnología resulta más barata tanto por razones de equipamiento como de configuración.

- ADSL plantea el problema técnico y comercial de que sólo opera a distancias de hasta 6 kilómetros y medio. Y si los operadores han de instalar repetidores digitales en el bucle local para poder llegar hasta los usuarios, es evidente que los costes subirán substancialmente.

- El ancho de banda es asimétrico (es mayor en el sentido de la Internet hacia el usuario) lo cual lo hace inviable para empresas que provean servicios en Internet (como hosting, web mail, etc)

2.5.3.6. Red Digital Integrada

La digitalización de la red telefónica analógica ha dado lugar a la Red Digital Integrada (RDI)[32] en la que lo único que no es digital son las líneas de acceso de los abonados (bucle de abonado). La evolución de la RTPC hacia una red digital se dio primero en los enlaces troncales.

Años 60:

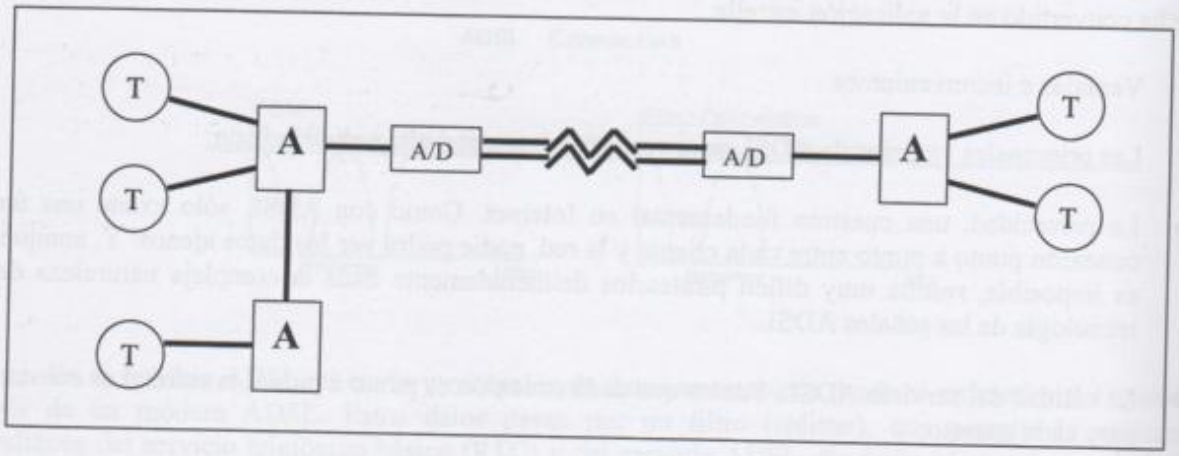


FIGURA 5.16. (T: teléfono)

Años 70:

Posteriormente aparecieron las centrales digitales, que utilizan computadoras y otros sistemas digitales. Éstas son menos propensas a fallos que las centrales analógicas y permiten además controlar más líneas de usuarios y realizar las conexiones mucho más rápidamente. En estas centrales la voz se almacena y se transmite como información digital, y es procesada por programas informáticos.

Hasta hoy se han solventado las necesidades de comunicación de datos, con la RTC, Red de Telefonía Conmutada, y con líneas Punto a Punto tanto analógicas como digitales, éstas últimas considerablemente más caras. También se proporcionaron servicios de paquetes como X.25, etc.

Años 80:

Las compañías telefónicas se enfrentan a un nuevo desafío. Las grandes empresas están interesadas en poder interconectar sus computadores, para satisfacer esta nueva demanda se crean las primeras redes experimentales de transmisión de datos.

[32] En Inglés: IDN (Integrated Digital Network)

2.5.4. Frame Relay

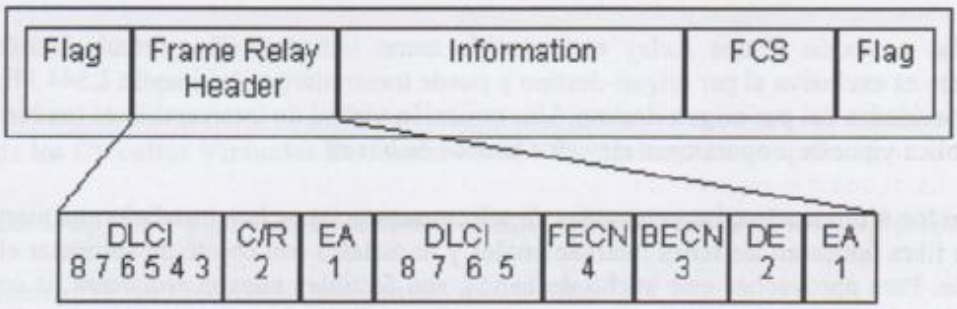
Frame Relay **(retransmisión de marco)** es un servicio para personas que quieren una forma lo más austera posible, orientada a la conexión, para mover bits de *A* a *B* a una velocidad razonable. Su existencia se debe a cambios en la tecnología en las últimas dos décadas. Hace 20 años, las comunicaciones a través de líneas telefónicas era lenta, analógica y no confiable, y las computadoras eran lentas y caras. En consecuencia, se requirieron protocolos complejos para enmascarar los errores, ya que (como X.25) las computadoras de los usuarios eran demasiado caras para ponerlas a hacer este trabajo.

La situación ha cambiado en forma radical. Ahora, las líneas telefónicas rentadas son digitales, poseen un buen ancho de banda y son confiables, y las computadoras son rápidas y baratas. Esto sugiere el uso de protocolos simples, con la mayor parte del trabajo realizado por las computadoras de los usuarios en vez de la red. Este es el ambiente para el que está pensado Frame Relay.

El estándar de Frame Relay, una extensión del estándar RDSI, es CCITT I.122. Además responde a las RFC 1490 y 2427

Es un protocolo de transmisión de paquetes de datos en ráfagas de alta velocidad a través de una red digital, fragmentados en unidades de transmisión llamadas **Frames**.

En la siguiente figura observamos un Frame y sus campos:



También, se puede pensar en Frame Relay como una **línea virtual rentada**. Es como una alternativa a las líneas alquiladas de ancho de banda fijo. El cliente renta un circuito virtual permanente entre dos puntos y entonces puede enviar marcos o *frames* (es decir, **paquetes**) de hasta 1600 bytes entre ellos. También es posible rentar circuitos virtuales permanentes entre un lugar determinado y muchas otras localidades, de modo que cada marco lleve un número de 10 bits que le diga cuál circuito virtual usar.

La diferencia entre una **línea rentada real** y una **virtual** es que, con una real, el usuario puede enviar tráfico durante todo el día a máxima velocidad. Con una línea virtual, se pueden enviar ráfagas de datos a toda velocidad, pero el uso promedio a largo plazo deberá ser inferior a un nivel predeterminado. A cambio, la portadora cobra mucho menos por una línea virtual que por una física.

Además de competir con las líneas rentadas, Frame Relay también compite con los circuitos virtuales permanentes de X.25, excepto que opera a altas velocidades, usualmente a 1.5 o 2 Mbps y ofrece menos funciones.

Sin embargo, Frame Relay no es sólo para el ahorro de costos: también puede ser implantada por una mejor calidad de servicio.

Frame Relay requiere una conexión exclusiva durante el período de transmisión. Esto no es válido para transmisiones de video y audio ya que requieren un flujo constante de transmisiones. Es una tecnología de paquete-rápido ya que el chequeo de errores no ocurre en ningún nodo de la transmisión, los extremos son los responsables del chequeo de errores. Los errores en redes digitales son extremadamente menos frecuentes en comparación con las redes analógicas. Proporciona un servicio mínimo que básicamente es una forma de determinar el inicio y el fin de cada marco y detectar errores de transmisión. Si se recibe un marco defectuoso, Frame Relay simplemente lo descarta. Corresponde al usuario descubrir que se perdió un bloque y emprender la acción necesaria para recuperarlo. A diferencia de X.25, no proporciona acuses de recibo ni control de flujo normal. Sin embargo, tiene un bit en el encabezado que un extremo de la conexión puede encender para indicar al otro que hay problemas. El uso de este bit es opción de los usuarios.

Una red Frame Relay puede ser altamente viable por poder escoger una nueva ruta en el caso del fallo de la línea y, por consiguiente un rico patrón de interconexión, además, puede reducir el número de saltos entre nodos intermedios dando tiempos de respuesta imprevistos.

Frame Relay transmite paquetes en el nivel de enlace de datos del modelo de Interconexión Sistemas Abiertos (OSI) antes que en el nivel de enlace de datos del modelo OSI. Distintamente a una celda, que es de tamaño fijo, un *frame* es variable en tamaño y puede ser tan largo como mil bytes o más.

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

En los últimos años, las compañías de telecomunicaciones han instalado una cierta abundancia de cables de fibra óptica en las redes internacionales y mundiales con objeto de aumentar el ancho de banda disponible. Para aprovechar este ancho de banda, son factibles nuevos esquemas de comunicación que eliminan la sobrecarga inherente a otros esquemas. Frame Relay lo consigue evitando el control de flujo y la gestión de errores dentro de la propia red, originadores de retardos. En comparativa, la antigua X.25 realiza una verificación exhaustiva de errores al asumir que se utilizan líneas telefónicas no fiables para la transmisión de datos. La eliminación de estas características en Frame Relay no presenta ningún problema, incluso cuando los errores hacen acto de aparición. Frame Relay asume que los nodos finales son máquinas programables que pueden realizar su propia gestión de errores. Los sistemas finales no se encuentran sobrecargados con este control de errores debido a que generalmente se producen muy pocos. En contraste, X.25, asumía que la red podría necesitar realizar esta acción debido a que los nodos finales consistían en terminales bobas conectadas a computadoras centrales.

En Frame Relay, los nodos intermedios (conmutadores) simplemente realizan una retransmisión de tramas a través de un trayecto predefinido. En X.25, los nodos intermedios deben recibir completamente cada paquete y realizar una verificación de errores antes de reenviarlo. Si existe un error, el nodo solicita una retransmisión desde el emisor. De esta forma, el emisor puede retransmitir un paquete tan pronto como se haya perdido. Las tablas de estado utilizadas por X.25 en cada nodo intermedio, que tratan la gestión, el control de flujo y la verificación de errores no son necesarias en Frame Relay. Si se produce la corrupción o pérdida de un paquete debido a la congestión en una red Frame Relay, el sistema receptor detectará la pérdida de la trama y solicitará la retransmisión.

Las redes Frame Relay ponen toda su energía en el movimiento de los paquetes. Los nodos de conmutación de la subred no realizan ningún tipo de corrección de errores, aunque pueden detectar paquetes corruptos. Los paquetes se descartan tras su detección. Frame Relay surgió como un avance o actualización a las nuevas necesidades de X.25. se hizo un estudio de las necesidades reales en retransmisión de datos a alta velocidad.

2.5.4.1. Características técnicas

- **Velocidad de acceso:** desde 64 Kbps a 2 Mbps.
- **Caudal (bidireccional) garantizado:** 8, 16, 32, 48, 64, 96, 128, 256, 512, 1024, 1536, 1984 Kbps.
- **Acceso alternativo RDSI:** para velocidades de hasta 256 Kbps, back-up de 64 Kbps a través de RDSI.
- **Gestión de Red:** permanente.
- **Soporte del Servicio:** permanente (ventanilla única).
- **Facilidades de Gestión de Cliente:** Informe de tráfico cursado y PC para Gestión de Cliente (PGC).
- **Interfaz física:** < 2 Mbps. V.35, V.36.
  = 2 Mbps. G.703/704.
- **Ámbito de los Circuitos Virtuales Permanentes (CVP):** nacional e internacional.
- **CVP de Back-up:** CVP plus. Ámbito nacional. Iguales atributos que el de los CVP estándar.
- Destino alternativo para reencaminamiento en caso de fallo.

2.5.4.2. Ventajas

Ahorro en los costos de telecomunicaciones

Con este servicio los usuarios podrán transportar simultáneamente, compartiendo los mismos recursos de red, el tráfico perteneciente a múltiples comunicaciones y aplicaciones, y hacia diferentes destinos.

Solución Compacta de Red

Según las necesidades del cliente, tras un estudio personalizado de las características del mismo, la empresa de telecomunicaciones realiza el diseño de la red de comunicaciones *frame relay*.

Servicio gestionado extremo a extremo

La propia empresa prestataria del servicio se ocupa de la configuración, administración, mantenimiento, supervisión y control permanente durante las 24 horas del día, los 365 días del año, tanto de los elementos de red como de módems, líneas punto a punto, etc.

Tecnología punta y altas prestaciones

Frame Relay proporciona alta capacidad de transmisión de datos por la utilización de nodos de red de alta tecnología y bajos retardos como consecuencia de la construcción de red (backbone) sobre enlaces a 34 Mbps y de los criterios de encaminamiento de la Red de Datos, orientados a minimizar el número de nodos de tránsito.

Flexibilidad del servicio

Es la solución adaptable a las necesidades cambiantes, ya que se basa en circuitos virtuales permanentes (CVP), que es el concepto de Red Pública de Datos, equivalente al circuito punto a punto en una red privada. Sobre una interfaz de acceso a la red se pueden establecer simultáneamente múltiples circuitos virtuales permanentes distintos, lo que permite una fácil incorporación de nuevas sedes a la Red de Cliente.

Servicio normalizado

Es un servicio normalizado según los estándares y recomendaciones de UIT-T, ANSI y Frame Relay Forum, con lo que queda garantizada la interoperatividad con cualquier otro producto Frame Relay asimismo normalizado.

2.5.4.3. Estudio comparativo de los tipos de redes en esquemas OSI

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

Sin entrar en detalles sobre el modelo OSI, que fue desarrollado por la Organización Internacional de Estandarización (ISO), llega con decir que el protocolo X.25 usa los niveles uno, dos y tres del modelo OSI., mientras que el protocolo Frame Relay, usa sólo los dos primeros:

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

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

- **Nivel 3,** el nivel de red, la unidad fundamental del intercambio de datos es el paquete. El nivel 3, prepara los *frames* de datos del nivel 2 en paquetes y rutas de datos a través de la red a través de circuitos virtuales permanentes (PVCs). El nivel 3 también realiza detección y corrección de

errores con peticiones de retransmisión de los *frames* y paquetes dañados. Este es el punto en el que X.25 y Frame Relay divergen. X.25 usa el nivel 3 en su totalidad, mientras que Frame Relay usa esencialmente sólo los niveles 1 y 2, La razón para esto es que Frame Relay está basado en la premisa de que las redes digitales son mucho menos propensas a errores que las que analógicas que había en el pasado. Esta premisa es debida exactamente al cambio a digital y a la fibra óptica.

Así por lo tanto con X.25, por el uso de los niveles altos del modelo OSI, ambos, detención de errores y corrección de errores, son usados en cada uno y en todos los nodos a lo largo de la ruta, lo que provoca que la velocidad de transmisión se vea severamente limitada, por ejemplo, pensemos que tenemos una conexión X.25, que va desde nuestra oficina principal a una oficina satélite y que pasamos a través de 3 compañías de telecomunicaciones. Bajo el uso de X.25 los datos son empaquetados y enviados al primer nodo. Los datos son chequeados, y en caso de errores, pide la retransmisión del paquete, en caso de no encontrarlos envía una señal de final al origen, y envía el paquete al siguiente nodo. Este proceso se repite en cada uno de los nodos, hasta llegar al destino, y el proceso vuelve a comenzar con el siguiente paquete.

Con Frame Relay, basado en redes mucho menos "contaminadas", la detección de errores es llevada a cabo, pero no la corrección. la red. Frame Relay simplemente toma cada *frame* de información y lo retransmite (relay) al siguiente nodo. Si, en raras ocasiones, se detecta un error, Frame Relay simplemente descarta el frame de datos erróneo y depende del nivel superior usado por controladores inteligentes en cada extremo de la red para pedir una retransmisión.

2.5.4.4. Topologías de conexión

Las dos características más destacadas entre los usuarios de Frame Relay son:

Poseen una red que interconecta LANs usando routers para circuitos alquilados o de ancho de banda controlado y están buscando reducción de costos o el crecimiento de la red. Las redes están basadas en topología de estrella.

Esta topología de estrella puede consistir de una estrella simple o múltiples estrellas, que pueden estar en una cascada, o estructura de árbol.

La razón para la configuración de estrella es, doble. Primeramente, esto refleja la estructura organizacional y flujo de datos de los negocios, con administración centralizada y funciones locales. Secundariamente, esto es impuesto por la tecnología de las líneas alquiladas.

El uso de Frame Relay abre las puertas a una gran flexibilidad a la topología de conexión. Mientras la estructura de tráfico podría tender entre configuraciones estrella, La disciplina impuesta por las líneas alquiladas las facilita y el actual flujo de tráfico que podrá ser mucho mejor incorporado a la topología.

2.5.4.5 Aplicaciones

Intercambio de información en tiempo real, dentro del ámbito empresarial. Correo electrónico. Transferencia de ficheros e imágenes. Impresión remota. Aplicaciones host-terminal. Aplicaciones cliente-servidor. Acceso remoto a bases de datos. Construcción de bases de datos distribuidas. Aplicaciones de CAD/CAM.

2.5.5. SONET

En los primeros días de la fibra óptica, cada compañía de teléfonos tenía su propio sistema óptico TDM patentado. Después de que AT&T se dividió en 1984, las compañías de teléfonos locales se tuvieron que conectar a múltiples portadoras de larga distancia, todas con diferentes sistemas ópticos TDM, de modo que se hizo obvia la necesidad de la estandarización. En 1985, *Bellcore*, empezó a trabajar en un estándar llamado SONET **(Red Óptica Sincrónica)**. Más tarde el CCITT se unió al esfuerzo, que en 1989 produjo en estándar SONET y un conjunto de recomendaciones paralelas del CCITT (G.707, G.708 y G.709). A las recomendaciones del CCITT se las llama **SDH (Jerarquía Digital Sincrónica)** pero difieren de SONET únicamente en detalles menores.

Virtualmente, todo el tráfico telefónico de larga distancia en Estados Unidos y una buena parte del mismo en los demás países, tiene ahora troncales que funcionan con SONET en la capa física. Al hacerse más baratos los circuitos SONET, las tarjetas de interfaz SONET para computadora pueden llegar a tener mayor difusión y se puede hacer más fácil para las compañías conectar sus computadoras en forma directa al corazón de la red telefónica por líneas rentadas especialmente acondicionadas.

El diseño de SONET tuvo cuatro objetivos principales:

- Primero, tenía que hacer posible la interconexión de redes de diferentes portadoras. El logro de este objetivo requirió que se definiera un estándar de señalización común con respecto a la longitud de onda, la temporización, las estructura de marcos y otras consideraciones.
- Segundo, se necesitaron medidas para unificar los sistemas digitales estadounidense, europeo y japonés, todos los cuales se basaban en canales PCM de 64 Kbps, pero combinados en formas diferentes (e incompatibles).
- Tercero, tenía que proporcionar un mecanismo para multiplexar varios canales digitales. En el momento que se creó SONET, la portadora digital de mayor velocidad que se usaba más ampliamente en Estados Unidos era la T3, a 44.736 Mbps. Parte de su misión era continuar la jerarquía a gigabits/seg y más allá. También se necesitaba una forma estándar de multiplexar canales más lentos en un solo canal SONET.
- Cuarto, tenía que proporcionar apoyo para las operaciones, la administración y el mantenimiento (OAM). Los sistemas anteriores no hacían esto muy bien.

Una decisión temprana fue convertir a SONET en un sistema TDM tradicional. Con todo el ancho de banda de la fibra dedicada a un canal que convirtiera segmentos de tiempo para los distintos subcanales.

Como tal, SONET es un sistema sincrónico, controlado por un reloj maestro con una precisión de alrededor de una parte en 10^9. En una línea SONET, los bits se envían a intervalos extremadamente precisos, controlados por el reloj maestro.

Cuando posteriormente se propuso que la conmutación de células fuera la base de la RDSI de banda ancha, el hecho de que permitiera la llegada de células a intervalos irregulares le confirió la etiqueta de modo de transferencia asíncrono (esto es ATM) para contrastarlo con el funcionamiento sincrónico de SONET.

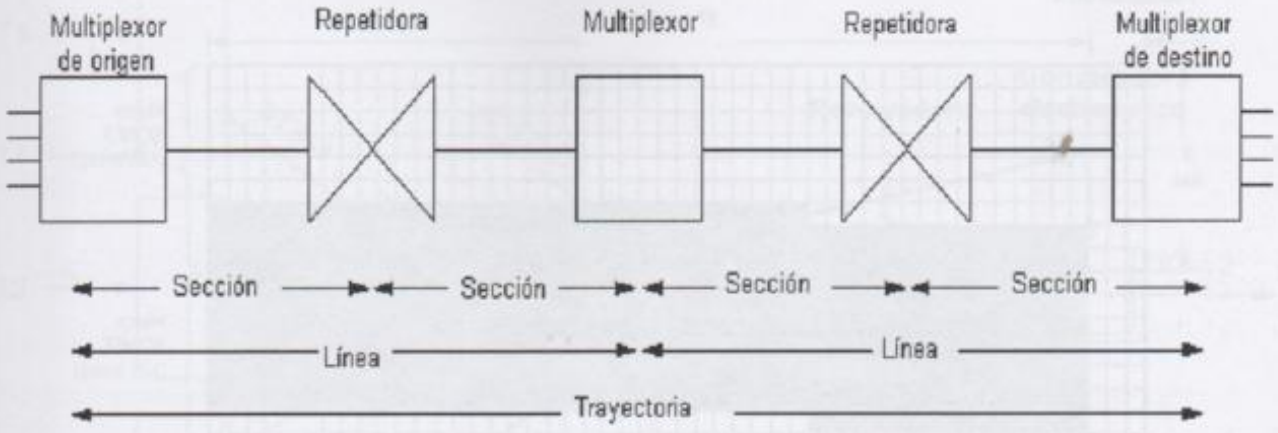


FIGURA 5.17: Una trayectoria SONET.

Un sistema SONET consiste en conmutadores, multiplexores y repetidoras, conectados todos por fibra. En la terminología de SONET, una fibra que va desde un dispositivo hasta cualquier otro en forma directa, con nada en medio, se llama **sección**. Una conexión entre dos multiplexores (posiblemente con una o más repetidoras en el medio) se llama **línea**. Finalmente, la conexión entre la fuente y el destino (posiblemente con uno o más multiplexores y repetidoras) se llama **trayectoria**. (Ver **figura 5.17**) La topología de SONET puede ser una malla, pero es frecuente que sea anillo dual.

El marco básico es un bloque de 819 bytes que se emite cada 125 µseg. Puesto que SONET es sincrónica, los marcos se emiten haya o no datos útiles para enviar. La velocidad de 8000 marcos/seg coincide perfectamente con la tasa de muestreo de los canales de PCM que se utilizan en todos los sistemas de telefonía digital.

Los marcos de 810 bytes de SONET se pueden describir mejor como un rectángulo de bytes, de 90 columnas de ancho por 9 filas de altura. De este modo, 8 x 810 = 6480 bits se transmiten 8000 veces por segundo, dando una tasa de datos aproximada de 51.84 Mbps. Éste es el canal básico de SONET y se llama **STS-1 (señal sincrónica de transporte 1)**. Todos los troncales de SONET son múltiplos de STS-1.

Las primeras tres columnas de cada marco se reservan para información de administración del sistema, como se ilustra en la **figura 5.18**. Las primeras tres filas contienen la información extra de la sección; las siguientes seis contienen la información extra de la línea. La primera se genera y verifica al comienzo y al final de cada sección, mientras que la segunda se genera y verifica al comienzo y al final de cada línea.

Las 87 columnas restantes contienen 87 x 9 x 8 x 8000 = 50.112 Mbps de datos de usuario. Sin embargo, los datos de usuario, llamados **SPE (Envoltura de carga útil sincrónica)**, no siempre empieza en la fila 1, columna 4. La SPE puede empezar en cualquier parte del marco. La primera fila de la información extra de línea contiene un apuntador al primer byte. La primera columna de la SPE es la información extra de la trayectoria (esto es, la cabecera para el protocolo de subcapa de la trayectoria de extremo a extremo).

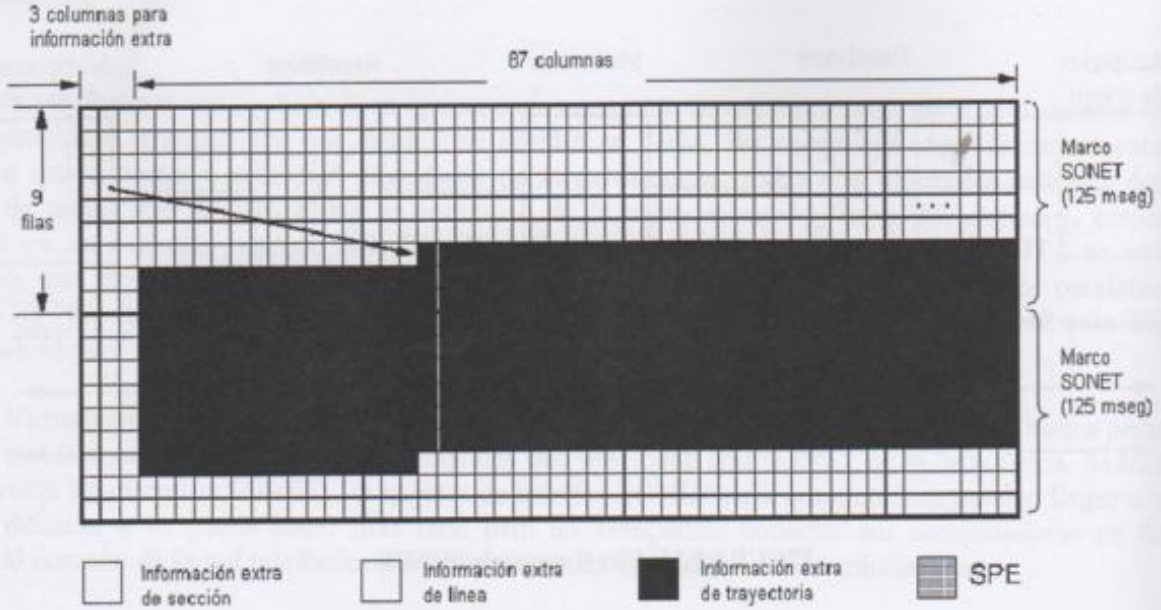


FIGURA 5.18: Dos marcos SONET consecutivos.

La facultad de que la SPE empiece en cualquier lugar dentro del Marco SONET o incluso abarque dos marcos, como se muestra en la **figura 5.18**, confiere una flexibilidad adicional al sistema. Por ejemplo, si una carga útil llega al origen mientras se está construyendo un marco SONET falso, se puede insertar en el marco actual, en lugar de retenerlo hasta el inicio del siguiente.

Esta facultad también es útil cuando la carga útil no se ajusta de manera exacta a un marco, como en el caso de una secuencia de células de ATM de 53 bytes. En tal caso, la primera fila de información extra de línea puede apuntar al inicio de la primera célula llena y establecer la sincronización.

La información extra de sección, de línea y de trayectoria contiene una profusión de bytes que se usan para operaciones, administración y mantenimiento. Puesto que cada byte ocurre 8000 veces por segundo, esto representa un canal de PCM. De hecho, tres de éstos se usan para proporcionar canales de voz al personal de mantenimiento de sección, línea y trayectoria. Se emplean otros bytes para encuadrado, paridad, vigilancia de errores, identificaciones, medición del tiempo, sincronización y otras funciones.

La multiplexación de varias corrientes de datos, llamadas **tributarias**, desempeña un papel importante en SONET. La multiplexación se ilustra en la **figura 5.19**. A la izquierda, comenzamos con varias corrientes de entrada de baja velocidad que se convierten a la velocidad básica STS-1 de SONET, por lo regular añadiendo un relleno para redondear a 51.84 Mbps. A continuación, tres tributarias STS-1 se multiplexan en una corriente de salida STS-3 de 155.52 Mbps. A su vez, esta corriente se multiplexa con otras tres en una corriente final de salida que tiene 12 veces la capacidad de la corriente STS-1. En este punto la señal se resuelve para evitar que las series largas de ceros o unos interfieran en la medición del tiempo, y se convierte de señal eléctrica en óptica.

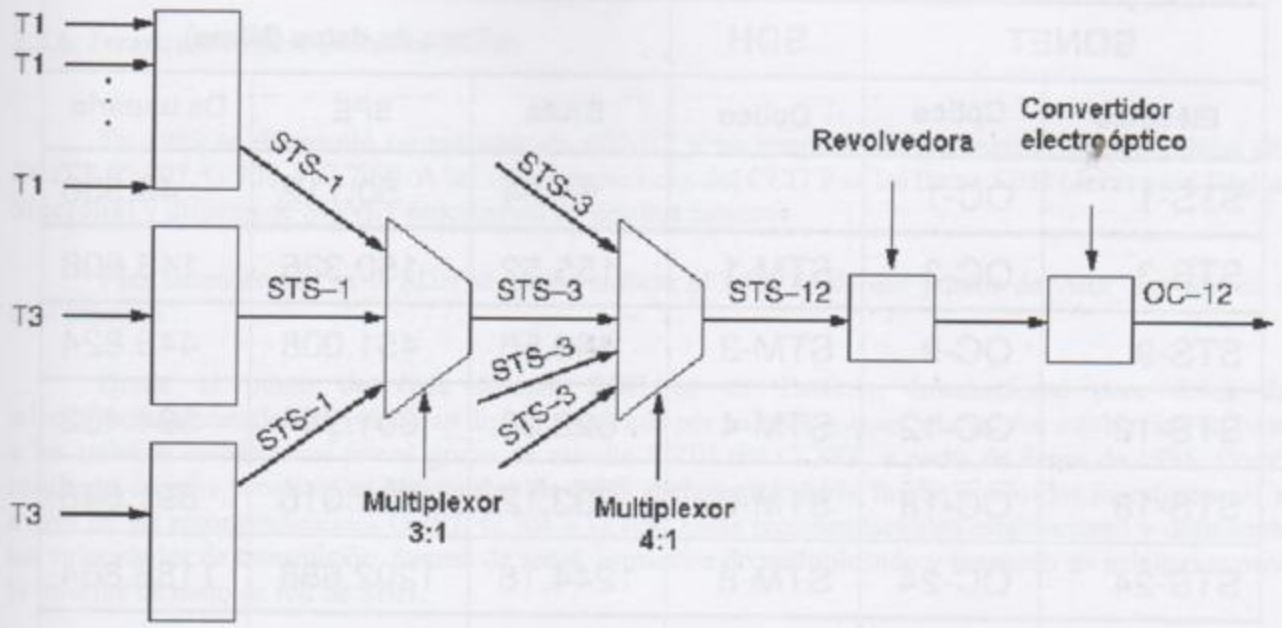


FIGURA 5.19: Multiplexión en SONET.

La multiplexión se hace byte por byte, por ejemplo, cuando tres tributarias STS-1 a 51.84 Mbps, el multiplexor emite primero un byte de la tributaria 1, después uno de la tributaria2, y finalmente, uno de la tributaria 3, antes de regresar a la 1.

La figura de STS-3 análoga a la **figura 5.18** muestra (de izquierda a derecha) las columnas de las tributarias1, 2 y 3 , en ese orden, después otra tripleta, y así sucesivamente, hasta la columna 270. Uno de estos marcos de 270 x 9 bytes se envía cada 125 µseg, lo que da una tasa de transmisión de datos de 155.52 Mbits por segundo.

2.5.5.1. Jerarquía de multiplexión y definición del OC-N

En la **figura 5.20** se muestra la jerarquía de multiplexión de SONET. Se definieron tasas de STS-1 a STS-48. La portadora óptica que corresponde a cada STS-n se llama **OC-n**, pero bit a bit es la misma, excepto por la revoltura que aparece en la **figura 5.19**.

Los nombres de SDH son diferentes de los de SONET y empiezan en 155Mb/s, o sea en OC-3 porque los sistemas basados en CCITT tienen una tasa de transmisión cercana a los 155 Mbps.

La portadora OC-9 está presente porque se aproxima mucho a la velocidad de uno de los principales troncales de alta velocidad que se usan en Japón. Las OC-18 y OC-36 se usarán en Japón en el futuro. La tasa bruta de transmisión de datos incluye toda la información extra. La tasa de transmisión de SPE excluye la información extra de línea y de sección, la tasa de transmisión de datos de usuario excluye toda la información extra y cuenta solamente las 86 columnas disponibles para la carga útil.

SONET		SDH	Tasa de datos (Mbps)		
Eléctrico	Optico	Optico	Bruta	SPE	De usuario
STS-1	OC-1		51.84	50.112	49.536
STS-3	OC-3	STM-1	155.52	150.336	148.608
STS-9	OC-9	STM-3	466.56	451.008	445.824
STS-12	OC-12	STM-4	622.08	601.344	594.432
STS-18	OC-18	STM-6	933.12	902.016	891.648
STS-24	OC-24	STM-8	1244.16	1202.688	1188.864
STS-36	OC-36	STM-12	1866.24	1804.032	1783.296
STS-48	OC-48	STM-16	2488.32	2405.376	2377.728

FIGURA 5.20: Tasa de multiplexión de SONET y SDH.

Por cierto, cuando una portadora, como la OC-3, no se multiplexa, sino que conduce datos de una fuente única, la letra C (de concatenado), se agrega a la designación, de modo que OC-3 indica una portadora de 155.52 Mbps que consiste en tres portadoras OC-1 independientes, pero OC-3c indica una corriente de datos de una sola fuente a 155.52 Mbps.

Las tres corrientes OC-1 dentro de una corriente OC-3c se entrelazan por columnas, primero la columna 1 de la corriente 1, a continuación la columna 1 de la corriente 2, después la columna 1 de la corriente 3 seguida de la columna 2 de la corriente 1, y así sucesivamente, lo que conduce a un marco de 270 columnas de ancho y 9 filas de profundidad.

La cantidad de datos de usuarios reales en una corriente OC-3c es un poco más alta que en una OC-3 (149.760Mbps contra 148.608 Mbps) porque la columna de información extra de trayectoria se incluye dentro de la SPE sólo una vez, en lugar de tres, en el caso de tres corrientes independientes OC-1.

En otras palabras, en OC-3c están disponibles para datos de usuario 260 de las 270 columnas, mientras que en OC-3 solamente están disponibles 258 columnas para datos de usuario. También existen marcos concatenados de orden más alto (por ejemplo, OC-12c).

Ahora debe quedar claro porque ATM funciona a 155 Mbps; la intención es transportar células de ATM por troncales OC-3c de SONET. También debe quedar claro que la cifra tan citada de 155 Mbps es la velocidad de transmisión bruta que incluye la información extra de SONET. Además, en algún momento alguien redondeó de manera incorrecta los 155.52 Mbps a 155 Mbps en lugar de 156 Mbps y ahora todos los demás lo hacen mal también.

2.5.6. Jerarquía Digital Síncrona (SDH)

En 1989 se desarrolló un estándar de SONET y un conjunto de recomendaciones paralelas del CCITT (G.707, G.708, y G.709). A las recomendaciones del CCITT se las llama **SDH (Jerarquía Digital Síncrona)** y difieren de SONET únicamente en detalles menores.

Para entender qué es la SDH se puede enfocar el tema desde dos puntos de vista: uno formal y otro práctico.

Desde el punto de vista formal, SDH es un Estándar Internacional para redes de telecomunicaciones de alta velocidad digital soportada por enlaces ópticos, el cual fue establecido en base a los trabajos comenzados por el grupo de estudio XVIII del CCITT, a partir de Junio de 1986. Como resultado de esos estudios, en Noviembre de 1988, dichos estándares fueron conocidos mundialmente a través de las recomendaciones G.707, G.708 y G.709. Estas recomendaciones establecieron y definieron las velocidades de transmisión, formas de señal, estructura de multiplexado y mapeado de tributarios para la interfaz de nodo de red de SDH.

El CCITT estableció luego, nuevas recomendaciones referidas a los tipos, características y bloques funcionales de los *múltiplex SDH*, como así también lo referido a la gestión de red (TMN), interfaces ópticas y sistemas de línea digital para SDH, en las recomendaciones G.781, G.782, G.783, G.784, G.957 y G.958 respectivamente.

El punto de vista práctico fue el de crear un nuevo sistema de transporte síncrono que diera a los operadores de comunicaciones, una infraestructura de red a nivel mundial más simple, económica y flexible.

Dichas redes plesiócronas (PDH) fueron desarrolladas en un momento en que el requerimiento fundamental de la red, era la conexión punto a punto, lo cual limita la capacidad del operador de dicha red a responder rápidamente a la demanda de circuitos para un punto intermedio de dicho enlace. Entendiendo la flexibilidad como la capacidad de acceder fácilmente a una señal de tributario individual y poder ser ésta re-enrutada por otro sistema de transporte, el actual sistema plesiócrono (que debe demultiplexar por ejemplo una trama de 140 Mbps para extraer los tributarios de 2 Mbps) es claramente no flexible. Más aun, para re-enrutar ese tributario extraído, se deben hacer los pasos de multiplexado (2 a 8; 8 a 34; 34 a 140 Mbps), para colocar ese tributario en una trama de transporte más rápida.

Teniendo en cuenta que existen tres jerarquías plesiócronas (Estados Unidos, Japón y Europa), los problemas de enlace y re-encaminamiento plesiócrono son evidentemente complicados, no sólo en el ámbito de un país, sino peor aun cuando diferentes países adoptan diferentes estándares plesiócronos.

Otro tema a tener en cuenta son los conceptos de gestión y mantenimiento de la red actual, los cuales se basan en la *cross-conecction* manual de señales y mediciones fuera de servicio respectivamente, por lo que no se necesitó que las estructuras de trama tuvieran una capacidad extra de bits para esos fines específicos. Se verá que la trama SDH tiene en su estructura dicha "sobre capacidad".

Para finalizar con las limitaciones de las redes actuales, no existe un estándar común para los sistemas de alta velocidad, por lo tanto, cada uno de los fabricantes tiene su propio diseño, de manera que el comprador queda obligado a comprar ambos extremos del enlace al mismo proveedor sin posibilidad de compatibilizar con los productos de otro proveedor.

2.5.6.1. Ventajas de SDH

Como contrapartida de lo ya comentado, la SDH se basa en el principio del multiplexado síncrono, lo cual es la clave para flexibilizar la red a un costo mucho más efectivo, esto significa que una señal de tributario puede ser multiplexada y demultiplexada directamente en una señal SDH de mayor velocidad sin etapas intermedias de multiplexado y demultiplexado. Los elementos de red SDH pueden luego ser interconectados directamente con los ahorros de costo y equipamiento respecto de la red actual.

Para que dicha flexibilidad sea efectiva es necesario que la estructura de la trama SDH provea la capacidad de contener con bits destinados a funciones de gestión de red y funciones de mantenimiento. De hecho, un 5% de la capacidad de la trama está destinada a estos fines en los denominados encabezados.

A través de diferentes esquemas de mapeado, la señal SDH puede transportar a todas las diferentes señales tributarias de las diferentes jerarquías plesiócronas, de manera de establecer un esquema de red universal, tanto en el área urbana, interurbana, o internacional, esto significa que al estar el estándar SDH en toda la red, permite la provisión de equipos de diferentes fabricantes para todo el sistema.

La trama SDH además es capaz de acomodar los más avanzados servicios que en un futuro estarán a la orden del día: ATM, redes LAN FDDI, redes metropolitanas DQDB, etc.

2.5.6.2. Segmentos de la red

Se puede distinguir en el esquema siguiente, tres segmentos de la red (ver **figura 5.22**):

- El trayecto (PATH).
- La sección del multiplexor.
- La sección del regenerador.

Cada segmento de red SDH tendrá su propio *overhead* de manera que éste provea las señales de soporte y mantenimiento asociadas con la transmisión a través de dicho segmento de red, por lo tanto aparecen tres tipos diferentes de *overheads* **(taras)**:

- PATH overheads **(POH)** o tara de trayecto **(TTY)**.
- Multiplex Section Overhead **(MSOH)**.
- Regenerador Section Overhead **(ROSH)**.

El trayecto (PATH) de una red SDH es la conexión lógica entre los puntos donde se ensamblan las señales de tributario dentro de su VC **(contenedor virtual)**, y el punto donde se desarma dicho VC para obtener la señal de tributario.

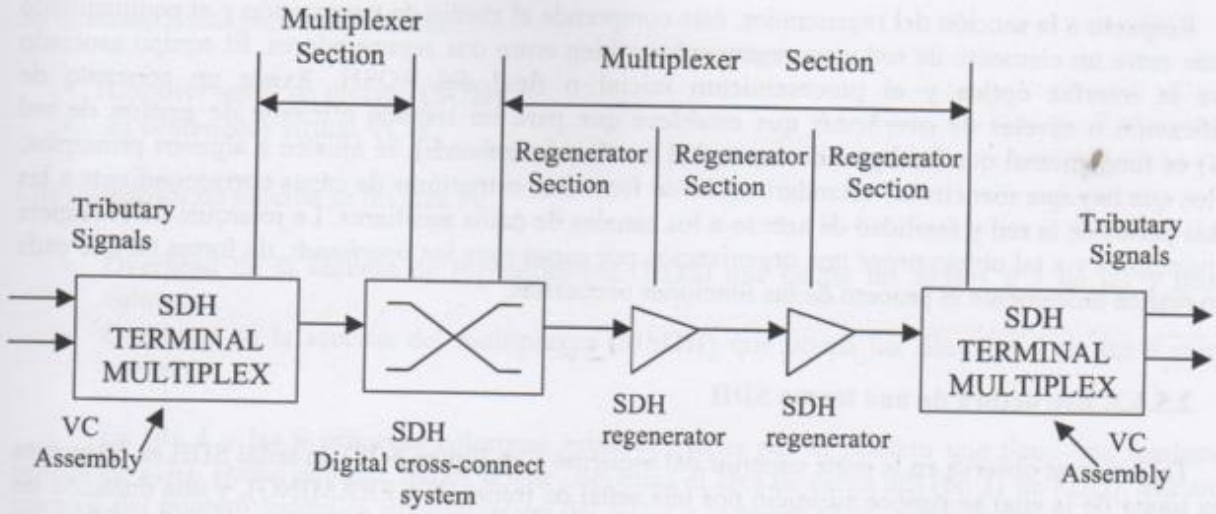


FIGURA 5.22: Segmentos de la red.

La sección del Multiplexor de una red SDH comprende el medio de transmisión, junto con el equipo asociado (incluyendo los generadores), que proveen los medios de transporte de información entre dos nodos consecutivos de la red (por ejemplo: Multiplex SDH, Cross-connect SDH). Uno de los nodos de red crea el MSOH mientras el otro nodo lo recibe y allí termina dicho MSOH.

En las redes SDH, la sección del Multiplexor tiene una fundamental importancia, ya que es a este nivel que la red provee la protección contra fallas o degradaciones de la performance del equipo, que en caso de producirse, dicha red conmutará el o los VC asociados a otro circuito de transmisión (*back-up*) de protección que incluye el medio de Tx, los regeneradores (si hacen falta) y el equipo de fin de la sección del multiplex.

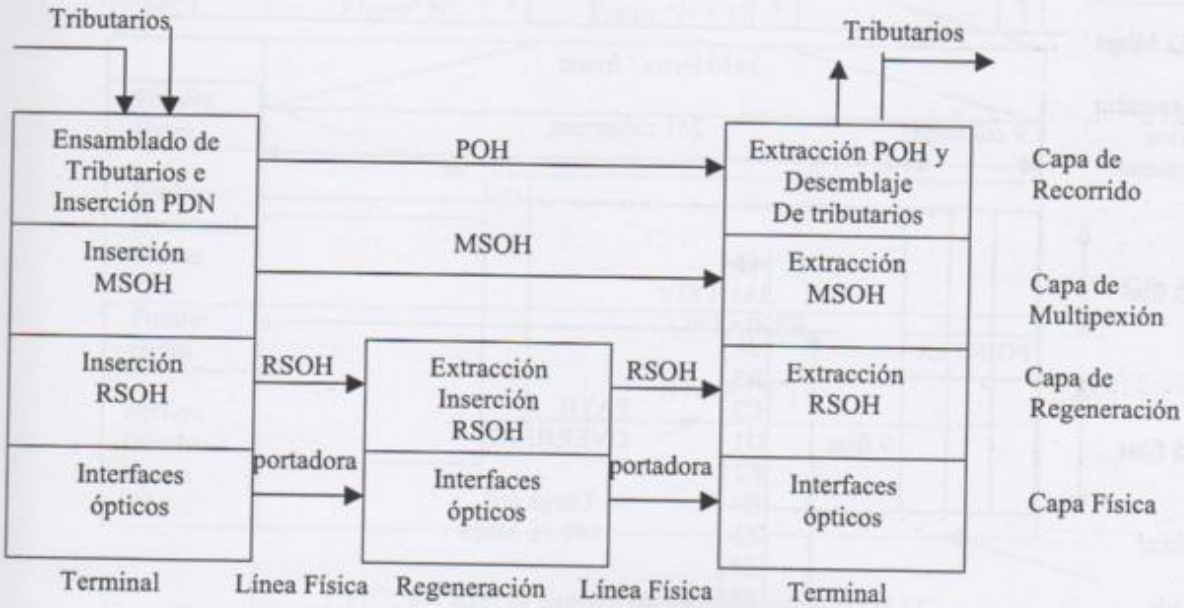


FIGURA 5.23: Estratificación de los encabezamientos (overheads).

Respecto a la sección del regenerador, ésta comprende el medio de transmisión y al equipamiento asociado entre un elemento de red y un regenerador o bien entre dos regeneradores. El equipo asociado incluye la interfaz óptica y el procesamiento inicial o final del ROSH. Existe un concepto de estratificación o niveles de *overheads* que establece que para un sistema eficiente de gestión de red (TMN) es fundamental que los bytes de capacidad auxiliar (*overheads*), se ajusten a algunos principios, entre los que hay que mencionar: estandarización de formatos, estructuras de capas correspondiente a las distintas partes de la red y facilidad de acceso a los canales de datos auxiliares. La jerarquía SDH respeta estos principios y a tal objeto prevé una organización por capas para los *overheads*, de forma tal que cada equipo realice únicamente el proceso de las funciones necesarias.

2.5.6.3. Estructura de una trama SDH

Tal como se observa en la parte superior del esquema (ver **figura 5.24**), la señal SDH se estructura en una trama de la cual se conoce su inicio por una señal de trama (F = FRAMING), y una duración de 125µs, momento en que se inicia la trama siguiente. Dentro de la trama, los bits se agrupan de a 8 bits, es decir, bytes. Dichos bytes, se conocen y se ubican con su posición respecto a los bits de alineación (F = FRAMING) similar a la trama PDH. Sin embargo, para mayor claridad, la secuencia en serie de bits (uno detrás del otro) se representa por una matriz de 2 dimensiones, como se describe en la parte inferior de la misma. La señal básica de SDH es el denominado Módulo de Transporte Síncrono de primer nivel **(STM-1)**, el cual se puede representar como una matriz de 9 filas por 270 columnas, es decir, una capacidad de 2430 bytes (9 x 270) o lo que es lo mismo 19,440 bits por trama (9 x 270 x 8). Como la trama se repite cada 125 µs, la señal STM-1 tiene una velocidad de 155,52 Mbps (9 x 270 x 8 x 8000). Los bits de la trama se envían en serie comenzando por el bit más significativo del byte ubicado en la fila 1 columna 1; se envía toda la fila 1, luego la fila 2, etc., hasta enviar el último bit del byte ubicado en la fila 9 columna 270, luego del cual comienza la secuencia de la trama siguiente.

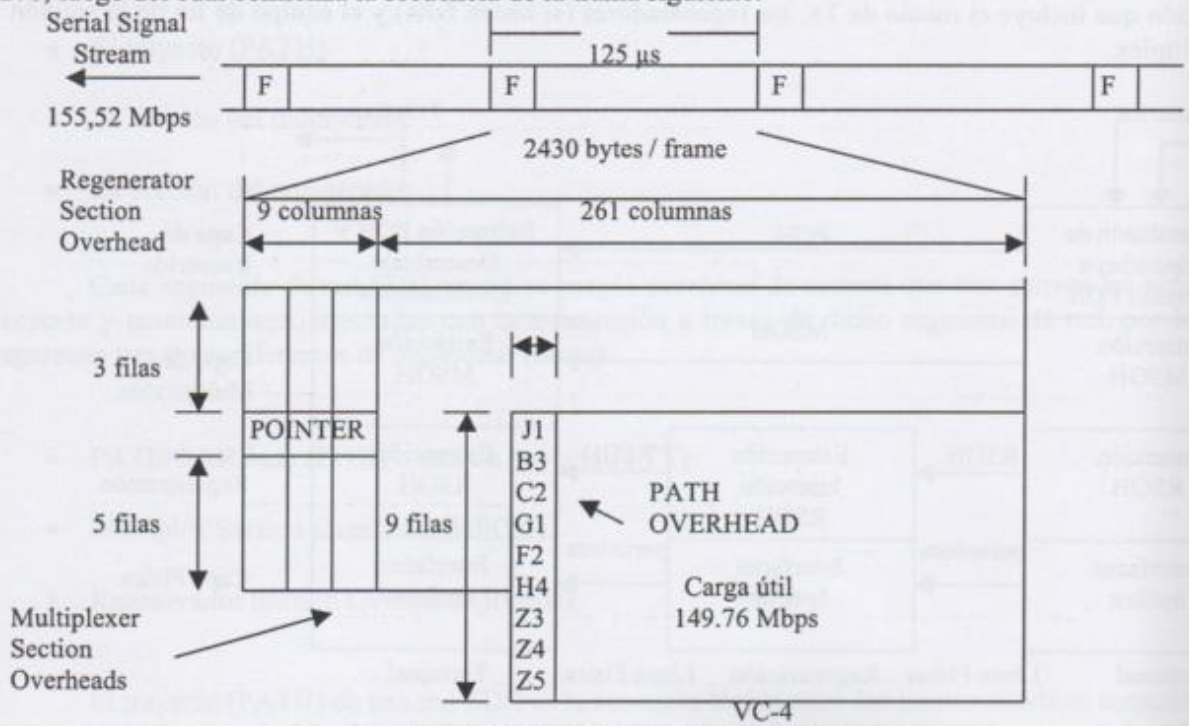


FIGURA 5.24: Estructura de trama SDH.

Se destacan zonas bien diferenciadas:

- Los *overheads* de sección **(SOH)**.
- El contenedor virtual VC-4.

Los *overheads* de sección se dividen en:

- Overhead de la sección de regeneradores **(ROS)** que ocupa las filas 1 a 3 de las 9 primeras columnas.
- Overhead de la sección del multiplexor **(MSOH)** que ocupa las filas 5 a 9 de las 9 primeras columnas.

La fila 4 y las 9 primeras columnas están ocupadas por el puntero que tiene una fundamental misión en SDH. Dicho puntero, indica donde comienza el área de carga útil (bit J1 de POH), adelantos y retrasos del puntero logran la sincronización del VC-4 a la trama SDH, posibilitando que el VC-4 flote libremente dentro del espacio disponible dentro del STM-1 de manera de realizar ajustes de fase entre éstos. Esto significa que el VC-4 puede comenzar en cualquier lugar de la capacidad de carga del STM-1, por lo tanto es improbable que dicho VC-4 entre totalmente en una trama. Lo más probable es que el VC-4 comience en una trama y finalice en la siguiente.(Ver **Figura 5.25**).

Observando el esquema de estructura de trama de SDH, desde la columna 10 hasta la columna 270, se encuentra el VC-4, formado por 9 bytes de POH y 2340 bytes (260 x 9) de carga útil. Esto provee una capacidad de carga de 149,76 Mbps (260 x 9 x 8 x 8000), es decir, puede acomodar un tributario de 140 Mbps. Los contenedores virtuales VC-1, VC-2, VC-3, se logran por subdivisiones del VC-4.

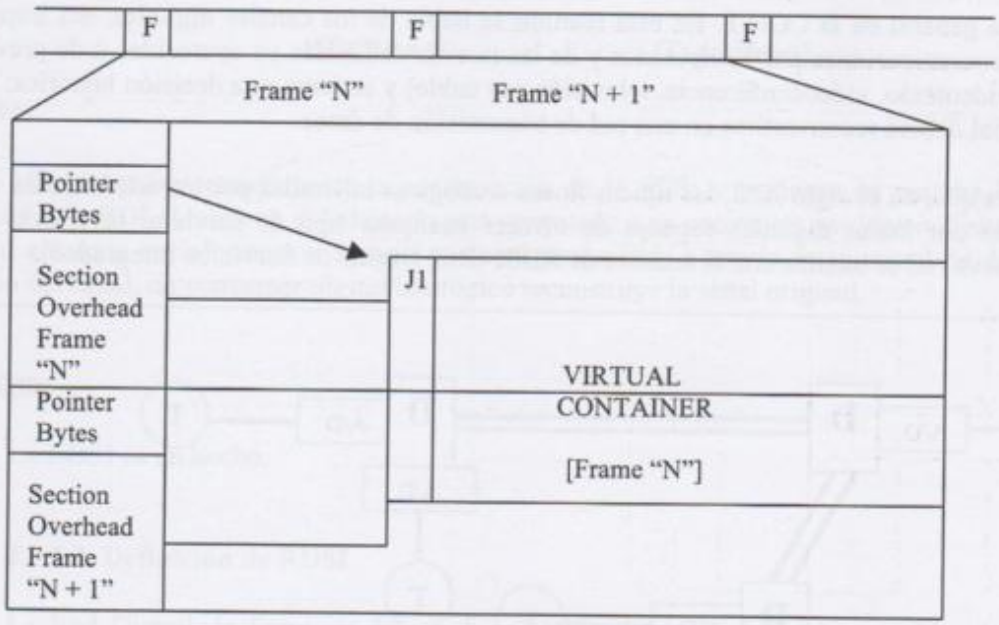


FIGURA 5.25: El puntero indica donde comienza el VC.

2.5.7. Red Digital de Servicios Integrados (RDSI)[33]

2.5.7.1. Introducción

Continuando con la reseña histórica de la evolución tecnológica que sufrió la red telefónica podemos situarnos en el año de creación de la RDSI.

Año 1984:

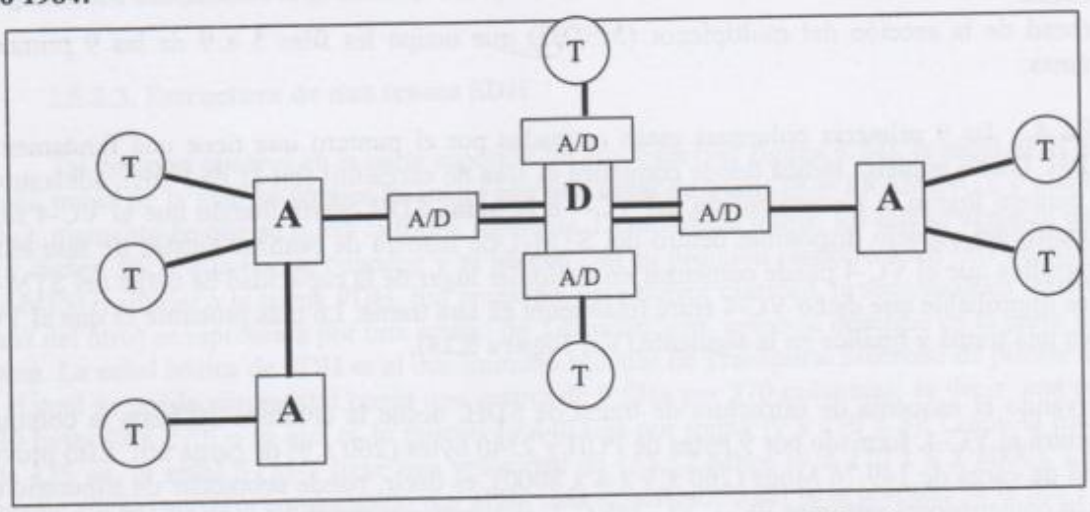


FIGURA 5.29 **(T: teléfono)**

Asamblea general de la CCITT. En esta reunión se habla de los canales digitales, del imparable aumento de las comunicaciones por computador y de las nuevas demandas ya aparecidas o de previsible aparición (fax, videotexto, videoconferencia, televisión por cable) y se toma una decisión histórica: la red telefónica mundial deberá reconvertirse en una red de transmisión de datos.

El plan es que, en el siglo XXI, las típicas líneas analógicas utilizadas por los teléfonos de voz se habrán sustituido por líneas digitales capaces de ofrecer cualquier tipo de servicio, inventado o por inventar; esta nueva red se bautiza con el nombre de RDSI (Red Digital de Servicios Integrados).

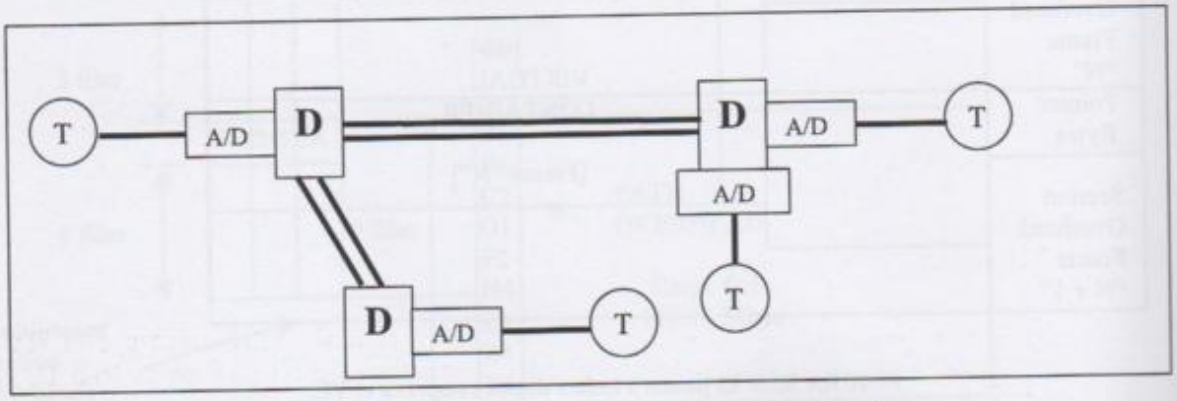


FIGURA 5.30 **(T: teléfono)**

[33] En Inglés: ISDN (Integrated Services Digital Network)

La idea era muy buena, pero presentaba un problema enorme, la construcción de esta red. Si se quería que el proyecto fuera viable, la nueva RDSI debía crearse a partir de la vieja red de voz. El esquema finalmente elegido fue el de un desarrollo en dos fases; en una primera fase se sustituirían las viejas centrales de *relees* por nuevas centrales computarizadas, que aunque serían compatibles con los sistemas antiguos podrían ofrecer los servicios requeridos por la nueva red; paralelamente, todos los canales de comunicación (no sólo de larga distancia) se irían reconvirtiendo en canales digitales. Esto permitiría la existencia de un período de transición durante el cual estarían entremezclados enlaces analógicos y digitales (Ver **figura 5.29**) y que concluiría en la RDI (Red Digital Integrada), una red en la que el único enlace analógico sería el que une el teléfono del abonado con la central (Ver **figura 5.30**). Llegados a este punto, se entraría en la segunda fase, que consistiría en alargar los enlaces digitales hasta los abonados (Ver **figura 5.31**); la RDSI habría nacido.

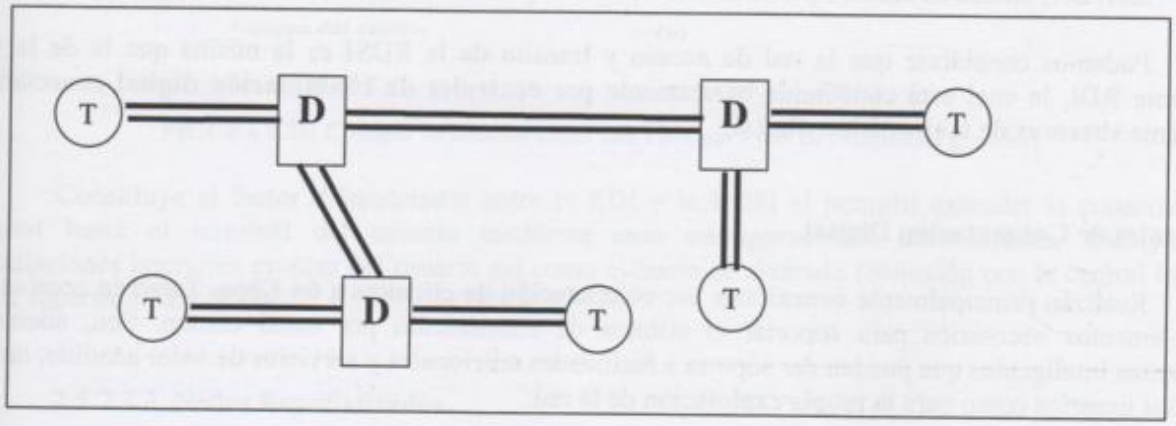


FIGURA 5.31 **(T: teléfono)**

Años 90:

Muchos países completaron la construcción de la RDI; y pusieron en marcha la RDSI. En el contexto de la RDI el teléfono del abonado está conectado a un conversor *analógico/digital* que convierte la señal eléctrica en información binaria que será transmitida a través de un canal de datos; en el otro extremo del canal, un conversor *digital/analógico* reconstruye la señal original.

Año 2000:

La RDSI es un hecho.

2.5.7.2. Definición de RDSI

La Red Digital de Servicios Integrados (RDSI), según la definición establecida por la ITU-T (Unión Internacional de Comunicaciones) es una red que procede por evolución de la Red Digital Integrada y que facilita conexiones digitales extremo a extremo para proporcionar una amplia gama de servicios, tanto de voz como de otros tipos, y a la que los usuarios acceden a través de un conjunto definido de interfaces normalizados.

Más comúnmente puede describirse como una red que procede por evolución de la red telefónica existente que al ofrecer conexiones digitales extremo a extremo permite la integración de una multitud de servicios en un único acceso, independientemente de la naturaleza de la información a transmitir, y del equipo terminal que la genere.

Esta red coexiste con las redes convencionales de telefonía y datos e incorpora elementos de interfuncionaminto para su interconexión con dichas redes, tendiendo a convertirse en una Red de Telecomunicaciones universal.

2.5.7.3. Estructura general de la RDSI

2.5.7.3.1. Redes de Acceso y Tránsito

Podemos considerar que la red de acceso y tránsito de la RDSI es la misma que la de la ya existente RDI, la cual está constituida básicamente por **centrales de conmutación digital** conectadas mediante **sistemas de transmisión digital**.

Centrales de Conmutación Digital

Realizan principalmente conexiones por conmutación de circuitos a 64 Kbps. También contienen los elementos necesarios para soportar el sistema de señalización por canal común. Son, además, elementos inteligentes que pueden dar soporte a facilidades adicionales y servicios de valor añadido, tanto para los usuarios como para la propia explotación de la red.

2.5.7.3.2. Acceso de Usuario

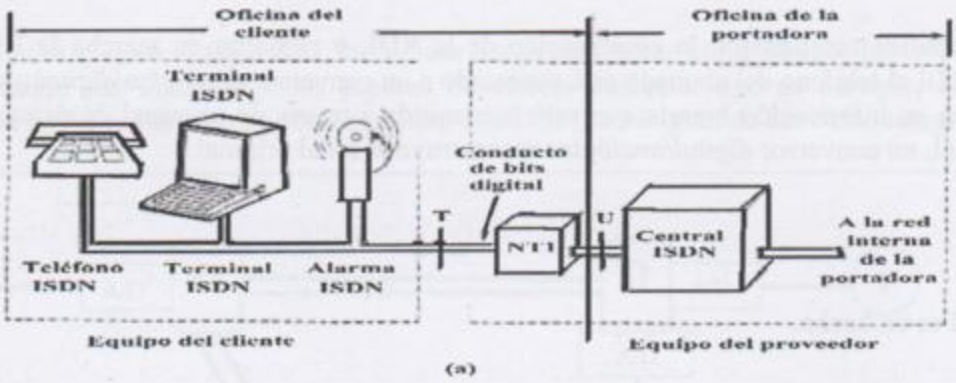


FIGURA 5.32: Ejemplo de sistema ISDN para uso del hogar.

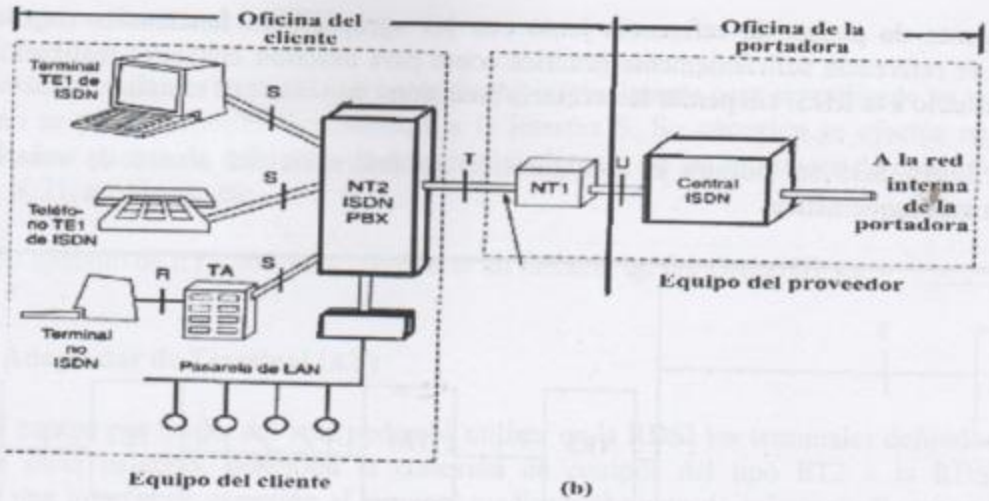


FIGURA 5.33: Ejemplo de sistema ISDN con PBX para uso en compañías grandes.

Constituye el factor diferenciador entre la RDI y la RDSI al permitir extender la conectividad digital hasta el terminal del usuario mediante unas configuraciones normalizadas. Incluye las instalaciones interiores propias del usuario así como el bucle de abonado (conexión con la central local). (Ver **figuras 5.32** y **5.33**)

2.5.7.3.3. Nodos Especializados

Pueden ser de diversos tipos, como por ejemplo, servicios de valor añadido, centros de explotación de red, etc.

2.5.7.4. Estructura genérica del acceso de usuario a la RDSI

Como ya se mencionó anteriormente, en el acceso de usuario pueden distinguirse dos partes principales:

- **Instalación interior de usuario**, formada por los equipos terminales de usuario y por una red interior que conecta dichos terminales a la línea de transmisión digital. Ciertas instalaciones de usuario pueden contener, además, equipos de conmutación local como, por ejemplo, centralitas digitales.

- **Red local**, formada por los sistemas de transmisión digital entre la instalación de usuario y la central local y, en ocasiones, por otros elementos auxiliares de conexión como, por ejemplo, multiplexores.

En el acceso de usuario se definen Puntos de Referencia y Agrupaciones Funcionales. Las agrupaciones funcionales representan o definen entidades que realizan funciones de manera agrupada. Se pueden corresponder con un equipo físico en su totalidad, o con parte de él. Los puntos de referencia identifican las interfaces entre agrupaciones funcionales distintas y se pueden corresponder con interfaces reales o con interfaces virtuales (internas en un equipo).

El conjunto de puntos de referencia junto con las agrupaciones funcionales constituyen una configuración de referencia suficientemente genérica como para describir cualquier realización práctica de acceso de usuario a la RDSI sin perder la necesaria precisión.

En la **figura 5.35** se muestra la configuración de referencia del acceso de usuario en una representación más esquemática.

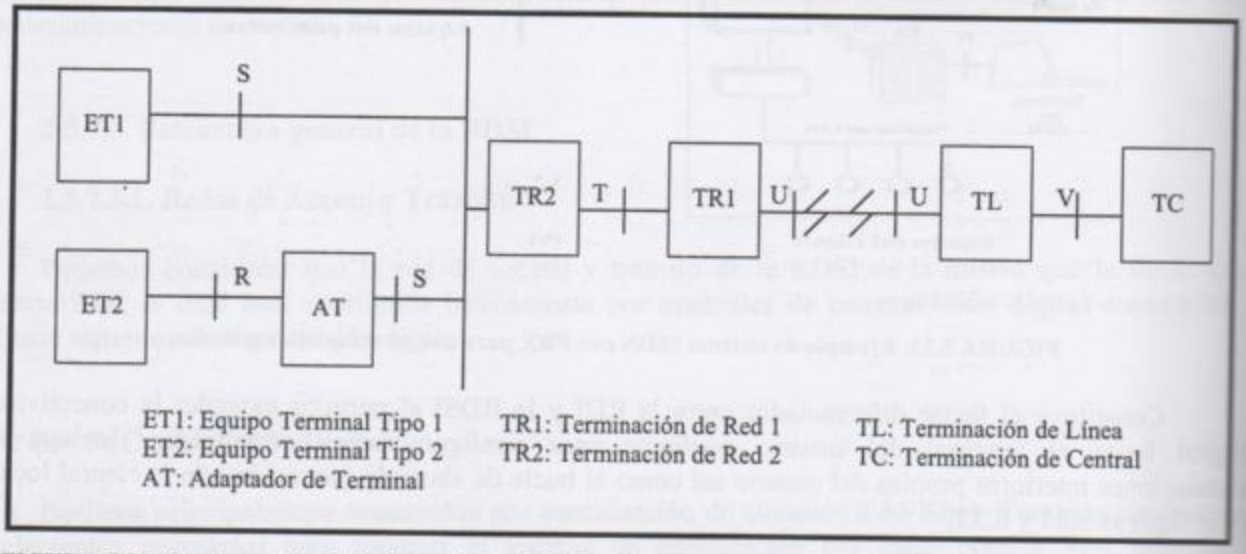


FIGURA 5.35: Configuración de Referencia. La RDSI está configurada por un conjunto de equipos y elementos, denominados "agrupaciones funcionales", separados entre ellos por los llamados "puntos de referencia".

2.5.7.4.1. Agrupaciones Funcionales

Si procedemos a describir las entidades funcionales tal y como se las puede encontrar partiendo desde el terminal de usuario, avanzando por la red interior del mismo para alcanzar finalmente la central de conmutación telefónica, nos encontraremos las agrupaciones funcionales que se describirán a continuación.

Considerando que iniciamos la descripción en el terminal de usuario, encontraremos terminales específicamente desarrollados para la RDSI o terminales procedentes y preparados para cualquier otro tipo de red. En función de su origen, podremos establecer dos tipos de terminales distintos: equipo terminal de tipo 1 o más comúnmente ET1 y equipo terminal de tipo 2 o ET2.

2.5.7.4.1.1. Equipo Terminal 1 (ET1)

Es el equipo terminal que está diseñado específicamente para conectarse directamente a la RDSI sin necesidad de ningún equipo adicional. Se conecta a la RDSI en el punto de referencia S. La realización práctica de este punto de referencia puede ser una roseta conectada en un bus, o un conector integrado en un elemento que, por el momento, denominaremos genéricamente terminación de red.

Un ejemplo de ET1 es un fax de Grupo IV, un teléfono RDSI, la tarjeta SPC2, etc.

2.5.7.4.1.2. Equipo Terminal 2 (ET2)

Representa cualquier terminal que no se diseñó originalmente para ser utilizado en la RDSI y que, por tanto, no se puede conectar directamente a la interfaz S. Su conexión se efectúa en el punto de referencia R. Los puntos de referencia R designan cualquiera de las interfaces de conexión conocidos, V.28, V.35, X.21, analógico, etc.

Como ejemplo de ET2 podemos considerar un módem, un fax Grupo III, etc.

2.5.7.3.1.3. Adaptador de Terminal (AT)

Es el equipo por medio del cual podemos utilizar en la RDSI los terminales definidos en el punto anterior. En otras palabras, posibilita la conexión de equipos del tipo ET2 a la RDSI. Para ello proporciona una interfaz de conexión al terminal mediante el punto de referencia R, y se conectará a la RDSI en un punto de referencia S.

Ejemplos de adaptador serían adaptadores de interfaz analógico (AT-a/b), adaptadores de interfaz V.35, etc.

Supongamos ahora, lo que constituiría el caso más general de instalación interior de abonado, que los terminales descriptos con anterioridad están conectados a algún tipo de elemento de red privada de abonado tal y como podría ser una centralita, un concentrador, etc. Este tipo de agrupación se define como:

2.5.7.3.1.4. Terminación de Red 2 (TR2)

Es una agrupación funcional que realiza funciones de conmutación, concentración y control en el interior de las instalaciones del cliente.

Una TR2 se conectará a la RDSI en el punto de referencia T y proporciona al usuario el punto S necesario para conectar agrupaciones del tipo ET1 o AT.

Un ejemplo de TR2 puede ser una centralita, una red de área local o un sistema multilínea.

No es imprescindible la existencia de TR2 en las instalaciones interiores de usuario, en cuyo caso los puntos de referencia T y S son coincidentes. A veces encontraremos esta coincidencia descripta explícitamente en la expresión *punto de referencia S/T* aunque, por lo general, también en estas instalaciones se habla del punto de referencia S de manera abreviada. En todo caso, podrá existir o no una TR2, pero siempre se necesitará el elemento "frontera" entre la instalación interior y la red local. Este elemento, presente siempre, es la TR1.

2.5.7.3.1.5. Terminación de Red 1 (TR1)

Es el elemento que permite la interconexión entre la instalación interior del usuario a 4 hilos y la red exterior, a 2 hilos.

La instalación interior del usuario se conecta a la TR1, en el caso más general, en el punto de referencia T. Sin embargo, el caso más habitual es aquel en que no existe TR2 y por tanto el punto de

referencia asociado es el S/T. El código de línea de la instalación interior de usuario es único y, por lo tanto, independiente del sistema que provea el acceso a la RDSI.

La TR1 se conecta a la red exterior en el denominado punto de referencia U. Este punto de referencia no define una única interfaz ya que existen dos tipos de interfaz caracterizados por dos códigos de línea distintos:

- 4B3T asociado a centrales 1240 de ALCATEL.
- 2B1Q propio de los sistemas SESS de LUCENT y AXE de ERICSSON.

La TR1, además de permitir la interconexión, proporciona facilidades de mantenimiento y supervisión de los aspectos relacionados con la transmisión.

2.5.7.4.1.6. Terminación de Línea (TL)

En la central local que proporciona el acceso se encuentra la TL, la cual, en cuanto a sus funciones, puede considerarse como el equivalente de la TR1.

2.5.7.4.1.7. Terminación de Central (TC)

La TC, que está ubicada en la central local, realiza la conexión de los canales de información con las etapas de conmutación de la central, soporta el procesamiento de la señalización del usuario, controla la *activación/desactivación* de la línea digital y realiza el mantenimiento correspondiente del acceso de usuario. En ciertos casos, los equipos de TC y de TL están integrados en el mismo equipo físico por lo que el punto de referencia que separa a ambos, el V, se convierte en un punto de referencia virtual.

2.5.7.4.2. Puntos de Referencia

A continuación se definen los puntos de referencia que han ido apareciendo en la descripción de las distintas agrupaciones funcionales.

2.5.7.3.2.1. Punto de Referencia R

Representa el punto de conexión de cualquier terminal que soporte un interfaz normalizado (no RDSI) como pueden ser terminales modo paquete X.25, terminales con interfaz V.24 o terminales con interfaz analógica a 2 hilos.

2.5.7.4.2.2. Punto de Referencia S

Se corresponde con la conexión física de los terminales de abonado a la RDSI. Es un interfaz a 4 hilos, 2 para transmisión y 2 para recepción.

2.5.7.3.2.3. Punto de Referencia T

Representa la separación entre las instalaciones de usuario y equipos de transmisión de línea. Posee las mismas características eléctricas que el interfaz S.

2.5.7.4.2.4. Punto de Referencia U

Representa la línea de transmisión entre las dependencias del cliente y la central telefónica y se corresponde físicamente con el bucle de abonado a 2 hilos actualmente existente.

2.5.7.4.2.5. Punto de Referencia V

Representa la separación entre los elementos de transmisión y los de conmutación dentro de la central local de RDSI.

2.5.7.4.3. Topologías del Acceso Básico

La red interior de usuario, en general, no es sino un cable de dos pares que discurre desde la TR1 según distintas topologías hasta un punto extremo en el que se conectará, siempre, unas resistencias de terminación. A lo largo de este cable se encuentran una serie de rosetas de número variable.

Atendiendo a la configuración del cableado, podemos distinguir entre tres tipos de configuración del acceso básico:

2.5.7.4.3.1. Bus pasivo corto

En esta configuración, se dispone de un cable de hasta 200 m, sobre el que se pueden instalar, distribuidas aleatoriamente, un máximo de 10 rosetas en las que se permite tener conectados simultáneamente hasta 8 terminales.

Existen dos modalidades de esta configuración: en la más habitual, la TR1 se ubicará en uno de los extremos del bus que se extenderá en la longitud mencionada hasta finalizar en una roseta que incluirá una resistencia de terminación. La otra posibilidad consiste en ubicar la TR1 en un punto intermedio del bus estableciendo de esta manera dos ramas, ninguna de las cuales podrán superar los 100 m. En este caso, la distancia entre los extremos del bus podrá ser de hasta 200 m y en ambos extremos habrá una resistencia de terminación. No se permiten configuraciones con más de dos ramas.

2.5.7.4.3.2. Bus pasivo extendido

En el caso de que 200 m no sean suficientes para llegar desde la TR1 hasta el emplazamiento donde se encuentran los terminales, se puede instalar este tipo de bus caracterizado porque con él se alcanzan hasta 500 m. Sin embargo, en este caso sólo se permite la conexión simultánea de un máximo de 4 terminales que, además, deberán encontrarse agrupados en los últimos 50 m del bus. Presenta una sola rama con resistencia de terminación en su extremo. En otras palabras, se gana alcance y se pierde flexibilidad: menos terminales y no se pueden conectar en cualquier punto del bus.

2.5.7.4.3.3. Bus largo

Si con el bus extendido no es suficiente, aun disponemos del bus largo, denominado así porque alcanza los 1000 m. Presenta una sola rama con resistencia de terminación en su extremo. En este caso, se puede conectar un único terminal.

Por razón de soportar un único terminal, se conoce también esta topología como bus punto a punto. No se debe confundir esta terminología que hace referencia a una configuración de cableado con la que en los mismos términos se refiere al modo de funcionamiento de la capa de datos del protocolo de canal D.

2.5.7.5. Canales de Acceso en la RDSI

Para la transferencia de información y señalización se han definido en la RDSI los siguientes tipos de canales digitales (o vías de transferencia de la información):

Canal B

Es un canal a 64 Kbps. que transporta la información generada por el terminal de usuario.

Canal D

Es un canal a 16 ó 64 Kbps., dependiendo de la estructura de acceso del abonado, que se utiliza para transportar la señalización en el interfaz *usuario-red*. También puede utilizarse para transmitir información de usuario a baja velocidad.

Canal n x 64

Permite la transferencia de información de usuario a velocidades superiores a 64 Kbps. Los valores válidos para *n* serán desde 2 hasta 30.

FIGURA 5.36: (a) Conducto digital de velocidad básica. (b) Conducto digital de velocidad primaria.

2.5.7.6. Configuraciones de acceso comercializadas

Los canales de acceso a la RDSI descriptos en el punto anterior, no se proporcionan de forma aislada, sino que se ofrecen agrupados en configuraciones normalizadas. Existen dos configuraciones elementales que se pueden comercializar de forma individual cada una de ellas, el denominado Acceso Básico y el Acceso Primario. (Ver **figura 5.37**) Cada una de estas configuraciones, a su vez, se pueden agrupar entre sí, o incluso de manera cruzada de tal forma que se obtengan funcionalidades que mejoran lo que ofrecería una simple agregación de prestaciones individuales; nos estamos refiriendo al Grupo de Salto y al Grupo ISPBX.

2.5.7.6.1. Acceso Básico

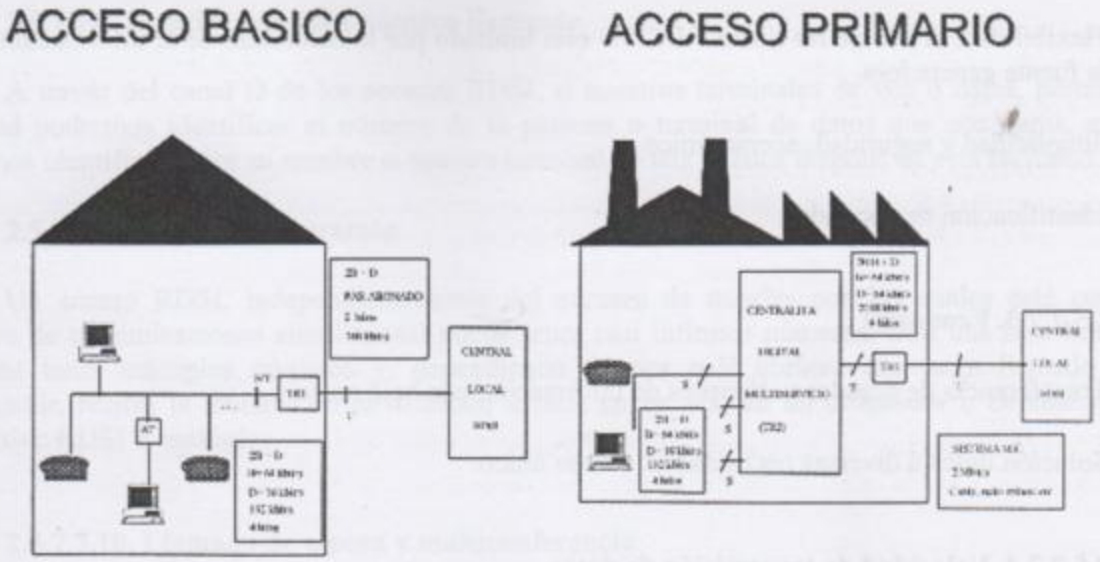


FIGURA 5.37: Estructura de Acceso.

Está constituido por dos canales B (a 64 Kbps.) para la transmisión de información, y un canal D (a 16 Kbps.) para la señalización de usuario. Permite conectar simultáneamente hasta 8 terminales.

En el lado de las instalaciones de usuario, (interfaz S/T), la velocidad de transmisión total es de 192 Kbps distribuidos de la siguiente manera: 2 canales B, 1 canal D, y la información adicional necesaria para el mantenimiento del sincronismo, el mantenimiento de la estructura multitramas, (actualmente no se utiliza), y el control de acceso al canal de señalización. Como ya se mencionó, está soportado por una configuración a 4 hilos (2 para transmisión y 2 para recepción). En el lado red, (interfaz U), la velocidad en línea es de 160 Kbps. y la transmisión es full-duplex con técnicas de cancelación de eco y está soportado en el bucle de abonado de cobre actualmente existente.

2.5.7.6.2. Acceso Primario

Está constituido por 30 canales B (a 64 Kbps) y un canal D (a 64 Kbps) con una velocidad total de 2 Mb/s. En el lado de las instalaciones de usuario (interfaz T) se dispone de una trama de 2048 Kbps que, a través de una agrupación funcional TR2 (normalmente una centralita digital cuyas extensiones pueden ser líneas de interfaz S) puede estructurarse en otras combinaciones de canales de entre las ya mencionadas. En el lado red, esto es, para enlazar las instalaciones de usuario con la central RDSI, el acceso está soportado por un sistema de transmisión MIC a 2 Mbps.

2.5.7.7. Ventajas que ofrece la RDSI

2.5.7.7.1. Calidad de servicios

- Mayor rapidez en los tiempos de *establecimiento/liberación* de llamada.
- Gran fiabilidad y calidad de audio.

- Alta velocidad de transmisión y baja tasa de errores.
- Flexibilidad: el uso de las líneas RDSI no está limitado por la naturaleza de la información ni por la fuente generadora.
- Simplicidad y seguridad: acceso único.
- Identificación de abonados.

2.5.7.7.3. Economía

- Transferencia de grandes volúmenes de información con bajo costo.
- Solución única a diversas necesidades: acceso único.

2.5.7.7.4. Velocidad de transmisión de datos

Los enlaces a través de accesos RDSI son en el peor de los casos tres veces más rápidos, en velocidad real, que un enlace realizado a través de una línea analógica convencional por RTB (Red Telefónica Básica). En ocasiones, y dependiendo del estado de la RTB en una determinada zona, la velocidad puede llegar a ser hasta cinco veces más rápida por RDSI que por RTB.

2.5.7.7.5. Ancho de banda regulable

La mayoría de dispositivos RDSI (tarjetas RDSI de ordenador, equipos de video-conferencia, etc.) permiten la suma de canales RDSI. Esto supone que si disponemos de un acceso básico RDSI y una tarjeta de ordenador RDSI adecuada, podremos transmitir información o navegar por Internet a 128 Kbps y no a 64 Kbps, dado que podremos sumar el ancho de banda de nuestra conexión, y por tanto la velocidad. Si disponemos de un acceso primario, y el dispositivo adecuado, podremos tener hasta 2 Mbps de ancho de banda (30 canales x 64 Kbps = 1.920 Kbps.)

2.5.7.7.6. Efectividad en la transmisión de datos

En muchas ocasiones cuando pensamos que hemos terminado de transmitir una archivo de datos a través de un módem, descubrimos que éste no llegó correctamente a su destino. Son muchas las razones que pueden producir pérdida de datos en la transmisión de datos, pero en el caso de una transmisión de datos a través de RDSI, las posibilidades de errores en la transmisión son casi despreciables frente a las transmisiones a través de la RTPC[34].

2.5.7.7.7. Seguridad de las comunicaciones de Voz y Datos

Las comunicaciones, sean de voz o datos, no podrán ser intervenidas en ningún caso a través de la RDSI, dado que viajan codificadas digitalmente y encriptadas.

[34] Red Telefónica Pública Conmutada.

2.5.7.7.8. Identificación del número llamante

A través del canal D de los accesos RDSI, si nuestros terminales de voz o datos, permiten esta facilidad podremos identificar el número de la persona o terminal de datos que nos llama, e incluso podremos identificarlo por su nombre si nuestro terminal de voz o datos dispone de esta facilidad.

2.5.7.7.9. Múltiple numeración

Un acceso RDSI, independientemente del número de canales por los cuales esté compuesto (número de comunicaciones simultáneas) puede tener casi infinitos números. Con una sola línea RDSI podemos tener múltiples números y, dependiendo de por cuál número nos haya llamado nuestro interlocutor, recibir la llamada en un teléfono u otro, en un fax, en un ordenador o en cualquier otro dispositivo RDSI o analógico.

2.5.7.7.10. Llamada de espera y multiconferencia

Cuando estamos en el transcurso de una comunicación de voz, si alguien nos llama a ese mismo número, la central pública del operador nos informará a través del canal D, que existe una llamada para nosotros, así como del número del interlocutor que nos llama. Entonces podremos, o bien retener la llamada en curso y atender la llamada entrante o realizar una multiconferencia, hablando las tres partes a la vez. También podremos realizar una multiconferencia con una llamada recibida y otra que nosotros hemos realizado o con dos llamadas realizadas por nosotros. No obstante, estas facilidades dependerán de las posibilidades del terminal telefónico del cual dispongamos.

2.5.7.7.11. Video-Conferencia

El estándar mundial de video-conferencia profesional, es el denominado H-323. Este estándar regula una serie de condiciones técnicas y de protocolos de comunicación que permiten que cuando llamamos a cualquier número para establecer una video-conferencia éste nos responda y podamos ver y hablar con nuestro interlocutor. Este estándar está basado en la RDSI como única red telefónica para el transporte de video-conferencia. El H-323 permite también compartir aplicaciones informáticas mientras vemos y hablamos con nuestro interlocutor. Esto es, poder estar modificando ambos, por ejemplo, una misma hoja de cálculo.

2.5.7.7.12 Ventajas de la RDSI frente a la Red Telefónica Pública Conmutada

En este punto veremos qué ventajas podemos obtener en caso de disponer de una línea RDSI. Hemos considerado que las ventajas de la RDSI frente a la RTPC son resumibles en tres grupos, éstos son ventajas en cuanto a velocidad, ventajas en cuanto a la no necesidad de múltiples interfaces (líneas telefónicas), y ventajas en cuanto a la señalización. Pasamos a ver cada uno de ellos:

Velocidad

El modem tuvo una gran importancia en las comunicaciones entre ordenadores. Permitió a los ordenadores comunicarse entre ellos convirtiendo la información digital que ellos producían en una señal analógica que fluía a través de la red telefónica pública. Pero existe un límite superior en cuanto a la cantidad de información que una línea telefónica analógica puede soportar (transmitir). Actualmente este

límite está en los 56 kbps usando un equipo especial. Usualmente los modems más extendidos tienen una velocidad máxima de transmisión de 33.6 kbps, aunque están limitados por la calidad de la conexión analógica y es rara la vez que van a velocidades mayores de 26.4 o 28.8 kbps.

RDSI, en cambio, permite tener múltiples canales digitales, y permite que operen simultáneamente a través del mismo cable telefónico. El cambio empieza cuando las centrales de conmutación de las redes telefónicas empiezan a soportar conexiones digitales. Así, el mismo cableado telefónico puede ser usado (con una señal digital en lugar de una analógica) para transmitir datos directamente. Este esquema permite un radio de transmisión de datos mucho mayor que el permitido por las líneas analógicas. Un canal RDSI Básico (BRI), usando un protocolo adicional para el canal (como Bonding, o Multilink - PPP) soporta una velocidad de transferencia de hasta 128 kbps (sin compresión de datos de ningún tipo).

Múltiples Dispositivos

Antes, era necesario tener una línea telefónica para cada dispositivo que se quisiera usar simultáneamente. Por ejemplo, era necesaria una línea telefónica para un teléfono, otra para un fax, otra para el ordenador y otra para un sistema de video-conferencia en caso de que se quisieran usar todos estos aparatos simultáneamente. Por lo tanto estar bajando un fichero, mientras está hablando por teléfono o viendo una animación real en una pantalla de video puede necesitar un número excesivamente alto de líneas telefónicas (sobre todo en precio). En cambio, la RDSI nos permite combinar diferentes fuentes de datos digitales y enrutar cada una de ellas al destino adecuado. Debido a que la línea es digital, es más fácil mantener los niveles de ruido e interferencias bajo mínimos mientras combinamos todas las señales que recibimos de los distintos dispositivos. RDSI técnicamente se refiere a un grupo específico de servicios digitales que nos son dados a través de un único interfaz estándar. Sin RDSI, serían necesarios diferentes interfaces para cada dispositivo.

2.5.9. Modo de Transferencia Asíncrono (ATM)[35]

El Modo de Transferencia Asíncrono, también conocido como retransmisión de celdas, es conceptualmente similar a la técnica de retransmisión de tramas (Frame Relay). Ambas técnicas presentan fiabilidad y fidelidad para ofrecer una conmutación de paquetes más rápida que X.25 en aplicaciones digitales modernas. ATM es incluso más funcional que retransmisión de tramas, pudiendo admitir velocidades de transmisión varios órdenes de magnitud superior.

Aparte de las similitudes físicas, ATM y retransmisión de tramas han seguido historias parecidas. La retransmisión de tramas se desarrolló como parte de la red RDSI, encontrando actualmente un gran uso en redes privadas y otras aplicaciones fuera de RDSI, en particular puentes y dispositivos de encaminamiento ("*routers*").

Por su parte ATM fue desarrollado como parte del trabajo en RDSI de banda ancha, pero inicialmente se destinó a entornos distintos de RDSI, donde eran necesarias elevadas velocidades de transmisión.

[35] En Inglés: Asynchronous Transfer Mode.

2.5.9.1. Arquitectura del protocolo

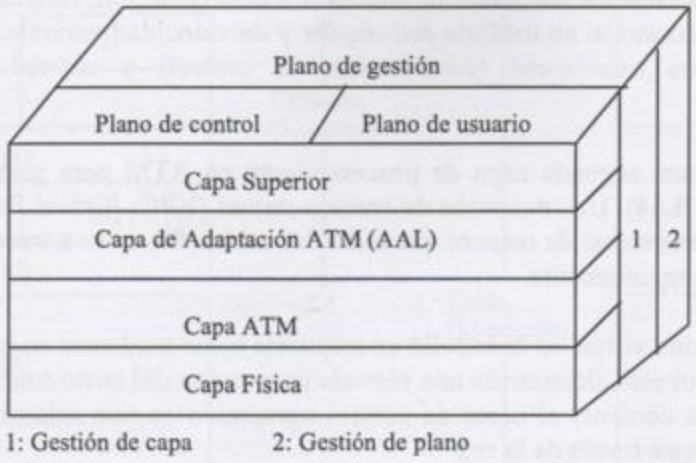


FIGURA 5.44: Modelo de referencia del protocolo ATM.

ATM es similar en muchos aspectos a la conmutación de paquetes X.25 y a la técnica de retransmisión de tramas. Al igual que ellas, ATM lleva a cabo la transferencia de los datos en trozos discretos. Además, al igual que X.25 y retransmisión de tramas, ATM permite la multiplexación de varias conexiones lógicas sobre una única interfaz física. En el caso de ATM, el flujo de información en cada conexión lógica se organiza en paquetes de tamaño fijo denominados celdas.

ATM es un protocolo con mínima capacidad de control de errores y de flujo, lo que reduce el costo de procesamiento de las celdas ATM y reduce el número de bits suplementarios requeridos en cada celda, posibilitando su funcionamiento a altas velocidades. El uso de ATM a altas velocidades se ve apoyado adicionalmente por el empleo de celdas de tamaño fijo, ya que de este modo se simplifica el procesamiento necesario en cada nodo ATM.

Las normalizaciones de ITU-T para ATM se basan en la arquitectura del protocolo mostrada en la **figura 5.44**, donde se ilustra la arquitectura básica para una interfaz entre usuario y red. la capa física especifica el medio de transmisión y un esquema de codificación de la señal. Las velocidades de transmisión especificadas en la capa física son 155,52 Mbps y 622,08 Mbps, siendo posibles velocidades superiores e inferiores.

Dos capas de la arquitectura se encuentran relacionadas con las funciones ATM. Existe una capa ATM común a todos los servicios de conmutación de paquetes, y una capa de adaptación ATM (AAL) dependiente del servicio. La capa ATM define la transmisión de datos en celdas de tamaño fijo, al tiempo que establece el uso de conexiones lógicas. El empleo de ATM crea la necesidad de una capa de adaptación para admitir compatibilidad con los protocolos de transferencia de información no basados en ATM. AAL agrupa información de capas superiores en celdas ATM para enviarlas a través de una red ATM, al tiempo que extrae la información de las celdas ATM y la transmite a las capas superiores.

2.5.9.2. Conexiones lógicas ATM

Las conexiones lógicas en ATM están relacionadas con las conexiones de canales virtuales (VCC: *Virtual Channel Connection*). Una VCC es similar a un circuito virtual en X.25 o a una conexión de

enlace de datos en la técnica de retransmisión de tramas; es la unidad básica de conmutación en una red ATM. Una VCC se establece entre dos usuarios finales a través de la red, intercambiándose celdas de tamaño fijo a través de la conexión en un flujo *full-duplex* y de velocidad variable. Las VCC se utilizan también para intercambios usuario-red (señalización de control) y red-red (gestión de red y encaminamiento).

Se ha introducido una segunda capa de procesamiento en ATM para gestionar el concepto de camino virtual (ver **figura 5.44**). Una conexión de camino virtual (VPC: *Virtual Path Connection*) es un haz VCC con los mismos extremos, de manera que todas las celdas fluyendo a través de las VCC de una misma VPC se conmutan conjuntamente.

El concepto de camino virtual se desarrolló en respuesta a una tendencia en redes de alta velocidad en la que el costo de control está alcanzando una elevada proporción del costo total de la red. La técnica del camino virtual ayuda a contener el costo de control agrupando en una sola unidad conexiones que comparten caminos comunes a través de la red.

Las acciones de la gestión de red pueden ser aplicadas a un pequeño número de grupos de conexiones en lugar de a un gran número de conexiones individuales.

2.5.9.3. Celdas ATM

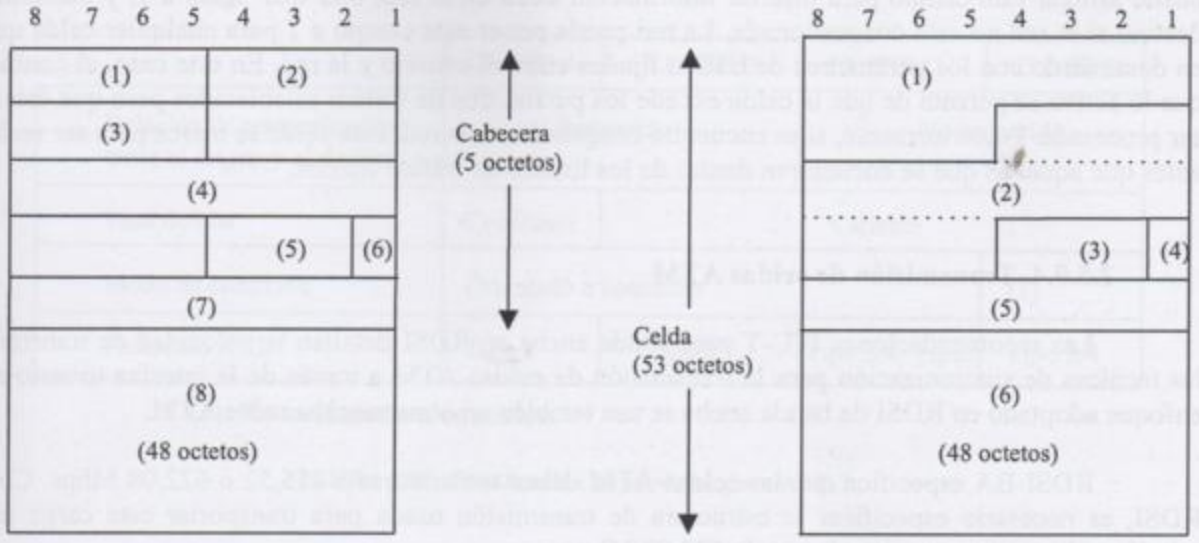
El modo de transferencia asíncrono utiliza celdas de tamaño fijo, que constan de 5 octetos de cabecera y de un campo de información de 48 octetos. El empleo de celdas pequeñas de tamaño fijo presenta varias ventajas. En primer lugar, el uso de celdas pequeñas puede reducir el retardo de cola para celdas de alta prioridad, ya que la espera es menor si se reciben ligeramente después de que una celda de baja prioridad haya conseguido el acceso a un recurso (por ejemplo, el transmisor). En segundo lugar, parece que las celdas de tamaño pequeño pueden ser conmutadas más eficientemente, lo que es importante para las altas velocidades de ATM. La implementación física de los mecanismos de conmutación es más fácil para celdas de tamaño fijo.

2.5.9.3.1. Formato de cabecera

La **Figura 5.46a** muestra el formato de cabecera en la interfaz usuario-red. En la **Figura5.46b** se muestra el formato de cabecera interno a la red, en el que no se especifica el campo de control de flujo genérico, que realiza funciones extremo a extremo. En cambio, el campo identificador de camino virtual pasa de 8 a 12 bits, lo que permite un gran número de VPC internos para dar cabida a los de los subscriptores y a los necesarios para realizar la gestión de la red.

El campo *control de flujo genérico* (GFC) no se incluye en la cabecera de las celdas internas a la red, sino sólo en la interfaz usuario-red, por lo que únicamente se puede usar en el control de flujo de celdas en la interfaz local usuario-red. El campo podría utilizarse para ayudar al usuario en el control del flujo de tráfico para diferentes calidades de servicio. Un candidato al empleo de este campo es un indicador de prioridad múltiple para controlar el flujo de información dependiente del servicio. En cualquier caso, el mecanismo GFC se usa con el fin de aliviar la aparición esporádica de sobrecarga en la red.

El *identificador de camino virtual* (VPI) es un campo de encaminamiento para la red. Éste es de 8 bits para la interfaz usuario-red y de 12 bits para la interfaz red-red, permitiendo un número superior de caminos virtuales en la red. El *identificador de canal virtual* (VCI) se emplea para encaminar a y desde el usuario final, funcionando como un punto de acceso al servicio.



(a)
(1): Control de flujo genérico
(2) y (3): Identificador de camino virtual
(4): Identificador de canal virtual
(5): Tipo de carga útil
(6): CLP
(7): Control de errores de cabecera
(8): Campo de información

(b)
(1): Identificador de camino virtual
(2): Identificador de canal virtual
(3): Tipo de carga útil
(4): CLP
(5): Control de errores de cabecera
(6): Campo de información

FIGURA 5.46 (a): Interfaz usuario-red. (b): Interfaz red-red.

El campo *tipo de carga útil* indica el tipo de información contenida en el campo de información. La tabla de la **Figura 5.47** muestra la interpretación de los bits PT. Un valor 0 en el primer bit indica información de usuario; es decir, información de la capa inmediatamente superior. En este caso, el segundo bit indica si se ha producido congestión; el tercer bit, conocido como bit de indicación ATM-usuario-ATM-usuario (AAU) es un campo de un bit que indica que la celda transporta información de gestión de red en una VCC de usuario sin afectar los datos de usuario, de modo que se proporciona información de control en banda.

Codificación PT	Interpretación
0 0 0	Celda de datos de usuario, AAU=0, congestión no experimentada.
0 0 1	Celda de datos de usuario, AAU=1, congestión no experimentada.
0 1 0	Celda de datos de usuario, AAU=0, congestión experimentada.
0 1 1	Celda de datos de usuario, AAU=1, congestión experimentada.
1 0 0	Celda asociada al segmento OAM F5.
1 0 1	Celda asociada a OAM F5 extremo a extremo.
1 1 0	Celda de gestión de recursos.
1 1 1	Reservada para funciones futuras.
AAU= indicación de usuario ATM a usuario ATM.	

FIGURA 5.47: Codificación del campo de tipo de carga útil (PT).

La prioridad de pérdida de celdas (CLP) se emplea para ayudar a la red ante la producción de congestión. Un valor 0 indica que la celda es de prioridad relativamente superior, no siendo descartada a menos que no quede otra opción; un valor 1 indica que la celda puede descartarse en la red. El usuario

puede utilizar este campo para insertar información extra en la red, con CLP igual a 1, y transmitirla al destino si la red no está congestionada. La red puede poner este campo a 1 para cualquier celda que esté en desacuerdo con los parámetros de tráfico fijados entre el usuario y la red. En este caso, el conmutador que lo activa se percata de que la celda excede los parámetros de tráfico establecidos pero que ésta puede ser procesada. Posteriormente, si se encuentra congestión en la red, esta celda se marca para ser rechazada antes que aquellas que se encuentran dentro de los límites de tráfico fijados.

2.5.9.4. Transmisión de celdas ATM

Las recomendaciones ITU-T para banda ancha en RDSI detallan la velocidad de transmisión y las técnicas de sincronización para la transmisión de celdas ATM a través de la interfaz usuario-red. El enfoque adoptado en RDSI de banda ancha se usa también en otras muchas redes ATM.

RDSI-BA especifica que las celdas ATM deben transmitirse a 155,52 o 622,08 Mbps. Como en RDSI, es necesario especificar la estructura de transmisión usada para transportar esta carga útil. Su estudio se ha pospuesto para el caso de 622,08 Mbps.

2.5.9.5. Capa de Adaptación ATM

El uso de ATM hace necesaria la existencia de una capa de adaptación para admitir protocolos de transferencia de información no basados en ATM. Dos ejemplos son voz PCM (Modulación por código de pulso) y LAPF. Voz PCM es una aplicación que produce una secuencia de bits a partir de una señal de voz. Para implementar esta aplicación sobre ATM es necesario agrupar bits PCM en celdas para su transmisión, y leerlas cuando sean recibidas en el receptor de manera que se obtenga un flujo constante de bits. LAPF es el protocolo de control de enlace de para retransmisión de tramas. En un entorno heterogéneo en el que existen redes conectadas con redes de retransmisión de tramas, una forma adecuada de integrar los redes es realizar una transformación entre tramas LAPF y celdas ATM, lo que implica la segmentación de una trama LAPF en celdas de transmisión y la agrupación de las celdas en receptor. Permitiendo el uso de LAPF sobre ATM es posible la implementación de aplicaciones de retransmisión de tramas y protocolos de señalización de control a través de redes.

2.5.9.5.1. Servicios AAL

El documento 1.362 de ITU-T especifica los siguientes ejemplos generales de servicios ofrecidos por AAL:

- Gestión de errores de transmisión.
- Segmentación y ensamblado para permitir la transmisión de bloques mayores de datos en el campo de información de celdas ATM.
- Gestión de condiciones de pérdida de celdas y de celdas mal insertadas.
- Control de flujo y temporización.

	CLASE A	CLASE B	CLASE C	CLASE D
Relación de temporización entre el origen y el destino	Requerido		No requerido	
Tasa de bits	Constante	Variable		
Modo de conexión	Orientado a conexión			(1)
Protocolo AAL	Tipo 1	Tipo 2	Tipo 3/4, Tipo5	Tipo 3/4

(1): No orientado a conexión.

FIGURA 5.49: Clasificación de servicios para AAL.

Con el fin de minimizar el número de protocolos AAL diferentes que pueden ser especificados según las distintas necesidades, ITU-T ha definido cuatro clases de servicios que cubren un amplio rango de requisitos (**Figura 5.49**). La clasificación se realiza teniendo en cuenta si la relación de temporización debe ser mantenida entre el origen y el destino, si la aplicación necesita una velocidad de transmisión constante y si la transferencia es o no orientada a conexión. Un ejemplo de un servicio clase A es la emulación de circuitos, en cuyo caso se usa una velocidad constante, lo que requiere el mantenimiento de una relación de temporización, y una transferencia orientada a conexión. Un ejemplo de servicio clase B es la transmisión de video a velocidad variable, como es el caso de videoconferencias. Aquí, la aplicación es orientada a conexión, siendo importante la temporización, pero la velocidad de transmisión varía dependiendo de la cantidad de actividad en la escena. Las clases C y D corresponden a aplicaciones de transferencia de datos. La velocidad puede variar en ambos siendo necesaria una relación de temporización especial; las diferencias en la velocidad de datos son gestionadas por los sistemas finales haciendo uso de memorias temporales. La transferencia puede ser orientada a conexión (clase C) o no orientada a conexión (clase D).

2.5.10. Redes Satelitales (VSAT)[36]

Estas redes llamadas de **terminales de abertura muy pequeña** o redes de microterminal caen en una de las dos categorías:

- Las redes más tempranas, y las más ampliamente establecidas. Emiten una señal de datos desde una estación central a todas las terminales de la red. Las VSAT mismas no pueden transmitir.
- La segunda categoría es la **red interactiva**. En esta caso, las VSAT pueden transmitir a la estación central, la cual puede estar conectada a una gran computadora corporativa. El enlace ascendente (up-link) generalmente tiene una capacidad de transmisión de datos más baja que el enlace descendente (down-link).

[36] En Inglés: Very Small Aperture Terminal.

Este tipo de redes se han propagado rápidamente debido a ventajas tales como: muy buena relación costo-eficiencia, precisión y transparencia, reconfigurabilidad y expandibilidad, corto tiempo de instalación, y sobre todo, independencia de los otros servicios alternativos.

La red VSAT presta un servicio ideal para infraestructuras de telecomunicaciones en áreas rurales de países del tercer mundo.

Una red de este tipo puede ser conveniente:

- Sobre redes de paquetes de datos ligeramente cargadas, transportando tráfico de ráfagas en el cual un gran número de periféricos remotos deben comunicarse con una central. Un buen ejemplo podría incluir consultas de verificación o de existencia de tarjetas de crédito.

- Donde los servicios de datos o líneas arrendadas digitales son buenos, pero no están rápidamente disponibles desde la compañía de telecomunicaciones o administración. El ejemplo podría incluir compañías que tienen muchas ubicaciones fuera de la ciudad o tienden a muchos movimientos.

Las redes VSAT tipo estrella son atractivas para grandes organizaciones con una estructura ramificada, como ser agencias de prensa, bancos, cadena de hoteles, compañías de seguros, agencias de viaje, etc.

Son posibles servicios tales como: intercambio de datos, telex, facsímil, transmisión de fotogramas y teléfono.

Las funciones que pueden ser soportadas incluyen, por ejemplo: instrucciones, reportes, cambios, bibliotecas, chequeos, telecomandos, telemetría, etc.

La información promedio está entre los 1,2 y 64 Kbps y hasta 2 Mbps.

2.5.10.1. Funciones básicas del sistema

En las aplicaciones el caudal del satélite es dividido en porciones de frecuencias. Una simple porción de frecuencia puede ser usada por una estación terrestre en las siguientes circunstancias:

- En ciertas ranuras de frecuencias, las que son ocupadas permanentemente y exclusivamente (FDMA: Acceso Múltiple por División de Frecuencia).

- Por un solo canal banda base por ranura (SCPC: Canal Único por Portadora).

- En ciertas ranuras de tiempo ocupadas exclusivamente (TDMA: Acceso Múltiple por División de Tiempo).

- Permanentemente junto con otras. La señal deberá ser inmunizada contra colisiones por codificación de propagación (CDMA: Acceso Múltiple por División de Código).

- Por un cierto porcentaje de tiempo, colectivamente, y con repetición de transmisión en el caso de colisiones (ALHOA).

- En ciertas ranuras de tiempo, colectivamente, y con petición de transmisión en el caso de colisiones (S-ALHOA: ALHOA Ranurado).

2.5.10.2. Componentes

2.5.10.2.1. Microestaciones VSAT

Al haber suficiente ancho de banda en el transponder del satélite, no hay límites prácticos en la cantidad de terminales que podrían ser instaladas en una única red. Estas microestaciones tienen antenas de 1,6 hasta 3 metros (diámetro menor que 5 longitudes de onda) y salidas de cerca de 1 watt de potencia. Las estaciones se simplifican pues, por un lado, el mayor ancho del haz (consecuencia del menor diámetro de la antena) elimina la necesidad de costosos equipos de rastreo. Todo esto ha permitido reducir considerablemente las estaciones.

El costo de tener estaciones de usuario final más baratas es un mayor retardo. Con estas VSATs instaladas en los usuarios finales, es ahora técnicamente posible interconectar puntos arbitrarios dentro de grandes regiones. De este modo, redes regionales extremadamente competitivas llegan a ser factibles, y son prometedoras para proveer de comunicaciones en áreas rurales del tercer mundo.

El enlace ascendente por lo general llega a 19,2 Kbps, pero el descendente es más rápido, con frecuencia de 512 Kbps. En muchos sistemas VSAT, ellas no tienen suficiente energía para comunicarse en forma directa unas con otras (desde luego, vía satélite). Para ello se necesita una estación terrena especial, el eje, con una antena grande de ganancia alta para retransmitir el tráfico entre VSAT. En este modo de operación, ya sea el emisor o el receptor tiene una antena grande y un amplificador potente. (Ver **figura 5.53**)

2.5.10.2.2. Hub Station

Para la **estación central** se elige un valor estándar de 5,6 m. Una estación maestra *hub station*, puede originar tramas con una ráfaga de referencia en cuyo inicio se asigna un pequeño segmento de tiempo a cada estación que así puede solicitar su transmisión.

La estación principal (*hub*) puede estar dedicada a un único usuario o puede ser compartida por un cierto número de usuarios; y puede estar localizada ya sea en el cliente o conectado sobre una línea arrendada. En todos los casos, es esencialmente transparente para el paso de señales a través de él, y aunque sea compartido, el usuario puede mantener efectivo control completo sobre esta red. En un edificio adicional están el **sistema receptor y transmisor** y el **sistema de manejo** de red.

2.5.10.3. Arquitectura del sistema

Un sistema Ku-band es descripto como sigue:

La información de salida contiene portadora TDM desde la estación central al grupo de VSAT iguales de 64 Kbps, los valores típicos y máximos son 512 Kbps y 1,5 Mbps respectivamente.

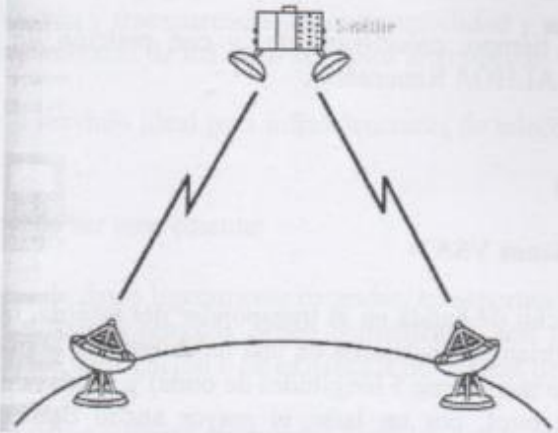


FIGURA 5.53: Enlaces punto a punto de microondas vía satélite.

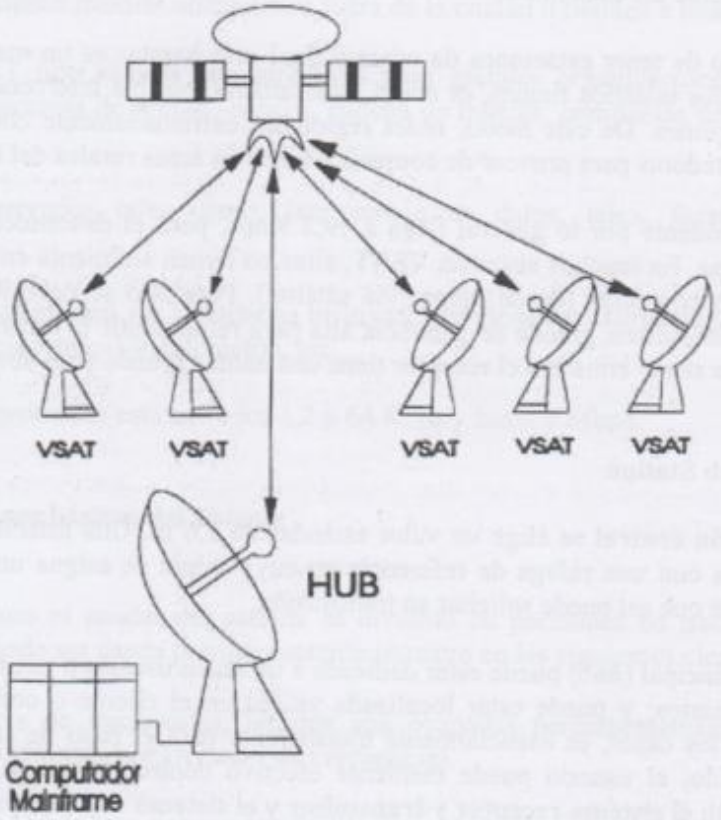


FIGURA 5.54: Grupos de microestaciones VSAT y Hub Station.

La información de una portadora desde el grupo VSAT a la estación central es de 96, 128, o 256 Kbps.

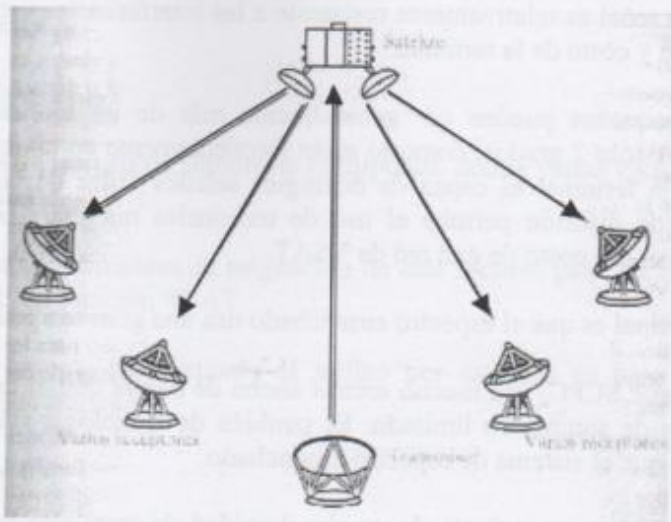


FIGURA 5.55: Enlaces de difusión de microondas vía satélite.

La modulación usada en ambas direcciones es BPSK (Modulación en Fase por Cambio de Clave Binaria).

El valor de la transmisión sobre el canal es dos veces el valor de la información, ya que una mitad del valor es aplicado para Corrección de Errores hacia delante FEC.

El enlace presupuestado tiene que ser tal que el valor del bit de error bajo buenas condiciones de tiempo e incluyendo el FEC es de diez a la menos siete (1/10.000.000).

Gracias al proyecto de acceso múltiple, con el cual es implementado al protocolo en el satélite, el valor real del error es mucho menor a causa de que se realizan chequeos regularmente para transmisión de error.

2.5.10.4. Técnicas de acceso

La principal diferencia técnica entre las diversas soluciones disponibles está en los esquemas usados en la estación principal (*Hub*) y (en redes interactivas), con la cual las VSAT obtienen el acceso al canal del satélite.

2.5.10.4.1. Redes de Broadcast

Para redes en una dirección (ver **figura 5.55**), hay básicamente dos técnicas en uso: **Sistema de Espectro Ensanchado (Spread Spectrum)** y **Canal Único por Portadora (SCPC: Single Channel Per Carrier)**.

En el primero, el flujo de datos de, por ejemplo 19,2 Kbps, es esparcido sobre una señal de transporte de 5 MHz utilizando un código de difusión. Debido a que los datos son esparcidos sobre un

amplio ancho de banda, la señal es relativamente resistente a las interferencias y esto tiene consecuencias importantes para el tamaño y costo de la terminal.

Los platos muy pequeños pueden *ver* generalmente más de un satélite, especialmente si los satélites están espaciados a sólo 2 grados, como lo están frecuentemente en la actualidad. Con una señal de espectro de difusión, la terminal es capaz de distinguir señales útiles de las espurias. Entonces la modulación del espectro de difusión permite el uso de terminales más baratas y más pequeñas, que construyen la porción mayor del costo de una red de VSAT.

La desventaja principal es que el espectro ensanchado usa una gran cantidad de ancho de banda.

En cuanto al enfoque SCPC, usa mucho menos ancho de banda que el anterior, de modo que es útil cuando el espectro es de suministro limitado. Es también de tecnología relativamente simple y es mejorable más fácilmente que el sistema de espectro ensanchado.

Sin embargo, sufre el inconveniente de mucha densidad de muy alto poder espectral que crea problemas de intermodulación a frecuencias más altas, produciendo interferencia potencial con otras señales. Esto significa que las señales tengan que ser esparcidas ampliamente y en tasa de uso altas, su mayor eficiencia de ancho de banda es menos marcado.

Una tercera tecnología llamada **FM en cuadratura** está en la actualidad emergiendo en el mercado de emisión por difusión (*broadcast*) de datos. La gran ventaja de este enfoque es que una tarjeta de expansión de PC de *FM en cuadratura* costará mucho menos que el plato y el convertidor de bajo ruido. La desventaja es que requiere de todo un transponder, de modo que no es realmente económico a menos que el número de terminales sea medido en miles.

2.5.10.4.2. Redes Interactivas

Algunas redes de dos vías también usan espectro de difusión o tecnología SCPC. Sin embargo, las demandas de este tipo de red son más bien diferentes, ya que es requerido un control de acceso de terminales. Como resultado, el enfoque más penetrante sobre el enlace terminal a estación principal es el **Acceso Múltiple por División de Tiempo (TDMA)**.

En un esquema TDMA, uno o más canales son compartidos entre un gran número de terminales, el promedio de canales para terminales depende de la carga de tráfico del canal patrón y la cantidad de demora que puede ser tolerada.

Este enfoque es particularmente ventajoso donde las redes están ligeramente cargadas, ya que algunos cientos de terminales pueden ser soportadas sobre un único canal de 64 Kbps, tomando al costo del enlace de transmisión sin importancia.

Hay tres variaciones generalmente en uso: **ALHOA puro**, **reservación TDMA**, y **ALHOA ranurado**.

2.5.10.5. Aplicaciones

2.5.10.5.1. Servicio VSAT

Los servicios VSAT son redes satelitales multipunto, donde varias estaciones terrenas comparten un mismo segmento espacial.

Una estación central administra la asignación de este recurso para dar satisfacción a la demanda específica de tráfico de cada estación VSAT.

Esta tecnología es apta para cuando el tráfico por estación es bajo o medio, y poseen una importante distribución geográfica.

Tipo de servicio

- Enlaces Punto-Multipunto.
- 24 hs/365 días.
- Tráfico bajo y medio.
- Interfaces normalizadas.
- Múltiples protocolos.

Aplicaciones

- Autorización de tarjetas de crédito.
- Reservas de pasajes.
- Consultas interactivas.
- Extensiones bancarias.

2.5.10.5.2. Servicios SCPC

Estos servicios son enlaces satelitales de asignación exclusiva y permanente, orientados a resolver necesidades de comunicación de tráfico intensivo y velocidades medias y altas. Para la conformación de estos enlaces se asignan en forma exclusiva y permanente una porción del segmento espacial.

Tipo de servicio

- Enlaces Punto-Punto.
- 24 hs/365 días.

- Tráfico alto y medio.
- Transparencias a los protocolos.
- Interfaces normalizadas.

Aplicaciones

- Transferencia de datos a alta velocidad.
- Enlaces Host a Host.
- Publishing.
- Voz y fax.

2.5.10.5.3. Servicios de Broadcasting

Son redes satelitales punto-multipunto, para aplicaciones de difusión de datos, audio y video.

Estos sistemas están implementados con la misma tecnología digital, lo que permite nuevas funciones no disponibles en los sistemas analógicos.

Desde la estación central de control se pueden supervisar individualmente todas las estaciones receptoras asociadas a cada cliente en particular.

Tipo de servicio

- Enlaces Punto-Multipunto.
- 24 hs/365 días.
- One Way (una dirección).
- Totalmente digital.

Aplicaciones

- Data Broadcasting:
  - Agencia de noticias.
  - Pizarra financiera.
  - Boletines metereológicos.
- Radio Broadcasting.
- Video Broadcasting.

Preguntas de Repaso a la Unidad 2

- 1) Cuando se transfieren archivos entre dos computadoras existen al menos dos estrategias de confirmación. La primera es que el archivo sea seccionado en paquetes y que el receptor confirme cada uno de ellos. La segunda es que, finalizada la transferencia del archivo, el receptor mande una confirmación referida a la recepción de todo el archivo. ¿Qué ventajas y desventajas trae cada una de estas estrategias?

- 2) En LANS, cuáles de los siguientes modos de acceso al medio son random:

  a. CSMA/CD..

  b. token passing.

  c. adjudicación de ranuras de tiempo

  d. ninguna de las anteriores

  e. cualquiera de las anteriores.

- 3) Explique las categorías de cable UTP para aplicaciones en redes LAN

- 4) En LANS, la capa LLC puede implementar un servicio orientado a conexión solamente sobre los protocolos:

  a. CSMA/CD (802.3).

  b. token bus (802.4).

  c. token ring (802.5).

  d. cualquiera de las anteriores.

  e. ninguna de las anteriores.

- 5) El servicio sin conexión del protocolo 802.2 (LLC) envía los datos en frames *unnumbered* (de control, sin número de secuencia, llamados ***U***) en lugar de usar frames *de información* (con número de secuencia y datos, llamados ***I***). ¿Por qué piensa que fue realizada esta elección?

- 6) La norma IEEE 802.3 especifica los niveles OSI:
  a. 1 y 3.
  b. mitad del 2.
  c. 1.
  d. 1 y mitad del 2.
  e. 1 y 2.
  f. 2.
  g. ninguna de las anteriores.

- 7) Describir la trama 802.3 (CSMA/CD) identificando en la misma el nombre y el tamaño de los distintos campos.

- 8) ¿Para qué se utiliza el campo de preámbulo de las tramas de las subcapas MAC 802.3 y 802.4?

- 9) ¿Qué pasaría en CSMA/CD, si luego de ocurrida una colisión las estaciones esperaran un tiempo fijo *t*, igual para cada una de ellas?

- 10) Recuerde qué es una NIC, para qué sirve, cuándo es necesario instalarla y cuáles son los datos que maneja internamente.

- 11) ¿Cuáles son las diferencias entre el protocolo 802.3 y el 802.11?

- 12) ¿Cuáles son las variantes de capa física del 802.11?

- 13) ¿Cuál es el formato de la trama 802.11?

- 14) ¿Por qué el campo de datos de las tramas de MAC 802.5 no tiene un límite inferior para su longitud?

- 15) Realizar los correspondientes diagramas de flujo que representen en forma simplificada el funcionamiento del protocolo CSMA/CD y sus variantes. Explicar el significado de las decisiones y flujos completados.

  EMISIÓN DE UNA TRAMA:

  RECEPCIÓN DE TRAMA:

  Explicar que evalúa la decisión "¿Trama Corta?" del diagrama. ¿Qué nombre recibe dicha trama?

- 16) ¿Cuáles de las siguientes capas del modelo OSI son innecesarias o muy simples en una LAN aislada?:

  a) presentación y red.

  b) aplicación y transporte.

  c) red.

  d) sesión.

  e) ninguna de las anteriores.

- 17) Se dice que CSMA/CD es inapropiado para aplicaciones en tiempo real porque el peor caso de intervalo de retransmisión no es limitado. ¿Bajo que circunstancias puede usarse el mismo argumento para un anillo con token passing? ¿Bajo que circunstancias tiene entonces un peor caso conocido? Asumir que el número de workstations en el anillo es fijo y conocido.

- 18) ¿Por qué las tramas de MAC 802.3 no tienen campos de control? ¿Porqué sí los tienen las de 802.4 y 802.5? Dar ejemplos de su uso.

- 19) ¿Para cuáles de los siguientes protocolos de la subcapa MAC puede garantizarse la existencia de una cota máxima de tiempo para la liberación de una trama al medio?:

  a) LLC (IEEE 802.2)

  b) CSMA/CD (IEEE 802.3)

c) token bus (IEEE 802.4)

d) token ring (IEEE 802.5)

e) cualquiera de los anteriores.

f) ninguna de las anteriores.

- 20) "Un repetidor es un dispositivo que puede instalarse en redes locales del tipo 802.3 (CSMA/CD). Su función consiste en retransmitir las secuencias de bits que le van llegando. La necesidad de su uso aparece esencialmente porque las señales eléctricas en un medio de TX sufren atenuaciones y distorsiones que son mayores, cuanto mayor es la distancia recorrida por ellas. A causa de esto, dependiendo del medio utilizado, existe una distancia *d* tal que para distancias mayores que *d*, una estación receptora no puede reconocer la señal original enviada por el emisor". Determinar si la afirmación anterior es verdadera.

- 21) El algoritmo para el cálculo del retardo para la transmisión en CSMA/CD es el siguiente:

```
if intentos <= 16 then

        k:= min(intentos,10);
        r:= random(0,2^k-1);
        retardo:= r * ranura_de_tiempo;
        intentos:= intentos+1;

end;
```

donde r es un número entero generado de manera aleatoria a partir de una función de distribución uniforme.

  - ¿Qué relación encuentra entre el nro. de colisiones que sufre un transmisor y el tiempo que deberá esperar para intentar retransmitir una trama?
  - ¿Qué tipo de prioridad implícita genera esto?
  - ¿Por qué el tiempo de retardo es múltiplo de un número entero de ranuras de tiempo?
  - ¿Qué ocurre en el protocolo si intentos es mayor que 16? ¿Por qué existe esta cota superior?
  - Compárela con el algoritmo de retardo en CSMA / CA

- 22) ¿Qué sucede en una LAN token ring si una estación acepta el token y entonces se cae inmediatamente? ¿Cómo maneja el protocolo este caso?

- 23) ¿El uso de *wire center* (MAU) tiene alguna influencia en la performance de una LAN token ring?

- 24) ¿Por qué en LANs se divide la capa de enlace de datos en dos subcapas? ¿Se ocupan ambas de controlar errores en los datos? ¿Qué tipos de servicios ofrece cada una de ellas? Explicar.

- 25) Cuál es el cableado utilizado en 10baseT, 100baseT, 1000baseT y 10GigaEthernet?

- 26) Explique qué es y para qué se utiliza un Switch en 802.3

- 27) Indique qué problemas pueden presentarse en 802.5 con respecto al mantenimiento del anillo y del token.

- 28) Explique cómo soluciona el Spanning Tree Protocol el problema de las tormentas de broadcast

- 29) Analizar la veracidad de la siguiente afirmación:

  "En MAC 802.3 (CSMA/CD), si una trama es transmitida al medio físico sin colisiones, puede asegurarse que la subcapa receptora la entrega correctamente a LLC"

- 30) Explique las características de las VLANs. Destaque su importancia en una LAN con numerosos grupos de trabajo.

- 31) Explique las estructuras de acceso de abonado a la ISDN. De ejemplos de aplicación de cada una de ellas

- 32) Para la Red Digital de Servicios Integrados (ISDN), defina:
  Servicio Portador
  Teleservicio
  Servicio Suplementario
  De ejemplos de cada uno de ellos

- 33) Realice un análisis de la celda ATM, explicando cada uno de sus campos. Explique las clases de servicios brindados por el protocolo

- 34) Respecto del protocolo ATM:
  Comente las características que le permiten obtener mayor velocidad que Frame Relay.
  El protocolo ATM; ¿puede manejar tráfico a tiempo real? Justifique su respuesta

- 35) ¿Qué ***ventajas*** poseen las redes VSAT frente a las redes interconectadas por líneas telefónicas conmutadas?. ¿En qué casos utilizaría las líneas telefónicas?:

- 36) En una red VSAT:
  Explique qué es y qué función cumple un telepuerto
  ¿Cuál es el principal problema por el cual una red VSAT no es optima para transmitir voz?

- 37) ¿Qué tipos de enlaces WAN puede contratar una empresa de Córdoba para interconectar su LAN con la de la casa central en Buenos Aires? Compare las distintas alternativas.

Bibliografía de la Unidad 2

- **Kurose, James; Ross, Keith:** *"Redes de computadores. Un enfoque descendente basado en Internet"*. Segunda Edición. PEARSON. Addison-Wesley. 2003
- **Mc. Querry, Steve.:** *"Interconexión de dispositivos de Red Cisco"* Cisco Press. USA 2001
- **Tanenbaum, A. S.**: *"Redes de Computadoras"*. Tercera Edición. Prentice Hall. 2000
- **Tanenbaum, A. S.**: *"Redes de Computadoras"*. Cuarta Edición. PEARSON Prentice Hall. México 2003
- **Esteve Domingo, Manuel y otros.**: *"Redes de Area Local y su interconexión"*.Servicio de Publicaciones de la Universidad Politécnica de Valencia. 2001
- **Schwartz, Mischa**. *"Redes de Telecomunicaciones: protocolos, modelado y análisis"*. Addison-Wesley Iberoamericana. USA 1994
- **TIA/EIA Standard**: *"Comercial Building Telecommunications Cabling Standard TIA/EIA 568 – A"*. 1995
- **Pratt, T. y Bostian, Ch.:** *"Satellite Communications"*. John Willey and Sons. New York 1998
- **Händel, Rainer y otros:** *"ATM Networks: Concepts, Protocols, Aplications"*. Addison-Wesley. London 1994
- **De Prycker, Martin**: *"Asynchronous Transfer Mode: Solution for Broadband ISDN"* Editorial Ellis Horwood. London 1993
- Paginas de Internet.
  - http://www.ieee802.org/
  - http://www.cisco.com/
  - http://www.sandrex.net/redes/redes.htm
  - http://www.discar.com/producto/cab-estr/cat5man.pdf
  - http://www.solnet.com.pe/cursos/redes_conceptos_generales/sld001.htm
  - http://www.techmall.com/smarthome/wirelist.html
  - http://www.att.com/nst/utp1.html
  - http://www.amp.com/
  - http://www.protocols.com/protoc.shtml
  - http://www.networking.ibm.com/mse/mse0c01.html

RFC de IETF

Sobre Frame Relay:

- RFC 1294: ***Multiprotocol Interconnect over Frame Relay.*** T. Bradley, C. Brown, A. Malis. January 1992. (Obsoleted by RFC1490, RFC2427) (Status: PROPOSED STANDARD)
- RFC 1490: ***Multiprotocol Interconnect over Frame Relay.*** T. Bradley, C. Brown, A. Malis. July 1993. (Obsoletes RFC1294) (Obsoleted by RFC2427) (Status: DRAFT STANDARD)
- RFC 2427: ***Multiprotocol Interconnect over Frame Relay.*** C. Brown, A. Malis. September 1998. Obsoletes RFC1490, RFC1294) (Also STD0055) (Status: STANDARD)

Sobre PPP:

- RFC 1331: ***The Point-to-Point Protocol (PPP) for the Transmission of Multi-protocol Datagrams over Point-to-Point Links.*** W. Simpson. May 1992. (Obsoleted by RFC1548) (Status: PROPOSED STANDARD)
- RFC 1548: ***The Point-to-Point Protocol (PPP)***. W. Simpson. December 1993. (Obsoletes RFC1331) (Obsoleted by RFC1661) (Updated by RFC1570) (Status: DRAFT STANDARD)
- RFC 1661: ***The Point-to-Point Protocol (PPP).*** W. Simpson, Ed.. July 1994. (Obsoletes RFC1548) (Updated by RFC 2153) (Also STD0051) (Status: STANDARD)
- RFC 2153: ***PPP Vendor Extensions***. W. Simpson. May 1997. (Updates RFC1661, RFC1962) (Status: INFORMATIONAL)

Sobre autenticaciones en PPP:

- RFC 1334: ***PPP Authentication Protocols***. B. Lloyd, W. Simpson. October 1992. (Obsoleted by RFC1994) (Status: PROPOSED STANDARD)
- RFC 1994: ***PPP Challenge Handshake Authentication Protocol (CHAP).*** W. Simpson. August 1996. (Obsoletes RFC1334) (Updated by RFC2484) (Status: DRAFT STANDARD)
- RFC 2484: ***PPP LCP Internationalization Configuration Option.*** G. Zorn. January 1999. (Updates RFC2284, RFC1994, RFC1570) (Status: PROPOSED STANDARD)

- NORMAS IEEE 802

- IEEE 802.1Q-1998, Virtual Bridged Local Area Networks
- IEEE 802.3-1985, Estándar Original a 10 Mb/s
- IEEE 802.3-2000, Método de Acceso CSMA/CD para múltiples especificaciones del nivel físico

- NORMA EIA/TIA 568 de cableado estructurado

Unidad 3

Direccionamiento IP

Administración del Tráfico

Objetivos

- Comprender el esquema de direccionamiento IP
- Comprender la división de redes en clases
- Comprender la utilización por parte del Router de la máscara de red / subred
- Entender la división en subredes
- Describir los protocolos del nivel de Interred (ICMP, ARP, etc)
- Vislumbrar la necesidad de ampliación de las direcciones IP y el nacimiento de IP versión 6
- Definir y explicar los conceptos de enrutamiento o encaminamiento.
- Definir y explicar los distintos algoritmos de enrutamiento o encaminamiento.
- Definir qué es la congestión y por qué se produce.
- Introducir los principios generales de la congestión.
- Definir y explicar los distintos algoritmos implementados para el control de congestión.

3.1. Protocolo IP (Protocolo Internet)

El protocolo de capa de red IP, es el principal protocolo utilizado hoy en día por Internet. Su trabajo es proporcionar un medio de mejor esfuerzo para el transporte de datagramas del origen al destino, sin importar si estas máquinas están en la misma red, o si hay otras redes entre ellas. El esquema de direccionamiento jerárquico que lo caracteriza, brinda la posibilidad de encaminar los paquetes a través de distintas redes y subredes.

Nota: *El protocolo IP está definido en las RFC 791,*

Un paquete o **datagrama IP** consiste en una parte de **cabecera** y una parte de **texto**. La cabecera tiene una parte fija de 20 bytes y una parte opcional de longitud variable. (Ver **figura 3.1**) El campo de **versión** lleva el registro de la versión del protocolo al que pertenece el datagrama. Al incluir la versión en cada datagrama es posible hacer que la transición entre versiones se lleve meses, o inclusive años, ejecutando en algunas máquinas la versión vieja y en otras la nueva.

Dado que la longitud de la cabecera no es constante, se incluye un campo, **IHL**, para indicar la longitud en palabras de 32 bits. El valor mínimo es de 5, cifra que se aplica cuando no hay opciones. El valor máximo es de 4 bits de 15, lo que limita la cabecera a 60 bytes y, por tanto, el campo de **opciones** a 40 bytes.

El campo **tipo de servicio** permite al *host* indicar a la subred el tipo de servicio que quiere. Son posibles varias combinaciones de confiabilidad y velocidad. Para voz digitalizada, la entrega rápida le gana a la entrega precisa. Para la transferencia de archivos, es más importante la transmisión libre de errores que la transmisión rápida. El campo mismo contiene (de izquierda a derecha) un campo de **precedencia**; tres indicadores, **D**, **T** y **R**; y dos bits no usados. El campo de precedencia es una prioridad, de 0 (normal) a 7 (paquete de control de red). Los tres bits indicadores permiten al *host* especificar lo que le interesa más del grupo {retardo (delay), rendimiento (throughput), confiabilidad (reliability)}. En la práctica, los enrutadores actuales, ignoran por completo el campo de tipo de servicio.

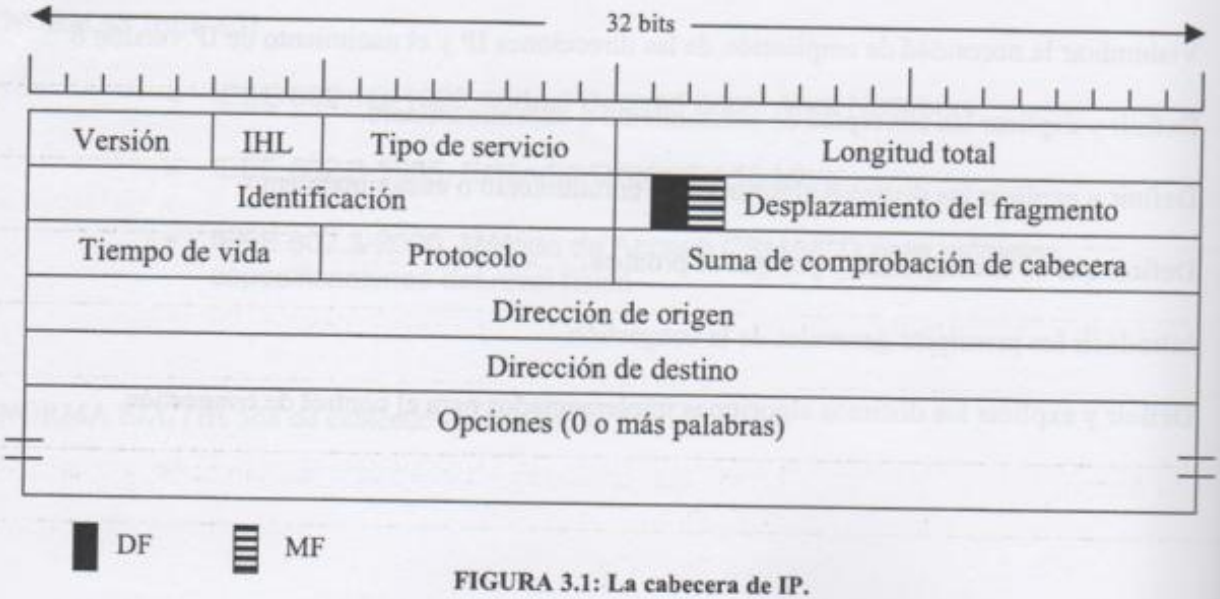


FIGURA 3.1: La cabecera de IP.

La **longitud total** incluye todo el datagrama: tanto la cabecera como los datos. La longitud máxima es de 65,535 bytes.

El **campo de identificación** es necesario para que el *host* de destino determine a qué datagrama pertenece un fragmento recién llegado. Todos los fragmentos de un datagrama contienen el mismo valor de identificación.

A continuación se viene un bit sin uso y luego dos campos de 1 bit. **DF** significa no fragmentar. **MF** significa más fragmentos. Todos los fragmentos excepto el último tienen establecido este bit, que es necesario para saber cuando han llegado todos los fragmentos de un datagrama.

El **desplazamiento del fragmento** indica en qué parte del datagrama actual va este fragmento. Todos los fragmentos excepto el último deben tener un múltiplo de 8 bytes, que es la unidad de fragmento elemental.

El campo tiempo de vida es un contador que sirve para limitar la vida de un paquete. En la práctica, simplemente cuenta los saltos. Cuando el contador llega a cero, el paquete se descarta y se envía de regreso un paquete de aviso al *host* de origen. Esta característica evita que los datagramas vaguen eternamente.

El campo **protocolo** indica la capa de transporte a la que debe entregarse. TCP es una posibilidad, pero también está UDP y algunos más.

La **suma de comprobación** de la cabecera verifica solamente la cabecera. Es útil para la detección de errores generados por palabras de memoria erróneas en un enrutador.

La **dirección de origen** y la **dirección de destino** indican el número de red y el número de *host*. Limitación de dirección de IP: la dirección se refiere a la conexión de la red, no al computador.
El campo de **opciones** se diseñó para proporcionar un recurso que permitiera que las versiones subsiguientes del protocolo incluyeran información no presente en el diseño original, para permitir a los experimentadores probar ideas nuevas y para evitar la asignación de bits de cabecera a información pocas veces necesaria. Las opciones son de longitud variable. (Ver **figura 3.2**)

Opción	Descripción
Seguridad.	Especifica qué tan secreto es el datagrama.
Enrutamiento estricto desde el origen.	Indica la trayectoria completa a seguir.
Enrutamiento libre desde el origen.	Da una lista de los enrutadores que no deben evitarse.
Registrar ruta.	Hace que cada enrutador agregue su dirección de IP.
Marca de tiempo.	Hace que cada enrutador agregue su dirección y marca de tiempo.

FIGURA 3.2: Opciones del IP.

3.1.1. Direcciones IP (versión 4)

Cada *host* y enrutador de Internet tiene una **dirección de IP**, que codifica su número de red y su número de *host*. La combinación es única: no hay dos máquinas que tengan la misma dirección de IP. Todas las direcciones son de 32 bits de longitud y se usan en los campos de dirección de origen y de destino de los paquetes de IP. Los formatos usados para las direcciones IP se muestran en la **figura 3.3**. Aquellas máquinas conectadas a varias redes tienen direcciones de IP diferentes en cada red.

Nota: *El procedimiento de división en subredes está descrito en RFC 950*

Existen cinco clases de redes: A, B, C, D y E

Los distintos formatos (clase A, B, C) obedecen a la necesidad de contar con redes de distinta jerarquía en cuanto a la cantidad de estaciones de trabajo que dichas redes pueden direccionar.

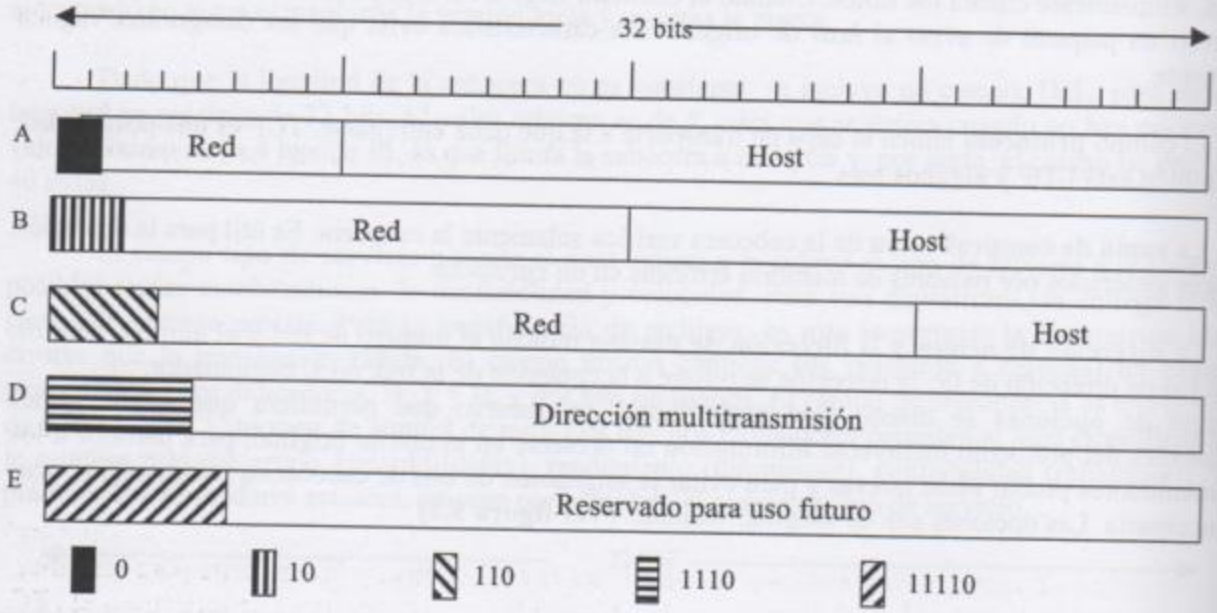


FIGURA 3.3: Formatos de Dirección IP.

Las direcciones de red, que son números de 32 bits, generalmente se escriben en **notación decimal con puntos**. En este formato cada uno de los 4 bytes se escribe en decimal.

- Las direcciones de Clase A usan 7 bits para el número de red dando un total de 126 (128-2) posibles redes de este tipo, ya que la dirección 0.0.0.0 se utiliza para reconocer la dirección de red propia y la dirección 127 es la del lazo interno de la máquina (*LOOPBACK*). Los restantes 24 bits son para el número de host – quitando las que son todos los bits a 0 (ya que corresponde a la dirección de la red) ó a 1 (ya que es la dirección de broadcast) – con lo cual tenemos hasta $2^{24} - 2 = 16.777.216 - 2 = 16.777.214$ direcciones. Son las redes 1.0.0.0 a 126.0.0.0

- Las direcciones de Clase B utilizan 14 bits para la dirección de red ($2^{14} = 16.382$ posibles redes de este tipo) y 16 bits para el host ($2^{16} - 2 = 65.534$ máquinas). Son las redes 128.0.0.0 a 191.255.0.0

- Las direcciones de clase C tienen 21 bits para la red (2.097.150 redes) y 8 bits para el host (254 máquinas). Son las redes 192.0.0.0 a 223.255.255.0
- Las direcciones de clase D están reservadas para multicasting; son usadas por direcciones de host en áreas limitadas.
- Las direcciones de Clase E están reservadas para uso futuro.

La clase que se elija para una red dada dependerá del número de máquinas que tenga y las que se prevean en el futuro. Como vimos antes el número de red es asignado por el NIC o por el organismo de cada país en quien él delegue. El número de host lo asignará el administrador que controla la red.

La dirección IP 0.0.0.0 es usada por los *hosts* cuando están siendo arrancados, pero no se usa después. Las direcciones de IP con 0 como número de red se refieren a la red actual. Estas direcciones permiten que las máquinas se refieran a su propia red sin saber su número (pero tienen que saber su clase para saber cuántos 0 hay que incluir). La dirección que consiste solamente en unos permite la difusión en la red local, por lo común una LAN. Las direcciones con un número de red propio y solamente unos en el campo de *host* permiten que las máquinas envíen paquetes de difusión a LAN distantes desde cualquier parte de Internet. Por último, todas las direcciones de la forma 127.xx.yy.zz se reservan para pruebas de realimentación. Los paquetes enviados a esa dirección no se colocan en el cable; se procesan localmente y se tratan como paquetes de entrada. Esto permite que los paquetes se envíen a la red local sin que el transmisor conozca su número. Esta característica también se usa para la detección de fallas en *software* de la red.

La autoridad de direcciones en IP es IANA[37].

3.1.1.1. Redes y Subredes. Máscaras de subred

Puede darse el caso de que una red crezca en un número de máquinas significativo o que se quiera instalar una nueva red además de la que ya existía.

Para conseguir mayor funcionalidad podemos dividir nuestra red en subredes (*subnetting*) dividiendo en dos partes el número de host, una para identificar la subred, y la otra parte para identificar la máquina (el host). Esto lo decidirá el responsable de la red (administrador) sin que intervenga el NIC. Podemos tener asignada una red –normalmente de las clases B ó C– y dividirla en dos o más subredes según nuestras necesidades comunicados por routers.

El conjunto formado por la subred y el número de host se conoce como dirección local o parte local. Un host remoto verá la dirección local como el número de host.

El número de bits correspondientes a la subred y al número de host son elegidos libremente por el administrador.

Esta división se realiza utilizando una ***máscara de subred***. Esta es un número binario de 32 bits. Los bits que estén a "1" indicarán el campo de la dirección IP dedicada a la red / subred, y los bits puestos a "0" indicarán la parte dedicada al host.

[37] En Inglés: Internet Assigned Number Authority.

La máscara de subred se representa normalmente en notación decimal.

Por ejemplo si no utilizamos subredes y dejamos la red como una sola, para una red clase B la máscara será:

11111111	11111111	00000000	00000000
255	255	0	0

Si queremos dividirla en subredes tomaremos los 16 bits de la parte local y pondremos a "1" la parte que queremos represente a las subredes. Por ejemplo si queremos 8 subredes necesitaremos en binario 3 bits para referenciarlas. La máscara que necesitamos será:

11111111.11111111.11100000.00000000

Es decir:

255.255.224.0

Al emplear 13 bits para el host podríamos tener hasta 2^{13}-2 = 8190 máquinas en cada subred.

Lo normal a la hora de añadir "unos" a la máscara inicial para definir las subredes es hacerlo de manera contigua para ver los campos claramente.

Si tenemos una red clase C cuya máscara sin subredes es 255.255.255.0 y queremos dividirla en 4 subredes solo necesitamos 2 bits para definirlas:

11111111	11111111	11111111	11000000
255	255	255	192

Esta máscara permitiría hasta 2^{6}- 2 = 62 hosts en cada subred.

3.1.1.2. FORMAS DE DIVISIÓN EN SUBREDES

Hay dos formas de dividir una red en subredes: longitud estática y longitud variable. Se pueden utilizar según el protocolo de encaminamiento. El encaminamiento IP nativo solo soporta longitud estática al emplear el protocolo RIP. Con el protocolo RIP2 se consigue utilizar longitud variable.

La subdivisión en longitud estática implica que todas las subredes deben tener la misma máscara lo que obligará a poner la que necesite la que tenga más ordenadores.

La subdivisión en longitud variable permite que no haya que variar las direcciones de red caso de cambios en una de sus subredes. Una subred que necesita dividirse en otras dos puede hacerlo a añadiendo un bit a su máscara sin afectar al resto. No todos los routers y host soportan la longitud variable de máscaras. Si un host no soporta este método deberá encaminarse hacia un router que si lo soporte.

Ejemplos de Subnetting estática

1) Supongamos que tenemos una red clase B,

140.155.0.0

Podemos dividir la dirección local con 8 bits para las subredes y otros 8 para el número de hosts. Sabemos que tendremos **256** subredes con **254** hosts cada una.

La máscara sería del tipo,

255.255.255.0

Es decir que en binario sería

11111111.11111111.11111111.00000000

2) Si tenemos una red clase C,

200.135.15.0

Podemos dividirla con una máscara de 3 bits, en 8 subredes ($2^3 = 8$), con lo cual la máscara sería:

255.255.255.224

En binario sería

11111111.11111111.11111111.11100000

Es decir que hemos dividido la porción local de la dirección en 3 bits para subredes y 5 bists para hosts. O sea $2^3 = 8$ subredes y $2^5 - 2 = 30$ hosts.

Las subredes serían:

$\mathbf{00}000000_{)2} = 0_{)10}$
$\mathbf{00}100000_{)2} = 32_{)10}$
$\mathbf{01}000000_{)2} = 64_{)10}$
$\mathbf{01}100000_{)2} = 96_{)10}$
$\mathbf{10}000000_{)2} = 128_{)10}$
$\mathbf{10}100000_{)2} = 160_{)10}$
$\mathbf{11}000000_{)2} = 192_{)10}$
$\mathbf{11}100000_{)2} = 224_{)10}$

3) Otro ejemplo:

Si nuestra red clase C es 193.144.238 y tomamos la máscara 255.255.255.224 anterior:

SUBRED	NÚMEROS DE HOST PARA CADA SUBRED
193.144.238.0	193.144.238.1 a 193.144.238.30
193.144.238.32	193.144.238.33 a 193.144.238.62
193.144.238.64	193.144.238.65 a 193.144.238.94
193.144.238.96	193.144.238.97 a 193.144.238.126
193.144.238.128	193.144.238.129 a 193.144.238.158
193.144.238.160	193.144.238.161 a 193.144.238.190
193.144.238.192	193.144.238.193 a 193.144.238.222
193.144.238.224	193.144.238.225 a 193.144.238.254

4) Si en cambio tomamos cuatro dígitos para subred, la máscara será: 255.255.255.240

Por ejemplo tomemos la red **192.168.250.0** con una máscara de 4 dígitos binarios:

Esto proveerá de 16 subredes cada una con 14 host
Rango de host de cada subred:

0 192.168.250.1 - 192.168.250.14
1 192.168.250.17 - 192.168.250.30
2 192.168.250.33 - 192.168.250.46
3 192.168.250.49 - 192.168.250.62
4 192.168.250.65 - 192.168.250.78
5 192.168.250.81 - 192.168.250.94
6 192.168.250.97 - 192.168.250.110
7 192.168.250.113 - 192.168.250.126
8 192.168.250.129 - 192.168.250.142
9 192.168.250.145 - 192.168.250.158
10 192.168.250.161 - 192.168.250.174
11 192.168.250.177 - 192.168.250.190
12 192.168.250.193 - 192.168.250.206
13 192.168.250.209 - 192.168.250.222
14 192.168.250.225 - 192.168.250.238
15 192.168.250.241 - 192.168.250.254

Si para la misma red tomamos 5 dígitos binarios para formar subredes, esto proveerá de 32 subnets cada una con 6 direcciones de host.

Rango de host de cada subred

0 192.168.250.1 - 192.168.250.6
1 192.168.250.9 - 192.168.250.14
2 192.168.250.17 - 192.168.250.22
3 192.168.250.25 - 192.168.250.30
4 192.168.250.33 - 192.168.250.38
5 192.168.250.41 - 192.168.250.46
6 192.168.250.49 - 192.168.250.54
7 192.168.250.57 - 192.168.250.62
8 192.168.250.65 - 192.168.250.70
9 192.168.250.73 - 192.168.250.78
10 192.168.250.81 - 192.168.250.86
11 192.168.250.89 - 192.168.250.94
12 192.168.250.97 - 192.168.250.102
13 192.168.250.105 - 192.168.250.110
14 192.168.250.113 - 192.168.250.118
15 192.168.250.121 - 192.168.250.126
16 192.168.250.129 - 192.168.250.134
17 192.168.250.137 - 192.168.250.142
18 192.168.250.145 - 192.168.250.150
19 192.168.250.153 - 192.168.250.158
20 192.168.250.161 - 192.168.250.166
21 192.168.250.169 - 192.168.250.174
22 192.168.250.177 - 192.168.250.182
23 192.168.250.185 - 192.168.250.190
24 192.168.250.193 - 192.168.250.198
25 192.168.250.201 - 192.168.250.206
26 192.168.250.209 - 192.168.250.214
27 192.168.250.217 - 192.168.250.222
28 192.168.250.225 - 192.168.250.230
29 192.168.250.233 - 192.168.250.238
30 192.168.250.241 - 192.168.250.246
31 192.168.250.249 - 192.168.250.254

Direcciones Broadcast

Hay diferentes tipos de broadcast:

- Direcciones de broadcast limitadas: La dirección con todos los bits a "1" –255.255.255.255– se usa en redes que soportan broadcasting, e indica todos los host de la subred. Los routers no reenvían la información fuera de la subred.
- Direcciones de broadcast de red: En una red sin subredes poniendo a "1" los bits del campo de número de host
- Direcciones de broadcast de subred: Poniendo a "1" solo la parte del número de host de la dirección local.
- Broadcast a todas las subredes: Poniendo toda la parte local a "1".

Multicasting

Para tener más flexibilidad que la proporcionada por el método broadcast que se dirige a todos los miembros de una subred o de una red, existe el método multicast, el cual nos permite dirigirnos a grupos de hosts dentro de la red.

El datagrama IP para multicast como vimos antes es de clase D cuyos cuatro primeros bits son 1110 –el primer octeto va de 11100000 a 11101111– luego el rango de direcciones será de 224.0.0.0 a 239.255.255.255.

Existen dos tipos de grupos:

Grupos permanentes: Son los que han sido estandarizados. Los hosts asignados a estos grupos no son permanentes, pueden afiliarse a él o ser quitados de él.

Grupos importantes de este tipo son:

224.0.0.0	Dirección reservada de base
224.0.0.1	Todos los sistemas de la subred
224.0.0.2	Todos los routers de la subred
224.0.0.5	Todos los routers OSPF
224.0.0.6	Todos los routers OSPF designados

Grupos transitorios: Son los grupos que no son permanentes y se van creando según las necesidades.

3.1.1.3. DIRECCIONES IP PRIVADAS

Las redes privadas de organizaciones que no están directamente conectadas a Internet –esto es, las redes que se conectan por medio de un proxy o un router a una única línea con una sola dirección IP dada por un proveedor de servicios– tienen asignado unos rangos de direcciones IP para su funcionamiento interno. Estos son:

Para clase A una única dirección de red: 10.0.0.0
Para clase B 16 redes del rango 172.16.0.0 a 172.31.0.0
Para clase C 256 direcciones de red: 192.168.0.0 a 192.168.255.0

Estas direcciones IP no son utilizadas por los routers para su comunicación con Internet, y se utilizan solo dentro de la organización. Estas redes (Intranet) tienen la ventaja de ser mucho menos accesibles a ataques desde el exterior. Para el caso de que algunos de los host de dicha red, quisieran acceder a Internet, el router debe convertirle su dirección IP privada a una dirección IP pública (mediante la ejecución del protocolo NAT explicado en 3.1.8).

3.1.2. Protocolo de configuración dinámica de host (DHCP)

DHCP (*Dynamic Host Configuration Protocol*) son las siglas que identifican a un protocolo empleado para que los *hosts* (clientes) en una red puedan obtener su configuración de forma dinámica a través de un servidor del protocolo. Los datos así obtenidos pueden ser: la dirección IP, la máscara de red, la dirección de *broadcast*, las características del DNS, entre otros. El servicio DHCP permite acelerar y facilitar la configuración de muchos *hosts* en una red evitando en gran medida los posibles errores humanos.

Nota: *El protocolo DHCP está definido en las RFC 1541, 1533, 2131*

Con una función similar a la del DHCP, pero con algunas restricciones, existe el BOOTP o *Internet Bootstrap Protocol*, el cual permite también la asignación de la configuración de red en forma dinámica pero a partir de su definición estática para cada cliente en una base de datos en el servidor. Esta información a diferencia de como se hace usualmente con DHCP no puede ser renovada.

Básicamente el servicio DHCP/BOOTP funciona de la siguiente forma. Existe un programa servidor en un *host* de la red que escucha las solicitudes de los clientes y que en su configuración almacena tablas de posibles direcciones IP a otorgar además del resto de la información.

Procedimiento DHCP

Cuando un cliente requiere del servicio envía una solicitud en forma de *broadcast* a través de la red. Todos los servidores alcanzados por la solicitud responden al cliente con sus respectivas propuestas, este acepta una de ellas haciéndoselo saber al servidor elegido, el cual le otorga la información requerida

Esta información se mantiene asociada al cliente mientras este no desactive su interfaz de red (posiblemente porque se apague la máquina) o no expire el plazo del ``contrato" (*lease time*). El plazo del ``contrato" o renta es el tiempo en que un cliente DHCP mantiene como propios los datos que le otorgó un servidor. Este se negocia como parte del protocolo entre el cliente y el servidor. Una vez vencido el plazo del contrato el servidor puede renovar la información del cliente, fundamentalmente su dirección IP, y asignarle otra nueva o extender el plazo, manteniendo la misma información. El cliente puede solicitar también la renovación o liberación de sus datos.

A continuación se listan los principales mensajes que se intercambian como parte del protocolo DHCP y para que se emplea cada uno:

1. `DHCPDISCOVER` - mensaje de *broadcast* de un cliente para detectar los servidores.
2. `DHCPOFFER` - mensaje de un servidor hacia un cliente con una oferta de configuración.
3. `DHCPREQUEST` - mensaje de un cliente a un servidor para:
   a) aceptar la oferta de un servidor determinado y por ende rechazar las otras
   b) confirmar la exactitud de la información asignada antes del reinicio del sistema
   c) extender el contrato de una dirección IP determinada
4. `DHCPPACK` - mensaje del servidor hacia un cliente para enviarle la configuración asignada excluyendo la dirección IP que ya fue aceptada.

5. DHCPNAK - mensaje del servidor al cliente para indicar que la dirección que tiene asignada es incorrecta (por ejemplo, cuando el cliente cambia de subred) o que el contrato ha expirado.
6. DHCPDECLINE - mensaje del cliente para el servidor indicando que aún está usando una dirección determinada.
7. DHCPRELEASE - mensaje del cliente para el servidor para indicar que renuncia a la dirección otorgada y cancela lo que queda del contrato establecido anteriormente.
8. DHCPINFORM - mensaje del cliente para el servidor para pedir sus parámetros de configuración excluyendo la dirección IP que ya tiene asignada.

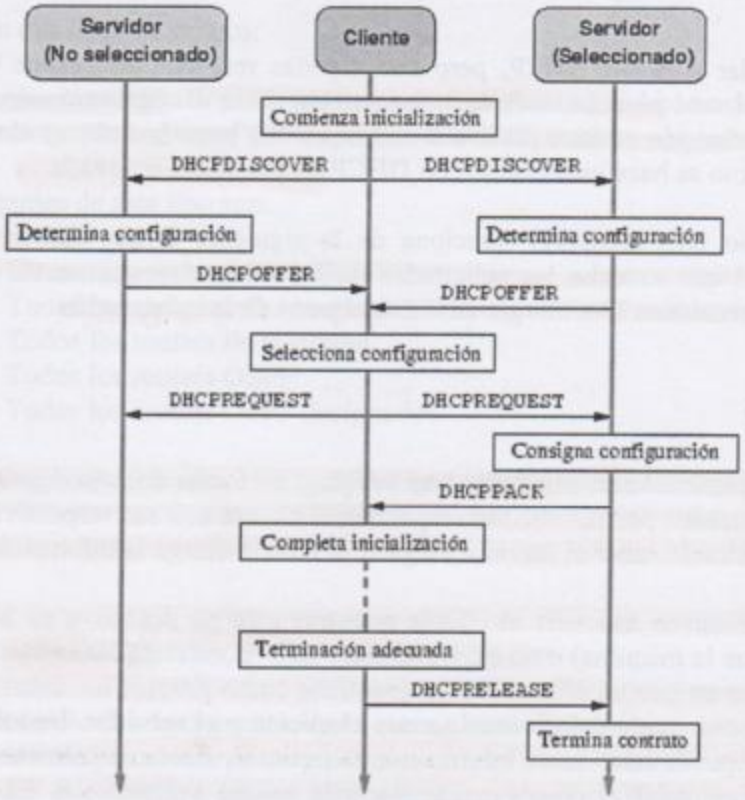


Figura: Representación simplificada del protocolo DHCP

Un servidor de DHCP puede identificar a cada cliente a través de dos formas fundamentales:

1. La dirección MAC (*Media Access Control*) de la tarjeta de red del cliente.
2. Un identificador que le indique el cliente.

Aunque la idea central del servicio DHCP es la dinamicidad de las direcciones IP asignadas no se excluye la posibilidad de utilizar direcciones fijas para algunos *hosts* que por sus características lo requieran, ejemplo de ello son las máquinas proveedoras de disímiles servicios como el correo electrónico o el DNS. Este tipo de *host* utilizaría las ventajas del servicio para obtener el resto de los datos que se pueden proveer mediante DHCP.

3.1.3. IPV6

En 1990 se comenzó a trabajar en una versión nueva del IP, una que nunca se quedaría sin direcciones, resolvería varios otros problemas y sería más flexible y eficiente también.

***Nota**: El protocolo IP v6 corresponde a la RFC 1752 y 1884*

Sus metas principales eran:

- Manejar miles de millones de *hosts*, aun con asignación de espacio de direcciones ineficiente.
- Reducir el tamaño de las tablas de enrutamiento.
- Simplificar el protocolo, para permitir a los enrutadores el procesamiento más rápido de los paquetes.
- Proporcionar mayor seguridad (verificación de autenticidad y confidencialidad) que el IP actual.
- Prestar mayor atención al tipo de servicio, especialmente con datos en tiempo real.
- Ayudar a la multitransmisión permitiendo la especificación de alcances.
- Posibilitar que un *host* sea móvil sin cambiar su dirección.
- Permitir que el protocolo evolucione.
- Permitir que el protocolo viejo y el nuevo coexistan por años.

El resultado fue el desarrollo de un protocolo llamado **SIPP (Protocolo Simple de Internet Mejorado)** al cual se le dio la designación **IPv6**. En general, IPv6 no es compatible con IPv4, pero es compatible con todos los demás protocolos Internet, incluidos TCP, UDP y otros, a veces requiriendo pequeñas modificaciones (principalmente para manejar direcciones más grandes).

Sus características principales son:

- Tiene direcciones más grandes que el IPv4; son de 16 bytes de longitud, lo que resuelve el problema que se buscaba resolver: proporcionar una cantidad prácticamente ilimitada de direcciones IP.
- Simplificación de la cabecera, que contiene sólo 7 campos (contra 13 en el IP). Este cambio permite a los enrutadores procesar con mayor rapidez los paquetes y mejorar, por tanto, el rendimiento.
- Mejor apoyo de las opciones. Este cambio fue esencial con la nueva cabecera, pues campos que antes eran obligatorios ahora son opcionales. Además es diferente la manera de representar las opciones.

- Las verificaciones de autenticidad y la confidencialidad son características clave del IP nuevo.
- Por último, se tenía que prestar mayor atención al tipo de servicio que en el pasado. El IPv4 de hecho tiene un campo de 8 bits dedicado a este asunto, pero con el crecimiento esperado del tráfico multimedia en el futuro, se requiere mucho más.

3.1.2.1. Cabecera principal del IPv6

El campo de **versión** siempre es de 6 para el IPv6 (y de 4 para el IPv4).

El campo de **prioridad** se usa para distinguir entre paquetes a aquellos que se les puede controlar el flujo y aquellos que no. Los valores 0 a 7 son para transmisiones capaces de reducir su velocidad en caso de congestionamiento. Los valores de 8 a 15 son para tráfico de tiempo real cuya tasa de envío es constante, aun si todos los paquetes se están perdiendo. El audio y video caen en esta última categoría.

El campo de **etiqueta de flujo** aun es experimental, pero se usará para permitir a un origen y a un destino establecer una seudoconexión con propiedades y requisitos particulares.

El campo de **longitud de carga útil** indica cuántos bytes siguen a la cabecera de 40 bytes. El nombre de campo se cambió de **longitud total** en el IPv4 porque el significado cambió ligeramente: los 40 bytes de cabecera ya no se cuentan como parte de la longitud, como antes.

El campo **siguiente cabecera** revela el secreto. La razón por la que pudo simplificarse la cabecera es que puede haber cabeceras adicionales (opcionales) de extensión. Este campo indica cuál de las seis cabeceras de extensión (actualmente), de haberlas, sigue a ésta. Si esta cabecera es la última cabecera de IP, el campo de **siguiente cabecera** indica el manejador de protocolo de transporte (por ejemplo TCP, UDP) al que se entregará el paquete.

El campo **límite de saltos** se usa para evitar que los paquetes vivan eternamente. En la práctica es igual al campo de tiempo de vida de IPv4, es decir, un campo que se disminuye en cada salto.

Luego vienen los campos de **dirección de origen** y **destino**. Se tiene una dirección de 16 bytes de longitud fija.

Además de manejar direcciones unitransmisión estándar (punto a punto) y multitransmisión, el IPv6 también maneja un nuevo tipo de direccionamiento: **transmisión a cualquiera**. Ésta es como la multitransmisión, en el sentido de que el destino es un grupo de direcciones, pero en lugar de tratar de entregar el paquete a todos, intenta entregarlo a uno solo, generalmente el más cercano.

Por ejemplo, al ponerse en contacto con un grupo de servidores de archivos cooperativos, un cliente puede usar la transmisión a cualquiera para llegar al más cercano, sin tener que saber quién es. La transmisión a cualquiera usa direcciones normales de unitransmisión. Es responsabilidad del sistema de enrutamiento escoger al afortunado *host* que recibirá el paquete.

Si comparamos la cabecera del IPv4 con la del IPv6, podemos decir que el campo **IHL** se fue porque la cabecera de IPv6 tiene una longitud fija. El campo de **protocolo** se retiró porque el campo de siguiente cabecera indica lo que le sigue a la última cabecera de IP.

Se retiraron todos los campos relacionados con la fragmentación, puesto que el IPv6 tiene un enfoque distinto hacia la fragmentación. Por último, el campo de **suma de comprobación** desaparece, porque su cálculo reduce en gran medida el desempeño.

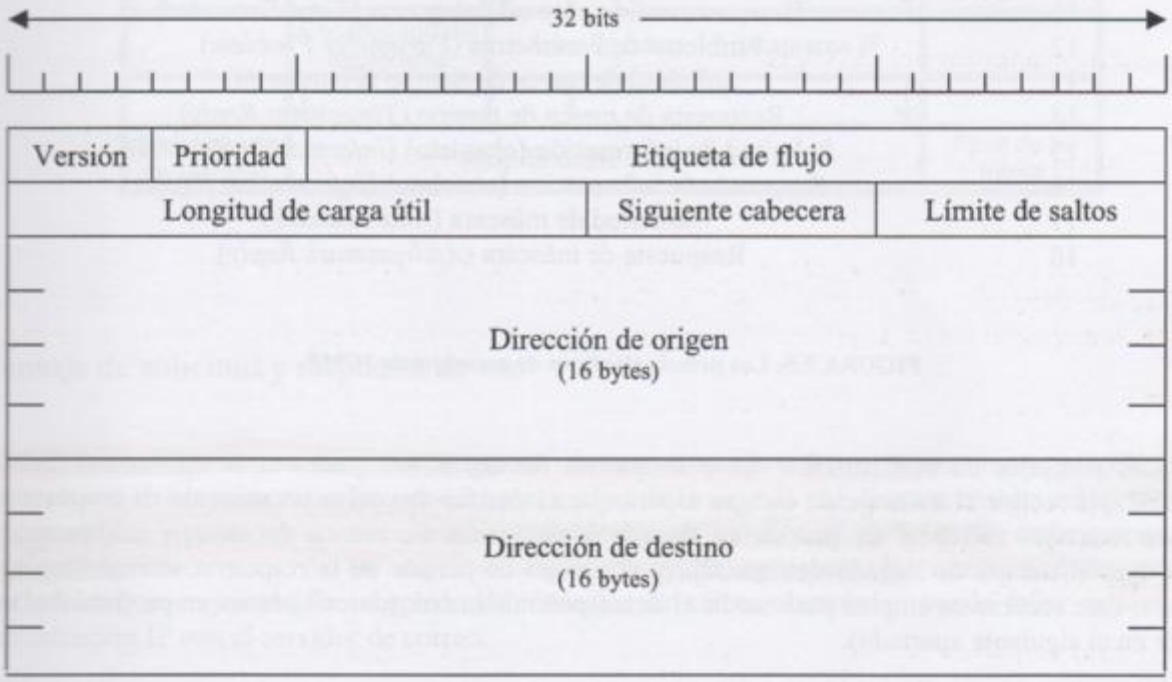


FIGURA 3.4. Cabecera fija del IPv6 (obligatoria).

3.1.4. Protocolo ICMP (Protocolo de Control de Mensajes de Internet)

Debido a que el protocolo IP no es fiable, los datagramas pueden perderse o llegar defectuosos a su destino. El protocolo ICMP (*Internet Control Message Protocol*, protocolo de mensajes de control y error) se encarga de informar al origen si se ha producido algún error durante la entrega de su mensaje. Pero no sólo se encarga de notificar los errores, sino que también transporta distintos mensajes de control.

Nota: *El protocolo ICMP está definido en la RFC 792*

El protocolo ICMP únicamente informa de incidencias en la red pero no toma ninguna decisión. Esto será responsabilidad de las capas superiores. Debido a que el protocolo IP no es fiable puede darse el caso de que un mensaje ICMP se pierda o se dañe. Si esto llega a ocurrir no se creará un nuevo mensaje ICMP sino que el primero se descartará sin más.

Los mensajes más importantes se listan a continuación (Ver **figura 3.5**). Los mensajes ICMP comienzan con un campo de 8 bits que contiene el tipo de mensaje, según se muestra en la tabla siguiente. El resto de campos son distintos para cada tipo de mensaje ICMP.

Campo de tipo	Tipo de mensaje ICMP
0	Respuesta de eco (*Echo Reply*)
3	Destino inaccesible (*Destination Unreachable*)
4	Disminución del tráfico desde el origen (*Source Quench*)
5	Redireccionar (cambio de ruta) (*Redirect*)
8	Solicitud de eco (*Echo*)
11	Tiempo excedido para un datagrama (*Time Exceeded*)
12	Problema de Parámetros (*Parameter Problem*)
13	Solicitud de marca de tiempo (*Timestamp*)
14	Respuesta de marca de tiempo (*Timestamp Reply*)
15	Solicitud de información (obsoleto) (*Information Request*)
16	Respuesta de información (obsoleto) (*Information Reply*)
17	Solicitud de máscara (*Addressmask*)
18	Respuesta de máscara (*Addressmask Reply*)

FIGURA 3.5: Los principales tipos de mensajes de ICMP.

Los mensajes de **solicitud de eco** y **respuesta de eco** sirven para ver si un destino dado es alcanzable. Al recibir el mensaje de eco, se espera que el destino devuelva un mensaje de respuesta de eco. Los mensajes **solicitud de marca de tiempo** y **respuesta de marca de tiempo** son parecidos, excepto que el tiempo de llegada del mensaje y el tiempo de partida de la respuesta se registran en la respuesta. Este recurso se emplea para medir el desempeño de la red. (describiremos en profundidad este mensaje en el siguiente apartado).

El mensaje **destino inalcanzable** se usa cuando la subred o un enrutador no pueden ubicar el destino, o un paquete con el bit DF no puede entregarse porque está en el camino una red de paquete pequeño. El mensaje **tiempo excedido** se envía cuando un paquete se descarta debido a que su contador llega a cero. Este suceso es un síntoma de que los paquetes están en ciclo, de que hay un congestionamiento enorme, o de que los valores de temporización son demasiados bajos.

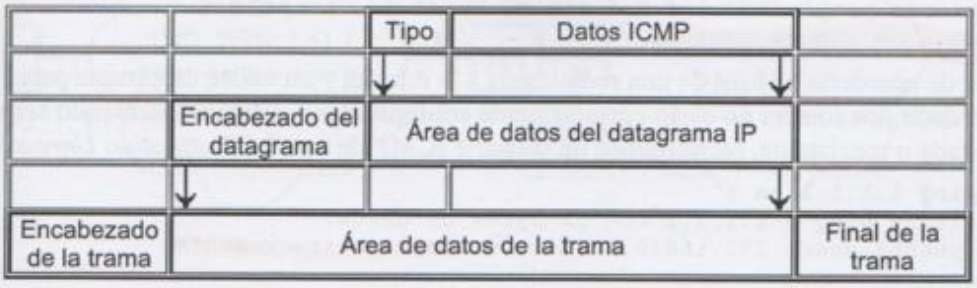
El mensaje de **tiempo de parámetro** indica que se ha detectado un valor ilegal en un campo de cabecera. El problema indica una falla en el *software* de IP del *host*, o probablemente en *software* de un enrutador transitado.

El mensaje **supresión de origen** se usaba antes para controlar a los *hosts* que enviaban demasiados paquetes. Al recibir un *host* este mensaje, se esperaba que se refrenaba.

El mensaje de **redireccionamiento** se usa cuando un enrutador se da cuenta de que un paquete parece estar mal enrutado. El enrutador lo usa para indicar al *host* transmisor el posible error.

Además de estos mensajes, hay cuatro más que tienen que ver con el direccionamiento de Internet, para permitir que los *hosts* descubran sus números de red y para manejar el caso de varias LAN que comparten una sola dirección IP.

Cada tipo de mensaje se encapsula en un paquete IP, como se puede apreciar en el siguiente esquema:



Mensaje de solicitud y respuesta de eco

Los mensajes de solicitud y respuesta de eco, tipos 8 y 0 respectivamente, se utilizan para comprobar si existe comunicación entre 2 hosts a nivel de la capa de red. Estos mensajes comprueban que las capas física (cableado), acceso al medio (tarjetas de red) y red (configuración IP) están correctas. Sin embargo, no dicen nada de las capas de transporte y de aplicación las cuales podrían estar mal configuradas; por ejemplo, la recepción de mensajes de correo electrónico puede fallar aunque exista comunicación IP con el servidor de correo.

La orden **PING** envía mensajes de solicitud de eco a un host remoto e informa de las respuestas.

Veamos su funcionamiento, en caso de no producirse incidencias en el camino.

A envía un mensaje ICMP de tipo 8 (*Echo*) a B
B recibe el mensaje y devuelve un mensaje ICMP de tipo 0 (*Echo Reply*) a A
A recibe el mensaje ICMP de B y muestra el resultado en pantalla

```
A>ping 172.20.9.7 -n 1
Haciendo ping a 172.20.9.7 con 32 bytes de datos:
Respuesta desde 172.20.9.7: bytes=32 tiempo<10ms TDV=128
```

En la orden anterior hemos utilizado el parámetro "-n 1" para que el host A únicamente envíe 1 mensaje de solicitud de eco. Si no se especifica este parámetro se enviarían 4 mensajes (y se recibirían 4 respuestas).

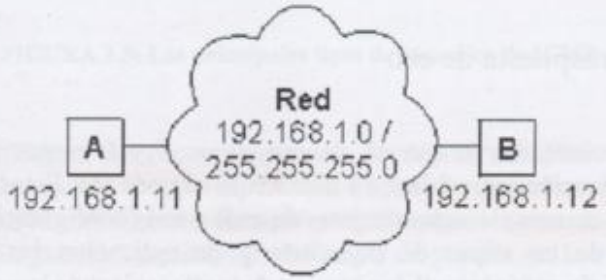
Si el host de destino no existiese o no estuviera correctamente configurado recibiríamos un mensaje ICMP de tipo 11 (*Time Exceeded*).

```
A>ping 192.168.0.6 -n 1
Haciendo ping a 192.168.0.6 con 32 bytes de datos:
Tiempo de espera agotado.
```

Si tratamos de acceder a un host de una red distinta a la nuestra y no existe un camino para llegar hasta él, es decir, los routers no están correctamente configurados o estamos intentando acceder a una red aislada o inexistente, recibiríamos un mensaje ICMP de tipo 3 (*Destination Unreachable*).

```
A>ping 1.1.1.1 -n 1
Haciendo ping a 1.1.1.1 con 32 bytes de datos:
Respuesta desde 192.168.0.1: Host de destino inaccesible.
```

Utilización de PING para diagnosticar errores en una red aislada



`A>ping 192.168.1.12`

- `Respuesta`. El cableado entre A y B, las tarjetas de red de A y B, y la configuración IP de A y B están correctos.
- `Tiempo de espera agotado`. Comprobar el host B y el cableado entre A y B.
- `Host de destino inaccesible`. Comprobar las direcciones IP y máscaras de subred de A y B porque no pertenecen a la misma red.
- `Error`. Probablemente estén mal instalados los protocolos TCP/IP del host A. Probar `A>ping 127.0.0.1` para asegurarse.

Nota: *El comando* ping 127.0.0.1 *informa de si están correctamente instalados los protocolos TCP/IP en nuestro host. No informa de si la tarjeta de red de nuestro host está correcta.*

Utilización de PING para diagnosticar errores en una red de redes

A continuación veremos un ejemplo para una red de redes formada por dos redes (1 solo router). La idea es la misma para un mayor número de redes y routers.

La orden **TRACERT** (**traceroute** en entornos Unix) hace una traza a un determinado host. TRACERT funciona enviando mensajes ICMP de solicitud de eco con distintos TTL; traceroute, en cambio, envía mensajes UDP. Si la comunicación extremo a extremo no es posible, la traza nos indicará en qué punto se ha producido la incidencia. Existen algunas utilidades en Internet, como Visual Route, que conocen la localización geográfica de los principales routers de Internet. Esto permite dibujar en un mapamundi el recorrido que siguen los datagramas hasta llegar a un host.

```
A>tracert 130.206.1.2

Traza a la dirección sun.rediris.es [130.206.1.2]
sobre un máximo de 30 saltos:

  1    1 ms    1 ms    1 ms  PROXY [192.168.0.1]
  2  122 ms  118 ms  128 ms  MADR-X27.red.retevision.es
[62.81.1.102]
  3  143 ms  232 ms  147 ms  MADR-R2.red.retevision.es [62.81.1.92]
  4  130 ms  124 ms  246 ms  MADR-R16.red.retevision.es [62.81.3.8]
  5  590 ms  589 ms  431 ms  MADR-R12.red.retevision.es
[62.81.4.101]
  6  612 ms  640 ms  124 ms  MADR-R10.red.retevision.es
[62.81.8.130]
  7  259 ms  242 ms  309 ms  193.149.1.28
  8  627 ms  752 ms  643 ms  213.0.251.42
  9  137 ms  117 ms  118 ms  213.0.251.142
 10  109 ms  105 ms  110 ms  A1-2-1.EB-Madrid00.red.rediris.es
[130.206.224.81]
 11  137 ms  119 ms  122 ms  A0-0-0-1.EB-Madrid3.red.rediris.es
[130.206.224.86]
 12  109 ms  135 ms  115 ms  sun.rediris.es [130.206.1.2]

Traza completa.
```

3.1.5. Protocolo de Resolución de Direcciones (ARP)

Aunque cada máquina de Internet tiene una o más direcciones IP, éstas no pueden usarse para enviar paquetes porque el *hardware* de la capa de enlace de datos no entiende las direcciones de Internet.

Hoy día, la mayoría de los *hosts* que están conectados a alguna LAN mediante una tarjeta de interfaz que sólo entiende direcciones de LAN. Por ejemplo, todas las tarjetas Ethernet que se han fabricado vienen equipadas con una dirección de Ethernet de 48 bits (dirección MAC). Los fabricantes de tarjetas Ethernet solicitan un bloque de direcciones de una autoridad central para asegurarse de que dos tarjetas no puedan tener la misma dirección (para evitar conflictos en caso de que las dos tarjetas aparezcan en la misma LAN).

Las tarjetas envían y reciben marcos con base en direcciones de Ethernet de 48 bits. No saben nada sobre las direcciones de IP de 32 bits.

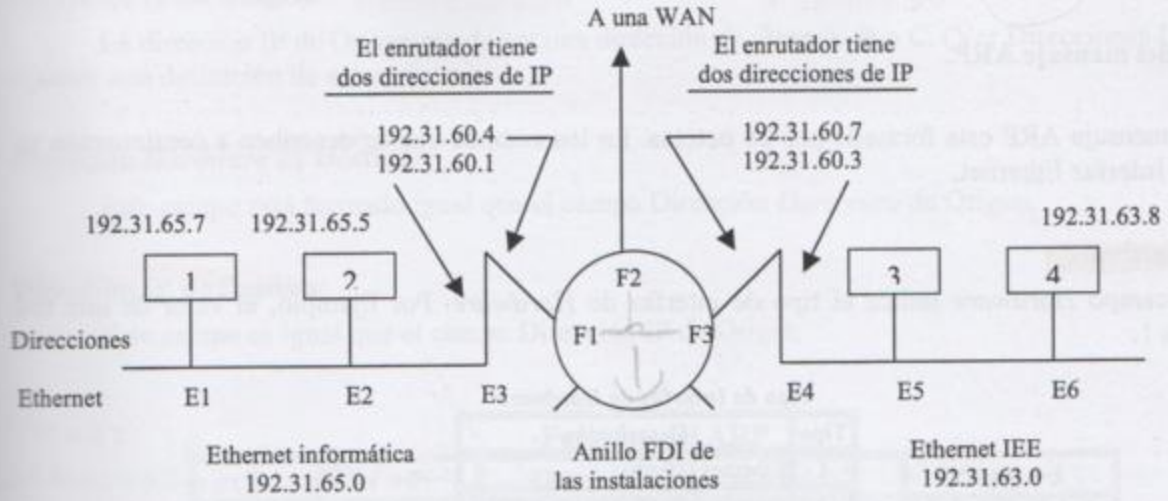


FIGURA 3.6: tres redes clase C interconectadas, dos Ethernets y un anillo FDDI.

TOMANDO Y REFERENCIANDO EL ENVIO DE PAQUETES

Para explicar el funcionamiento de cómo se proyectan las direcciones de IP en las direcciones de capa de enlace de datos, se utilizará el ejemplo de la **figura 3.6**, en la que se ilustra una universidad pequeña con varias redes clase C. Se tienen dos Ethernet, una en el Departamento de Informática, con una dirección IP de 192.31.65.0, y otra en el de Ingeniería Electrónica, con dirección de IP de 192.31.63.0. Éstas se conectan mediante un anillo FDI del campus con una dirección IP de 192.31.60.0. Cada máquina de un Ethernet tiene una dirección de Ethernet única, etiquetada E1 a E6, y cada máquina del anillo FDI, etiquetada F1 a F3.

Comencemos por ver la manera en que un usuario del *host 1* envía un paquete a un usuario del *host 2*. Supongamos que el transmisor sabe el nombre del receptor pretendido. El primer paso es encontrar la dirección IP del *host 2*. Esta búsqueda la lleva a cabo el **sistema de nombres de dominio (DNS)**. Éste devuelve la dirección IP del *host 2* (192.31.65.5).

El *software* de la capa superior del *host 1* construye un paquete con 192.31.65.5 en el campo de dirección de destino y lo entrega al *software* de IP para su transmisión. El *software* de IP puede ver la dirección y saber si el dominio está en su propia red, pero necesita una manera de encontrar algún lugar del sistema que proyecte las direcciones IP en las direcciones Ethernet. Esta solución ciertamente es posible pero, en organizaciones con miles de máquinas, el mantenimiento de estos archivos es una tarea susceptible a errores y con alto consumo de tiempo.

Una mejor solución es que el *host 1* envíe un paquete de difusión por el Ethernet preguntando "¿Quién es el dueño de la dirección IP 192.31.65.5?". La difusión llegará a cada máquina del Ethernet 192.31.65.0, y cada una revisará su propia dirección IP. Sólo el *host 2* responderá con su dirección Ethernet (E2). De esta manera el *host 1* aprende que la dirección IP 192.31.65.5 está en el *host* con la dirección Ethernet E2. El protocolo para preguntar esto y obtener la respuesta se llama **ARP (Protocolo de Resolución de Direcciones)**. Casi todas las máquinas de Internet lo ejecutan.

La ventaja del ARP sobre los archivos de configuración es la sencillez. El administrador del sistema no necesita hacer mucho, excepto asignar a cada máquina una dirección IP y decidir sobre las máscaras de subred. El ARP hace lo demás.

TOKEN RING SIMILAR } APRENDE.

MAC

Formato del mensaje ARP.

El mensaje ARP esta formado por 28 octetos. En los campos que se describen a continuación se supone un Interfaz Ethernet.

Tipo de *Hardware*

El campo *Hardware* indica el tipo de interfaz de *Hardware*. Por Ejemplo, el valor de una red Ethernet es 1.

Tipo de Interfaz de *Hardware*

Tipo	Descripción
1	Ethernet (10mb)
2	Experimental Ethernet (3 mb)
3	Amateur Radio X.25
4	Proteon ProNET Token Ring
5	Chaos
6	IEEE 802 Network
7	ARCNET
8	Hyperchannel
9	Lanstar
10	Autonet Short Ardes
11	LocalTalk
12	LocalNet

FORMA DE TRANSMIS DE AREA LOCAL

Números de Protocolo

El campo protocolo identifica el protocolo usado. Por ejemplo el valor del interfaz Ethernet es 0800 hex.

Longitud de la dirección *Hardware*

El valor para Ethernet es 6, lo que proporciona 48 bits para una dirección Ethernet (12 semi-octetos)

Longitud del Protocolo

Este campo se usa para definir la longitud de la dirección de red. Para una red IP es 4.

Operación

Especifica el código de la operación. La solicitud ARP tiene valor 1, y la respuesta ARP tiene valor 2.

Dirección *Hardware* del Origen

Los campos Direccion *Hardware* del Origen, Direccion IP del Origen, y Direccion IP del Destino los completa el emisor (si los conoce). El receptor añade la Direccion *Hardware* del Destino y devuelve el mensaje al emisor con el codigo de operacion 2. (El codigo de la Respuesta ARP). La dirección *Hardware* de Origen (para Ethernet) esta formada por octetos que representan una dirección Ethernet de 48 bits, o un numero.

Dirección IP de Origen

La dirección IP de Origen puede ser una dirección de clase A, B o C. (Ver Direcciones IP para obtener una definición de estas clases).

Dirección *Hardware* de Destino

Este campo está formado igual que el campo Dirección *Hardware* de Origen.

Dirección IP de Destino

Este campo es igual que el campo Dirección IP de Origen

Formato del ARP

	Octet +0	*Octet +1*	*Octet +2*	*Octet +3*
	7 6 5 4 3 2 1 0	7 6 5 4 3 2 1 0	7 6 5 4 3 2 1 0	7 6 5 4 3 2 1 0
+0	*Hardware*		*Protocol*	
+4	*Length HW Addr.*	*Protocol Length*	*Operation*	
+8	*Source Hardware Ardes*			
+12	*Source Hardware Address*		*Source IP Address*	
+16	*Source IP Address*		*Destination Hardware Address*	
+20	*Destination Hardware Address*			
+24	*Destination IP Ardes*			

3.1.6. RARP

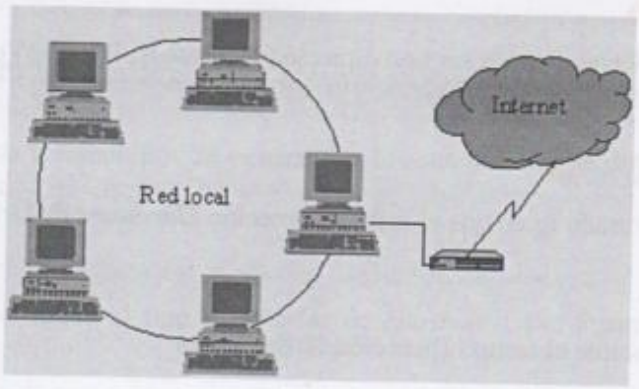
El protocolo RARP (Reverse Address Resolution Protocol) es el encargado de asignar una dirección IP a una dirección física.

Formato del Mensaje RARP

El formato del RARP es similar al del ARP. El valor del código de operación para una solicitud es 3, y el valor para una respuesta es 4.

3.1.7. Proxy

Imagine la siguiente situación: Se dispone de una red local en la cual varios computadores están conectados entre sí. Uno de ellos tiene además una conexión con Internet (a través de un ISP), ya sea telefónica o a través de un proveedor de acceso de banda ancha (ADSL, Cablemodem, Wireless, etc).



De este modo únicamente ese computador podría tener acceso a Internet. Evidentemente sería deseable que todos los demás computadores de la red local consigan acceder a Internet empleando esa única conexión.

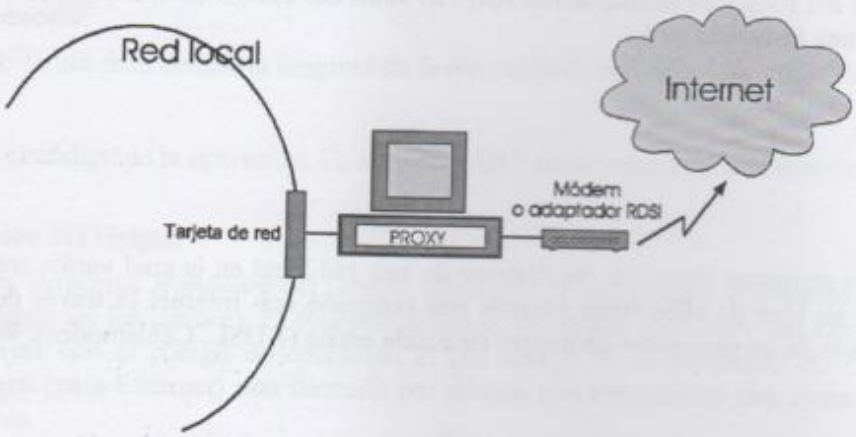
La solución tradicional consistía en emplear un dispositivo denominado encaminador (*router*) dedicado exclusivamente a esta tarea y que se encargara de transmitir la información de una red a otra. Esta es una solución muy cara y en el caso de las redes pequeñas no se justifica el gasto. Además esto exigiría que cada computador tuviera una dirección IP (pública) otorgada por el proveedor de servicios ISP.

Existe otra posibilidad que consiste en emplear un **proxy**, que es un programa que actúa como pasarela (*gateway*) entre redes, en el caso que nos ocupa entre la red local e Internet. Cada vez que alguno de los computadores de la red desea acceder a Internet realiza esta petición al proxy. El proxy utiliza la única conexión existente para enviar y recibir la información de Internet al computador que la solicita.

COCHE — FIREWALL

Cómo funciona un proxy

Desde el punto de vista del usuario de la red local, el sistema funciona como si tuviera realmente un acceso directo a Internet. El usuario accede inmediatamente desde su computador a una página Web o recibe su correo electrónico, sin siquiera saber que el proxy existe.



En realidad, al abrir un programa como Netscape o recoger el correo pendiente, la petición de servicio se realiza al proxy, no al servidor de Internet. El proxy es el encargado de redireccionar estas peticiones a la máquina correspondiente (el servidor de la página Web o el servidor de correo) y una vez recibida la información como respuesta, debe retransmitirla al computador que la solicitó.

Ventajas de un proxy

Las ventajas que ofrece la utilización de un proxy en una red local son las siguientes:

- Menor coste: El programa y la instalación tienen un precio mucho menor que cualquier router.
- Una sola línea telefónica: Sólo es preciso disponer de una línea telefónica normal, ADSL o RDSI
- Fácil instalación: La instalación emplea los dispositivos de la propia red local, por lo que se reduce la configuración de los programas.
- Seguridad: El proxy también actúa como una barrera (*firewall*) que limita el acceso a la red local desde el exterior.
- Dirección IP única: La dirección IP es la que identifica de forma unívoca a cada máquina en Internet. Si se utiliza un proxy basta con una dirección IP para toda la red local en lugar de tener una IP para cada uno de los computadores.
- Conexión automática (*autodialing*): No es necesario que el computador que actúa como proxy esté conectado permanentemente a Internet. Con esta función, cada vez que un usuario realiza una petición, el proxy establece la conexión. Del mismo modo el proxy la desconecta cuando no hay ninguna petición, todo ello automáticamente.
- Menor tráfico de red: Proxy almacena automáticamente en la memoria las páginas Web a las que se accede con mayor frecuencia, con lo que se reduce la cantidad de información que es necesario recuperar a través de Internet

3.1.8. Protocolo de Traducción de direcciones de Red (NAT)

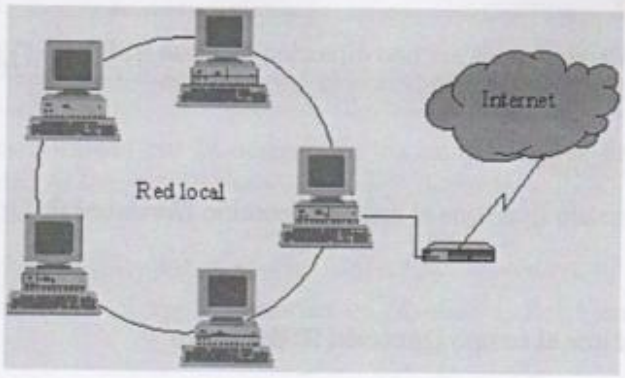
Nota: Este protocolo se describe en el RFC 1631.

La necesidad de la traducción de direcciones IP surge cuando las direcciones IP internas de la red no pueden ser usadas fuera de la red, bien porque no son válidas en el exterior (porque son direcciones IP privadas), bien porque el direccionamiento interno debe mantenerse separado de la red externa.

Las reglas de encaminamiento en Internet imponen que para que un paquete llegue a destino éste debe haber sido generado por un host y se debe dirigir a otro host que posea una dirección IP única (y pública). Debido al crecimiento de Internet la solicitud de direcciones IP es cada vez mayor y se complica el armado de las tablas de los enrutadores.

La solución para que todas las máquinas de una LAN de una pequeña empresa o las PC de ususarios particulares se puedan conectar simultáneamente a Internet, es que empleen direcciones IP privadas y que sea el ISP el que las convierta a direcciones IP públicas.

El protocolo de traducción de direcciones de Red (en inglés NAT) permite utilizar un rango de direcciones privadas (reservadas) en la red local y que el encaminador (enrutador propio o del ISP) se encargue de hacer el cambio (la traducción direcciones IP públicas (legales) y números de puertos). Cuando le llega un datagrama IP de alguna máquina de la red local, se fija en la tabla de traducciones de direcciones de red que posee y modifica el datagrama para que parezca que fue generado por el propio



De este modo únicamente ese computador podría tener acceso a Internet. Evidentemente sería deseable que todos los demás computadores de la red local consigan acceder a Internet empleando esa única conexión.

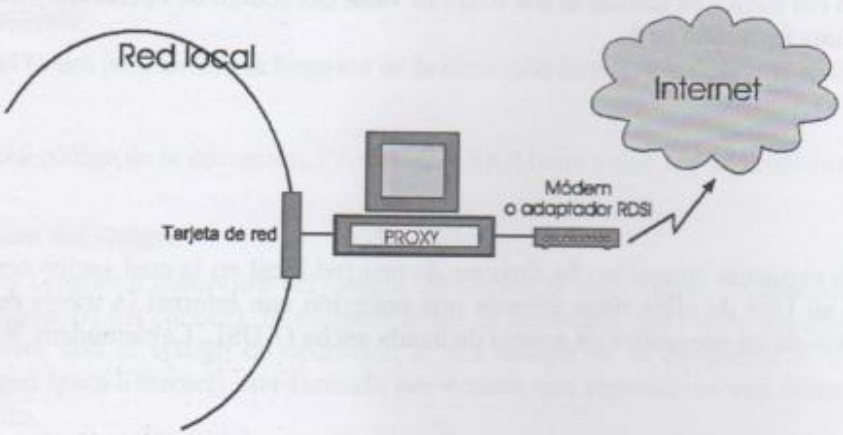
La solución tradicional consistía en emplear un dispositivo denominado encaminador (*router*) dedicado exclusivamente a esta tarea y que se encargara de transmitir la información de una red a otra. Esta es una solución muy cara y en el caso de las redes pequeñas no se justifica el gasto. Además esto exigiría que cada computador tuviera una dirección IP (pública) otorgada por el proveedor de servicios ISP.

Existe otra posibilidad que consiste en emplear un **proxy**, que es un programa que actúa como pasarela (*gateway*) entre redes, en el caso que nos ocupa entre la red local e Internet. Cada vez que alguno de los computadores de la red desea acceder a Internet realiza esta petición al proxy. El proxy utiliza la única conexión existente para enviar y recibir la información de Internet al computador que la solicita.

CACHE — FIREWALL

Cómo funciona un proxy

Desde el punto de vista del usuario de la red local, el sistema funciona como si tuviera realmente un acceso directo a Internet. El usuario accede inmediatamente desde su computador a una página Web o recibe su correo electrónico, sin siquiera saber que el proxy existe.



En realidad, al abrir un programa como Netscape o recoger el correo pendiente, la petición de servicio se realiza al proxy, no al servidor de Internet. El proxy es el encargado de redireccionar estas peticiones a la máquina correspondiente (el servidor de la página Web o el servidor de correo) y una vez recibida la información como respuesta, debe retransmitirla al computador que la solicitó.

Ventajas de un proxy

Las ventajas que ofrece la utilización de un proxy en una red local son las siguientes:

- Menor coste: El programa y la instalación tienen un precio mucho menor que cualquier router.
- Una sola línea telefónica: Sólo es preciso disponer de una línea telefónica normal, ADSL o RDSI
- Fácil instalación: La instalación emplea los dispositivos de la propia red local, por lo que se reduce la configuración de los programas.
- Seguridad: El proxy también actúa como una barrera (*firewall*) que limita el acceso a la red local desde el exterior.
- Dirección IP única: La dirección IP es la que identifica de forma unívoca a cada máquina en Internet. Si se utiliza un proxy basta con una dirección IP para toda la red local en lugar de tener una IP para cada uno de los computadores.
- Conexión automática (*autodialing*): No es necesario que el computador que actúa como proxy esté conectado permanentemente a Internet. Con esta función, cada vez que un usuario realiza una petición, el proxy establece la conexión. Del mismo modo el proxy la desconecta cuando no hay ninguna petición, todo ello automáticamente.
- Menor tráfico de red: Proxy almacena automáticamente en la memoria las páginas Web a las que se accede con mayor frecuencia, con lo que se reduce la cantidad de información que es necesario recuperar a través de Internet

3.1.8. Protocolo de Traducción de direcciones de Red (NAT)

Nota: Este protocolo se describe en el RFC 1631.

La necesidad de la traducción de direcciones IP surge cuando las direcciones IP internas de la red no pueden ser usadas fuera de la red, bien porque no son válidas en el exterior (porque son direcciones IP privadas), bien porque el direccionamiento interno debe mantenerse separado de la red externa.

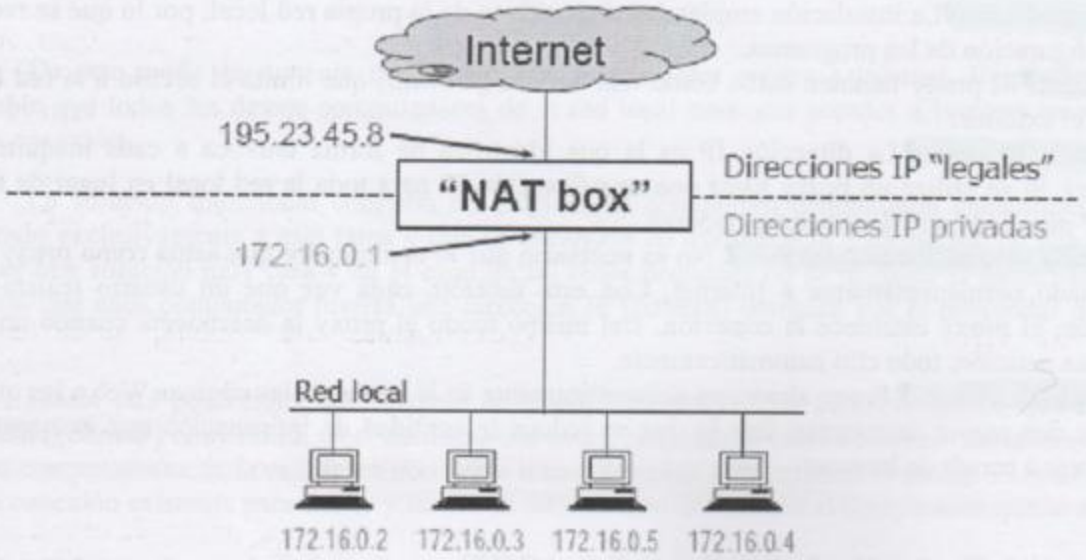
Las reglas de encaminamiento en Internet imponen que para que un paquete llegue a destino éste debe haber sido generado por un host y se debe dirigir a otro host que posea una dirección IP única (y pública). Debido al crecimiento de Internet la solicitud de direcciones IP es cada vez mayor y se complica el armado de las tablas de los enrutadores.

La solución para que todas las máquinas de una LAN de una pequeña empresa o las PC de ususarios particulares se puedan conectar simultáneamente a Internet, es que empleen direcciones IP privadas y que sea el ISP el que las convierta a direcciones IP públicas.

El protocolo de traducción de direcciones de Red (en inglés NAT) permite utilizar un rango de direcciones privadas (reservadas) en la red local y que el encaminador (enrutador propio o del ISP) se encargue de hacer el cambio (la traducción direcciones IP públicas (legales) y números de puertos). Cuando le llega un datagrama IP de alguna máquina de la red local, se fija en la tabla de traducciones de direcciones de red que posee y modifica el datagrama para que parezca que fue generado por el propio

encaminador. A continuación saca el datagrama a Internet donde aparece generado por una dirección IP pública de las que dispone el encaminador. Cuando la máquina destino recibe el datagrama cree que se ha originado en la máquina enrutadora, y responde a dicha dirección de Internet. Cuando el encaminador recibe un datagrama en su interfaz de red conectada a Internet, busca en su tabla de conexiones enmascaradas en curso para ver si el datagrama pertenece a alguna máquina de la LAN y, si es así, deshace la traducción que hizo en el primer datagrama y reenvía este datagrama de respuesta a la máquina local.

En la siguiente figura arece un ejemplo sencillo.



Tenemos una pequeña red LAN de tipo Ethernet en la que utilizamos uno de los rangos de direcciones reservadas. La red dispone de un encaminador con NAT, que proporciona acceso a Internet. Una de las máquinas de la red (172.16.0.3) desea establecer una conexión con el host remoto en Internet (supongamos el 209.1.106.178). El equipo encamina su datagrama por el encaminador con NAT, que identifica la petición de conexión como requiriente de los servicios de NAT. El encaminador entonces acepta el datagrama, sustituye la dirección IP de la máquina origen del datagrama por una IP de las que dispone, y transmite el datagrama al host destino. El host destino cree que ha recibido una petición de conexión de la máquina con dirección IP origen 195.23.45.8, y genera un datagrama de respuesta. La máquina enmascaradora, al recibir ese datagrama, halla la asociación en su tabla de enmascaramiento y deshace la sustitución que llevó a cabo en el primer datagrama. Entonces transmite el datagrama de respuesta a la máquina origen.

La máquina local (en la LAN) cree que se está comunicando directamente con el host remoto. El host remoto no sabe nada de la existencia de la máquina local y cree que ha establecido una conexión con la máquina. El encaminador sabe que las otras dos máquinas están hablando entre sí y en qué puertos, y realiza las traducciones de direcciones y puertos necesarias para que la comunicación tenga lugar.

El proceso de traducción de direcciones de red privadas a públicas se puede dar de dos formas:

- Estática: El enrutador posee una tabla de correspondencias "1 a 1" entre direcciones IP privadas y públicas. Dicha tabla es configurada por el administrador de red.

- Dinámica: El enrutador posee un conjunto de direcciones IP públicas a disposición de las máquinas que quieran establecer conexiones a Internet. Cuando una conexión finalice la dirección IP pública será liberada para que otro host pueda iniciar conexión con dicha dirección.

Ventajas y desventajas de la utilización de NAT

La funcionalidad de traducción de direcciones de red IP viene acompañada de su propio conjunto de efectos laterales, algunos son útiles y algunos pueden acabar siendo un problema.

Ninguna de las máquinas en la red detrás del encaminador enmascarador son jamás vistas directamente desde Internet. Consecuentemente, sólamente se necesita una dirección IP válida y rutable para permitir que todas las máquinas establezcan conexiones hacia Internet. Esto tiene un lado no tan bueno: ninguna de esas máquinas es visible desde Internet, y por lo tanto no se puede conectar directamente a ellas desde Internet. La única máquina visible en una red enmascarada es el propio encaminador enmascarador. Se trata de algo importante cuando se piensa en servicios como el correo o el FTP. Resulta de utilidad decidir qué servicios deberían ser provistos por la máquina enmascaradora y para cuáles debería actuar como proxy o tratar de algún otro modo especial.

Segundo, dado que ninguna de las máquinas enmascaradas son visibles, se encuentran relativamente protegidas de ataques del exterior. Eso puede simplificar (o eliminar) la necesidad de puesta a punto de funcionalidades de firewall en la máquina enmascaradora. No se debe confiar demasiado en ésto, puesto que la red local estará únicamente tan segura como lo esté la máquina enmascaradora. Así, si la seguridad es un punto importante, se debería utilizar un firewall para protegerla.

Tercero, el enmascaramiento IP tendrá cierto impacto negativo en el rendimiento de su red. En un escenario típico ese impacto negativo será probablemente insignificante. Si se tiene un gran número de sesiones enmascaradas activas puede ocurrir que se perciba cierta sobrecarga en la máquina enmascaradora que afecte negativamente al rendimiento de la red. El enmascaramiento IP implica un incremente considerable en el proceso que requiere cada datagrama comparado con el normalmente exigiría. Si piensa utilizar un 386SX16 como encaminador enmascarador para una conexión telefónica a Internet puede resultar, pero no espere demasiado si quiere usarlo como encaminador en su red corporativa a velocidades Ethernet.

Por último, ciertos servicios de red simplemente no funcionarán a través de enmascaramiento, o, al menos, no sin un poco de ayuda. Típicamente se trata de servicios que dependen de conexiones entrantes para funcionar, como ciertos tipos de Canales de Comunicación Directa (DCC), ciertas funciones del IRC, o algunos tipos de servicios de audio y vídeo multicast. Algunos de esos servicios disponen de módulos del kernel especialmente desarrollados para proporcionar una solución, y de ellos hablaremos dentro de un momento. Para otros es posible que no se encuentre soporte, así que se debe tener en cuenta que el enmascaramiento no es la solución adecuada en todas las situaciones.

COMO SE LLEGA DESDE EL ORIGEN DEL PAQUETE HASTA EL FINAL

3.2. Enrutamiento

3.2.1. Introducción

La función principal de la capa de red es enrutar paquetes de la máquina de origen a la de destino.

El **algoritmo de enrutamiento** es aquella parte de *software* de la capa de red, encargada de decidir la línea de salida por la que se transmitirá un paquete de entrada.

El algoritmo de enrutamiento debe ser capaz de adaptarse a los cambios de topología y tráfico, sin requerir el aborto de todas las actividades en todos los *hosts* y rearranque de la red con cada caída del enrutador.

Los algoritmos de enrutamiento pueden clasificarse en dos grupos:

1- **Los algoritmos no adaptables o estáticos**: la decisión de qué ruta se tomará para ir de *i* a *j*, se calcula por adelantado, fuera de línea, y se carga en los enrutadores al iniciar la red. Son aplicables en redes pequeñas donde el tráfico es predecible. Exigen la tarea de configuración por parte de los administradores de la red

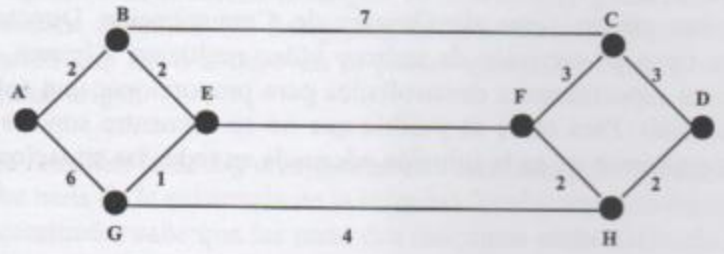
2- **Los algoritmos adaptables o dinámicos**: cambian la decisión de enrutamiento, para reflejar los cambios de topología y generalmente de tráfico. Aplicables en redes amplias donde las condiciones y las topologías varían constantemente. Requieren el intercambio de información entre enrutadores para actualización de las tablas

MENOR CANTIDAD DE SALTOS.

VENTAJA: SI UN NODO ESTA EN CONFLICTO LO SALTA.

3.3. Enrutamiento por la trayectoria más corta

La idea es armar un grafo de la subred, en él cada nodo representa un enrutador y cada arco del grafo una línea de comunicación. Para escoger una ruta entre un par de nodos dados, el algoritmo simplemente encuentra en el grafo, la trayectoria más corta entre ellos.



ROUTER

FIGURA 3.1: Enrutamiento de Trayectoria más Corta.

El concepto de la **trayectoria más corta** merece una explicación. Una manera de medir la longitud de una trayectoria es por la cantidad de escalas. Usando esta métrica, las trayectorias ABC y ABE de la **figura 3.1** tienen la misma longitud. Otra métrica es la distancia geográfica en kilómetros, en cuyo caso ABC es mucho mayor que ABE.

En el caso más general, las etiquetas de los arcos podrían calcularse como una función de la distancia, ancho de banda, tráfico medio, costo de comunicaciones, longitud media de las colas, retardo medio y otros factores. Cambiando la función de ponderación, el algoritmo calcularía la trayectoria media más corta de acuerdo con cualquiera de varios criterios, o una combinación de criterios.

Se conocen varios algoritmos de cálculo de la trayectoria más corta entre dos nodos de un grafo, por ejemplo el de **Dijkstra.** Cada nodo se etiqueta (entre paréntesis) con su distancia al nodo de origen a través de la mejor trayectoria conocida. Inicialmente no se conocen trayectorias, por lo que todos los nodos tienen la etiqueta de infinito. A medida que avanza el algoritmo y se encuentran las trayectorias pueden cambiar las etiquetas reflejando mejores trayectorias. Una etiqueta puede ser tentativa o permanente. Al descubrirse que una etiqueta representa la trayectoria más corta posible del origen a ese nodo, se vuelve permanente y no cambia más (**figura 3.2).**

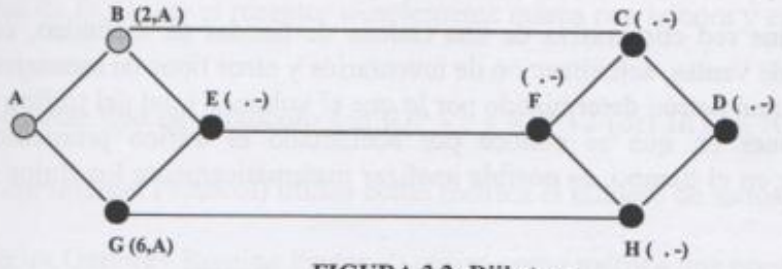


FIGURA 3.2: Dijkstra.

3.4. Inundación

Otro algoritmo estático es la **inundación** en la que cada paquete de entrada se envía por cada una de las líneas de salida, excepto por aquella por la que llegó. La inundación genera grandes cantidades de paquetes duplicados; de hecho, una cantidad infinita, a menos que se tomen algunas medidas para limitar el proceso. Una de las tales medidas es un contador de escalas contenido en la cabecera de cada paquete, el cual disminuye en cada escala, descartándose el paquete al llegar el contador a cero. Inmediatamente, el contador de escala debe inicializarse con la longitud de la trayectoria entre el origen y el destino. Si el transmisor no conoce el tamaño de la trayectoria, puede inicializar el contador al peor caso, es decir, el diámetro total de la subred.

Una técnica alterna para ponerle diques a la inundación, es llevar un registro de los paquetes diseminados, para evitar enviarlos una segunda vez. Una manera de lograr esta meta, es hacer que el enrutador de origen ponga un número de secuencia en cada paquete que recibe de sus *hosts*.

Una variación de la inundación, un poco más práctica, es la **inundación selectiva**. En este algoritmo, los enrutadores no envían cada paquete de entrada por todas las líneas, sino sólo por aquellas que van aproximadamente en la dirección correcta.

La inundación no es práctica en la mayoría de las aplicaciones, pero tiene algunos usos. Por ejemplo, en las aplicaciones militares, donde pueden volar en pedazos grandes cantidades de enrutadores

en cualquier momento, es altamente deseable la robustez de la inundación. En las aplicaciones de bases de datos distribuidas a veces es necesario actualizar concurrentemente todas las bases de datos, en cuyo caso puede ser útil la inundación. Un tercer posible uso de la inundación es como métrica contra la que pueden compararse otros algoritmos de enrutamiento. La inundación siempre escoge la trayectoria más corta posible, porque escoge en paralelo todas las trayectorias posibles.

3.5. Enrutamiento basado en flujo

Los algoritmos estudiados hasta ahora sólo tienen en cuenta la topología; no consideran la carga. En esta sección veremos un algoritmo estático que usa tanto la topología como la carga para el enrutamiento.

En algunas redes, la tasa media de flujo entre cada par de nodos es relativamente estable y predecible.

Por ejemplo, en una red corporativa de una cadena de tiendas de menudeo, cada tienda puede enviar pedidos, informes de ventas, actualización de inventarios y otros tipos de mensajes bien definidos a sitios conocidos siguiendo un patrón determinado por lo que el volumen total del tráfico varía poco de día en día. En las condiciones en que se conoce por adelantado el tráfico promedio de *i* a *j* y es razonablemente constante en el tiempo, es posible analizar matemáticamente los flujos para optimizar el enrutamiento.

La idea en que se basa el análisis es que, para una línea dada, si se conocen la capacidad y el flujo promedio, es posible calcular el retardo promedio de los paquetes en esa línea a partir de la teoría de colas. De los retardos promedios de todas las líneas, es directo el cálculo de un promedio ponderado por el flujo para obtener el retardo de paquete medio de la subred completa. El problema de enrutamiento se reduce entonces a encontrar el algoritmo de enrutamiento que produzca el retardo promedio mínimo para la subred (**figura 3.3**).

Para usar esta técnica, debe conocerse por adelantado cierta información. Primero debe conocerse la topología de la subred, segundo debe estar dada la matriz de tráfico, F_{ij}. Tercero, debe estar disponible la matriz de capacidad, *Cij* (donde se especifica la capacidad de cada línea en bps). Por último debe escogerse algún algoritmo tentativo de enrutamiento.

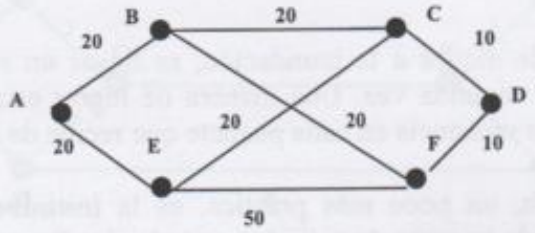


FIGURA 3.3: Enrutamiento Basado en Flujo.

3.6. Enrutamiento por vector de distancia

Estos algoritmos operan haciendo que cada enrutador mantenga una tabla (por ejemplo, un vector), que da la mejor distancia conocida a cada destino y la línea a usar para llegar ahí. Estas tablas se actualizan intercambiando información con los vecinos.

Cada enrutador mantiene una tabla de enrutamiento indexada por, y conteniendo un registro de, cada enrutador de la subred. Esta entrada comprende dos partes: la línea preferida hacia ese destino y una estimación del tiempo o distancia a ese destino. La métrica utilizada podría ser la cantidad de escalas, el retardo del tiempo en milisegundos, el número total de paquetes encolados por la trayectoria, o algo parecido; además presentan la facilidad de que el administrador pueda ponderar de distinta forma cada uno de los componentes de dicha métrica.

Se supone que el enrutador conoce la distancia a cada uno de sus vecinos. Si la métrica es de escalas, la distancia simplemente es una escala. Si la métrica es la longitud de la cola, el enrutador simplemente examina cada cola. Si la métrica es el retardo, el enrutador puede medirlo directamente con paquetes especiales de ECO que el receptor simplemente marca con la hora y envía de regreso tan rápido como puede.

Ejemplos de este tipo de protocolo son RIP v1 y RIP v2 (del IETF), IGRP de la empresa Cisco, etc.

RIP (Routing Internet Protocol) utiliza como métrica el número de saltos hasta la red destino

IGRP (Interior Gateway Routing Protocol) utiliza como métrica una combinación de:

- Ancho de banda de la línea
- Confiabilidad de la línea
- Número de saltos
- Retardo de propagación
- Porcentaje de carga de una línea

3.6.1. El problema del conteo a infinito

El enrutamiento por vector de distancia funciona en teoría, pero tiene un problema serio en la práctica aunque converge en la respuesta correcta puede hacerlo lentamente, en particular, reacciona con rapidez a las buenas noticias, pero con lentitud ante las malas. Esto se conoce como el problema de conteo infinito.

Por ejemplo consideremos la subred de cuatro nodos de la **figura 3.4.** Inicialmente, tanto A como B tienen una distancia a D de 2, y C tiene una distancia de 1 al mismo lugar.

Ahora supóngase que se desactiva la línea C-D. Usando el horizonte divido, tanto A como B le indican a C que no puede llegar a D. Por lo tanto, C concluye de inmediato que D es inalcanzable y le informa tanto a A como a B. Desafortunadamente A escucha que B tiene una trayectoria de longitud 2 a D, por lo que supone que puede llegar a D a través de B en tres escalas. De manera parecida, B concluye que puede llegar a D en tres escalas a través de A. En el siguiente intercambio cada uno establece en 4 su distancia a D. Ambos cuentan gradualmente a infinito, que es precisamente el comportamiento que estamos tratando de evitar.

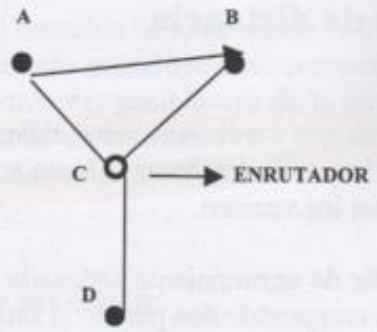


FIGURA 3.4: Conteo al infinito.

3.6.2. Recorte por horizonte dividido

El algoritmo del horizonte dividido funciona de la misma manera que el enrutamiento por vector de distancia, excepto que la distancia a un destino no se informa en la línea por la que se envían paquetes para ese destino. De esta forma evito publicar actualizaciones erróneas en la dirección del enrutador que me informó del cambio.

3.7. Enrutamiento por estado de enlace

El enrutamiento por vector de distancia se usó en Arpanet hasta 1979, cuando fue reemplazado por el enrutamiento de estado de enlace. Dos problemas principales causaron su defunción. Primero, dado que la métrica de retardo era la longitud de la cola, no tomaba en cuenta el ancho de banda al escoger rutas. Inicialmente las líneas eran de 56 kbps, por lo que el ancho de banda no era importante, pero una vez que se modernizaron algunas líneas a 230 kbps y otras a 1.544 Mbps, el no tomar en cuenta el ancho de banda se volvió un problema importante. Un segundo problema era que el algoritmo con frecuencia tardaba demasiado en converger, aun con trucos como el horizonte dividido.

El concepto en que se basa el enrutamiento por estado de enlace es sencillo y puede postularse en cinco partes.

Cada enrutador debe:

1- Descubrir a sus vecinos y conocer sus direcciones de red.
2- Medir el retardo o costo para cada uno de sus vecinos.
3- Construir un paquete que indique todo lo que acaba de aprender.
4- Enviar este paquete a todos los demás enrutadores.
5- Con todos los datos obtenidos, calcular la trayectoria más corta a todos los demás enrutadores.

A continuación veremos con más detalle los siguientes puntos:

3.7.1. Conocimiento de los vecinos

Al ponerse en operación el enrutador, su primera tarea es averiguar quiénes son sus vecinos, esto lo logra poniendo un paquete especial de **HOLA (hello)** por cada línea punto a punto. Se espera que el enrutador del otro extremo envíe de regreso una respuesta indicando quién es.

3.7.2. Medición del costo de la línea

El algoritmo de enrutamiento por estado de enlace requiere que cada enrutador sepa, o cuando tenga una idea razonable, del retardo a cada uno de sus vecinos. La manera más directa de determinar este retardo es enviar un paquete especial **ECO (echo)** a través de la línea, el cual debe enviar de regreso inmediatamente el otro lado. Si mide el tiempo de ida y vuelta y lo divide entre dos, el enrutador transmisor puede tener una idea razonable del retardo. Para obtener mejores resultados aún, la prueba puede llevarse a cabo varias veces y usarse el promedio.

3.7.3. Construcción de los paquetes de estado de enlace

Una vez que se ha recabado la información para el intercambio, el siguiente paso es que cada enrutador construya un paquete con todos los datos. El paquete comienza con la identidad del transmisor, seguida de un número de secuencia, una edad (que se describirá después) y una lista de vecinos. Para cada vecino, se cita el retardo a ese vecino. En la **figura 3.5** se da un ejemplo de subred, mostrándose el retardo en las líneas.

Es fácil construir los paquetes de enlace. La parte difícil es determinar cuándo construirlo. Una posibilidad es construirlos periódicamente, es decir, a intervalos regulares. Otra posibilidad es al ocurrir un evento significativo, como la caída o reactivación de una línea o de un vecino, o el cambio apreciable de sus propiedades.

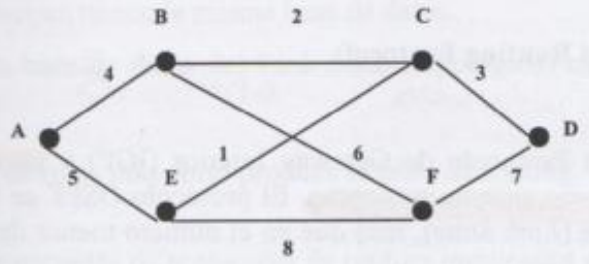


FIGURA 3.5: Subred.

3.7.4. Distribución de los paquetes de estado de enlace

Primero describiremos el algoritmo básico de distribución y luego lo reafirmaremos. La idea fundamental es usar inundación para distribuir los paquetes de estado de enlace. A fin de mantener controlada la inundación, cada paquete contiene un número de secuencia que se incrementa con cada paquete nuevo enviado. Los enrutadores llevan el registro de todos los pares (enrutador de origen, secuencia) que ven. Al llegar un paquete de estado de enlace, se revisa contra la lista de paquetes ya vistos. Si es nuevo, se reenvía a través de todas las líneas, excepto aquellos por la que llegó. Si es un duplicado, se descarta. Si llega un paquete con número de secuencia menor que el mayor visto hasta el momento, se rechaza como obsoleto.

Este algoritmo tiene algunos problemas, pero son manejables. Primero, si los números de secuencia vuelven a comenzar, reinará la confusión. La solución aquí es usar un número de secuencia de 32 bits. Con un paquete de estado de enlace por segundo, el tiempo para volver a empezar será de 137 años, por lo que puede ignorarse esta posibilidad.

Segundo, si llega a caerse un enrutador, perderá el registro de su número de secuencia. Si se comienza nuevamente en cero, se rechazará como duplicado el siguiente paquete.

Tercero, si llega a romperse un número de secuencia y se recibe 65,540 en lugar de 4 (un error de un bit), los paquetes de 5 a 65,540 serán rechazados como obsoletos, dado que se piensa que el número de secuencia actual es 65,540.

La solución a todos estos problemas es incluir la edad de cada paquete después del número de secuencia y disminuirla una vez cada segundo. Al llegar la edad a cero se descarta la información de ese enrutador.

3.7.5. Cálculo de las nuevas rutas

Una vez que un enrutador ha acumulado un grupo completo de paquetes de estado de enlace, puede construir el grafo de la subred completa porque todos los enlaces están completados. De hecho, cada enlace se presenta dos veces, una para cada dirección. Los valores pueden promediarse o usarse por separado.

Ahora puede ejecutarse localmente el algoritmo de **Dijkstra** para construir la trayectoria más corta posible a todos los destinos. Los resultados de este algoritmo pueden instalarse en las tablas de enrutamiento y reiniciarse la operación normal.

3.7.6. OSPF (Open Shortest Path First Routing Protocol)

Red interna - BDM IPS

OSPF está clasificado como un Protocolo de Gateway Interior (IGP) y se usa para distribuir información de routing dentro de un único sistema autónomo. El protocolo OSPF se basa en SPF o sea que es un protocolo de estado de enlace (*Link State*), más que en el número menor de saltos habitual de los protocolos de routing de Internet.

OSPF encamina paquetes basados solo en la dirección IP destino del paquete y no se requiere además de eso ninguna encapsulación. Es un protocolo dinámico el cual calcula rutas libres de bucles después de un periodo de convergencia corto y predecible. Cada Router mantiene una base de datos que describe el sistema autónomo, el cual consiste en entradas que describen cada estado local del Router, por ejemplo sus interfaces disponibles y los vecinos alcanzables. Todos los routers funcionan con el mismo algoritmo en paralelo.

OSPF permite a las redes agruparse conjuntamente dentro de áreas, y en cada área funciona una copia separada del algoritmo SPF. La topología interior del área es invisible fuera de ella, y los routers de dentro del área no tiene una detallada información de la topología exterior.

Cuando se configuran áreas "no OSPF", cada router tiene una base de datos idéntica desde la cual genera su tabla de routing calculando caminos en topología de árbol donde él es la raíz. Este árbol da la ruta completa a cualquier red destino, pero solo el salto (hop) siguiente es usado en el proceso de reenvío.

El uso de áreas reduce el tráfico de routing comparado al que tiene el sistema autónomo completo como una única área. El routing entre áreas se efectúa vía backbone o troncal, el cual consiste en redes las

cuales no están en ninguna área ni sus routers acoplados y también routers que conectan múltiples áreas. Con este supuesto los routers son divididos en diferentes categorías dependiendo de su localización, routers internos, routers de límite de área, routers de backbone.

OSPF soporta los siguientes tipos de red física:

a) **Punto a punto.** Los cuales unen un único par de routers. Por ejemplo una línea en serie.
b) **Broadcast.** Soporta muchos routers, con la capacidad de enviar un único mensaje a todos los dispositivos acoplados. Por ejemplo Ethernet.
c) **No broadcast.** Con múltiple acceso pero sin capacidad de broadcast. Por ejemplo X.25.

Resumen funcional de OSPF

1. Protocolo HELLO usado para determinar a sus vecinos y elegir un router particular.

2. Formar adyacencias con algunos vecinos y sincronizar las bases de datos de las topologías.

3. Paquetes de protocolo de routing son intercambiados con las adyacencias, en actualizaciones de bases de datos particulares.

4. Los routers indican su estado de línea por método de "inundación" del área, para asegurar que todos los routers tienen la misma base de datos.

5. Desde la base de datos del Link State (topológico) cada router calcula el árbol de rutas más corto.

6. El árbol de rutas más corto produce la tabla de routing.

Hay cinco tipos de paquetes de protocolos de routing implicados en este proceso:

i.	HELLO	-	descubre/mantiene vecindades
ii.	Database description	-	compendia los contenidos de las bases de datos
iii.	Link state request	-	descarga base de datos
Iv.	Link state update	-	actualiza la base de datos
v.	Link state ack	-	inundación de reconocimientos

El protocolo OSPF funciona directamente sobre IP, usando IP tipo 89, y utiliza una cabecera estándar como sigue:

Tipo de paquete	-	HELLO, etc.
Longitud de paquete	-	Longitud total del paquete OSPF
ID router	-	
ID área	-	Área a la que el paquete está siendo enviado
Checksum	-	Suma de verificación para la totalidad del paquete OSPF
Autentificación	-	Información de la autentificación

PROTOCOLO HELLO

El protocolo HELLO se usa para establecer y mantener vecindades, y sobre redes multiacceso elegidas por un router determinado. En redes tipo broadcast cada router envía paquetes HELLO multicast. Sobre redes "no broadcast" los mensajes HELLO son enviados a una lista configurada de routers designados potenciales.

Para hacer una adyacencia dos vecinos primero sincronizan sus bases de datos por medio del *database exchange process*. Este es un intercambio de secuencia de información con una relación master/slave entre dos routers (el master será el router del ID más alto). Después de este proceso cada router tiene una lista de avisos de link state más recientes de su vecino, siendo estos solicitados con el link state request. Cuando se completa los dos routers han completado la adyacencia plenamente y la han avisado como tal.

La adyacencia queda establecida si:

- La red es punto a punto.
- La red es un enlace virtual
- El router es un router designado
- El vecino es un router designado
- El vecino es un router designado como backup

El router designado es elegido por medio del protocolo HELLO. Cuando una primera interfaz llega a convertirse en operacional, chequea para ver si hay ya un router designado para la red. Si lo hay, este es aceptado; si no, el router con la prioridad más alta será el designado. Se elige también un router designado de backup. Este es también adyacente a todos los routers de la red y se usa si el que estaba previsto falla. Si esto no fuera hecho, entonces las adyacencias podrían estar formadas por todos los routers de la red, y la red podría no estar disponible durante la sincronización de las bases de datos.

Los paquetes HELLO son enviados desde cada interfaz de un router a intervalos regulares. Ellos contienen la router ID, intervalo HELLO, *Router Dead Interval*, una lista de todos los routers desde los cuales los HELLO han sido recientemente recibidos y también su propia elección de router designado y backup. Por medio de este proceso cada router construye una *neighbour data structure* para cada vecino con el cual se puede comunicar, y esto contiene toda la información necesaria para formar adyacencias apropiadas y también contiene el estado funcional del vecino, por ejemplo DOWN o FULL.

ESTRUCTURA DE LAS TABLAS DE ROUTING

La tabla de routing contiene toda la información necesaria para enviar datagramas IP hacia su destino. Cada entrada o unidad de información de la lista contiene el conjunto de mejores caminos para un destino determinado. Cuando se procesa un paquete la tabla es examinada buscando la mejor entrada para su destino, y proporciona la información del próximo salto -hop- para su retransmisión. La entradas de la tabla consisten en un tipo de destino, destino ID, área, tipo de camino, coste, siguiente hop y router de avisos.

Avisos de Link State

Cada router origina avisos de link state, los cuales describen como los routers de área y los enlaces están interconectados. El conjunto de avisos de estado de enlace forma la Link State Database topológicamente. Existen cinco tipos de mensajes de Link State; router links, network links, summary

link advertisements, cada uno de los cuales pasa diferente información. Hay una base de datos diferente para cada área y el cálculo del camino más corto es repetido en cada área.

Los contenidos de los avisos de Link State varían dependiendo del tipo de mensaje. Por ejemplo, para avisos router links el contenido describe las interfaces que trabajan del router (enlaces, links) para el área, y la información contenida varía según el tipo de red con la cual el interfaz está conectado.

TIPO DE LINK	DESCRIPCIÓN	LINK ID
1	Punto a punto	ID router vecino
2	Red de tránsito	Dirección IP del router designado
3	Red adaptadora	Número de red IP
4	Enlace (link) virtual	ID router vecino

Hay también una métrica asociada con el enlace, la cual identifica el coste usando este enlace de router fuera del límite. Si cuando se recibe en un router dado un aviso Link State se encuentra contenida información nueva o más reciente, se envía por unas interfaces seleccionadas en un mensaje de actualización de Link State para ser difundido por toda el área.

Cálculo de la tabla de routing

Usando la base de datos de Link State para un área un router eliminará su tabla de routing actual (pero guardará una copia) y ejecutará un proceso de búsqueda y construirá un árbol de camino más corto para todos los destinos utilizando el algoritmo de Dijkstra de la especificación OSPF. Si, durante este cálculo, un nuevo camino más corto es encontrado, el nuevo siguiente salto debe ser calculado para ese destino. Esto puede ocurrir repetidamente. Cambios en las entradas de la tabla de routing pueden requerir que un nuevo sumario de avisos de Link State sea generado. Durante este cálculo rutas de igual coste pueden ser mantenidas para su utilización, pero no se requiere que todas ellas sean conservadas.

COMPARACIÓN R.I.P. y O.S.P.F.

FUNCIÓN	R.I.P.	O.S.P.F.
ACTUALIZACIÓN DE ROUTING	Se completa la base de datos cada 30 segundos por broadcast.	Usa el protocolo HELLO para mantener adyacencias. Envía actualizaciones cuando hay un cambio en la base de datos.
MÉTRICA DE DISTANCIAS	Solo contador de saltos (hops).	Basada en el coste del enlace.
VELOCIDAD DE CONVERGENCIA	Lenta (Requiere particiones simples, técnicas de contención para eliminar lazos y lenta convergencia).	Más rápida. Multicast inunda toda el área.
CONTENIDO DE BASE DE DATOS	Contiene una ruta solo para cada red.	Contiene la totalidad de la topología del área en la base de datos.
TOPOLOGÍA DE RED	La totalidad de la red es la única área.	Con múltiples áreas se reduce administración.
TAMAÑO DE RED	15 saltos máximo.	No hay límite.

3.8. Enrutamiento jerárquico

A medida que crecen en tamaño las redes, crecen proporcionalmente las tablas de enrutamiento del enrutador. Las tablas que siempre crecen no sólo consumen memoria del enrutador, sino que también se necesita más tiempo de CPU para examinarlas y más ancho de banda para enviar informes de estado entre enrutadores. En cierto momento, puede crecer hasta el punto en que ya no es factible que cada enrutador tenga una entrada para cada uno de los demás enrutadores, por lo que el enrutamiento tendrá que hacerse jerárquicamente, como ocurre en la red telefónica. Al usarse el enrutamiento jerárquico, los enrutadores se dividen en lo que llamaremos regiones, donde cada enrutador conoce todos los detalles de la manera de enrutar paquetes a destinos dentro de su propia región, pero no saben nada de la estructura interna de las otras regiones.

Al interconectar diferentes redes, es natural considerar cada una como región independiente, a fin de liberar a los enrutadores de una red de la necesidad de conocer la estructura topológica de las demás.

En las redes enormes puede ser insuficiente una jerarquía de dos niveles; puede ser necesario agrupar las regiones en cúmulos, los cúmulos en zonas, las zonas en grupo, etc, hasta que se agoten los nombres para los agregados.

En la **figura 3.6** se da un ejemplo cuantitativo de enrutamiento en una jerarquía de dos niveles en cinco regiones.

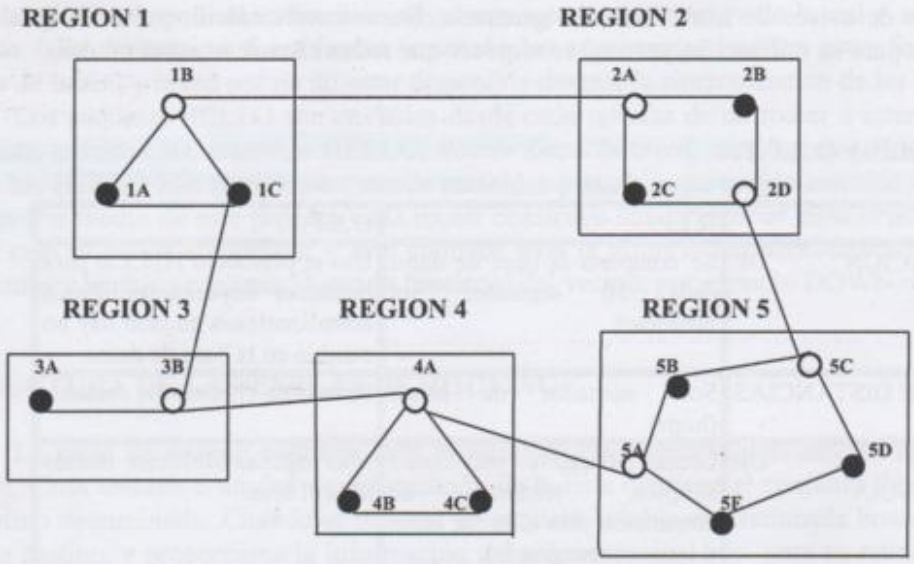


FIGURA 3.6: Enrutamiento Jerárquico.

3.9. Enrutamiento para hosts móviles

Hoy día, millones de personas tienen computadores portátiles, y generalmente quieren leer su correo electrónico y acceder a sus sistemas de archivos normales desde cualquier lugar del mundo. Estos

hosts móviles generan una nueva complicación: para enrutar un paquete a un *host* móvil, la red tiene primero que encontrarlo. El tema de la incorporación de *hosts* móviles en una red es muy joven, pero en esta sección plantearemos algunos de los problemas relacionados y sugeriremos una posible solución.

El modelo del mundo que usan generalmente los diseñadores de la red se muestra en la **figura 3.7**. Aquí tenemos una WAN que consiste en enrutadores y *hosts*. Conectadas a las WAN hay varias LAN, WAN y células inalámbricas.

Se dice que son estacionarios los usuarios que nunca se mueven; se conectan a la red mediante alambres de cobre o fibra óptica. En contraste podemos distinguir otros dos tipos de usuarios. Los usuarios migratorios estacionarios que se mueven de un lugar fijo a otro de tiempo en tiempo, pero que usan la red sólo cuando están conectados físicamente a ella. Los usuarios errantes hacen su cómputo en movimiento, y quieren mantener sus conexiones mientras se mueven. Usaremos el término **usuarios móviles** para indicar cualquiera de las dos últimas categorías.

La meta de enrutamiento en los sistemas con usuarios móviles es posibilitar el envío de paquetes a usuarios móviles usando su dirección base, y hacer que los paquetes lleguen eficientemente a ellos en cualquier lugar en el que puedan estar. Lo difícil, por supuesto, es encontrarlos.

En el modelo de la **figura 3.7**, el mundo se divide en unidades pequeñas. Llamémoslas áreas, siendo un área típicamente una LAN o una célula inalámbrica. Cada área tiene uno o más agentes foráneos, que llevan el registro de todos los usuarios que visitan el área. Además cada área tiene un agente de base, que lleva el registro de todos los usuarios móviles cuya base está en el área, pero actualmente están visitando otra área.

Al entrar un usuario nuevo en un área, ya sea al conectarse a ella o simplemente al entrar en la célula, su computadora debe registrarse con el agente foráneo de ese lugar. Idealmente, al salir un usuario de un área, también eso debe anunciarse para permitir que se borre el registro pero, cuando terminan, muchos usuarios apagan abruptamente su computadora.

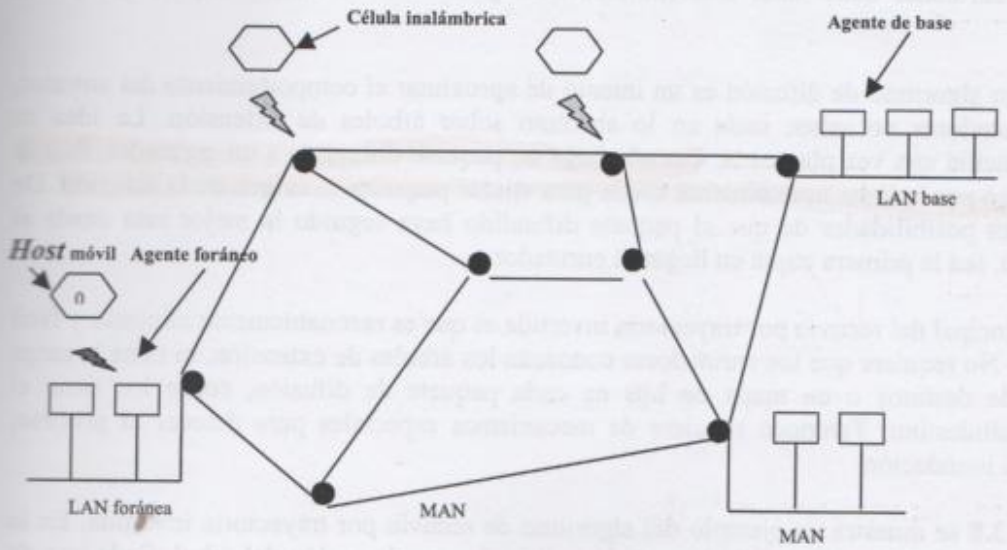


FIGURA 3.7: Enrutamiento por Difusión hacia un usuario movil.

3.10. Enrutamiento por difusión

El envío simultáneo de un paquete a todos los destinos se llama difusión; se han propuesto varios métodos para llevarlo a cabo.

Un método de difusión que no requiere de características especiales de la subred es que el origen simplemente envíe copias del paquete a todos los destinos. El método no sólo desperdicia ancho de banda, sino que también requiere que el origen tenga una lista completa de todos los destinos. En la práctica esta no puede ser la única posibilidad pero sí la menos deseable.

La inundación es otro candidato obvio. Aunque la inundación es poco adecuada para la comunicación punto a punto ordinaria, para difusión puede merecer consideración seria, especialmente si no es aplicable ninguno de los métodos descritos a continuación.

Un tercer algoritmo es un enrutamiento multidestino. Con este método cada paquete contiene una lista de destino, o un mapa de bits que indica los destinos deseados. Al llegar un paquete al enrutador, el enrutador revisa todos los destinos para determinar el grupo de líneas de salida necesarias. El enrutador genera una copia nueva del paquete para cada línea de salida a usar, e incluye en cada paquete sólo aquellos destinos que utilizan las líneas de salida. En efecto el grupo de destinos se divide en tres líneas de salida. Tras una cantidad suficiente de escalas, cada paquete llevará sólo un destino, así que puede tratarse como un paquete normal. El enrutamiento multidestino es como los paquetes con direccionamiento individual, excepto que cuando varios paquetes deben seguir la misma ruta, uno de ellos paga la tarifa y los demás viajan gratis.

Un cuarto algoritmo de difusión usa explícitamente el árbol de descenso para el enrutador que inicia la difusión, o cualquier árbol de extensión adecuado. El árbol de extensión es un subgrupo de la subred que incluye todos los enrutadores pero no contienen ciclos. Si cada enrutador sabe cuáles de sus líneas pertenecen al árbol de extensión, puede copiar un paquete de entrada difundido en todas las líneas del árbol de extensión, excepto por aquella por la que llegó. Este método hace un uso excelente del ancho de banda, generando la cantidad mínima de paquetes necesarios para llevar a cabo el trabajo. El único problema es que el enrutador debe tener conocimiento de algún árbol de extensión para que pueda funcionar.

Nuestro último algoritmo de difusión es un intento de aproximar el comportamiento del anterior, aun cuando los enrutadores no saben nada en lo absoluto sobre árboles de extensión. La idea es excepcionalmente sencilla una vez planteada. Cuando llega un paquete difundido a un enrutador, ésta lo revisa para ver si llegó por la línea normalmente usada para enviar paquetes al origen de la difusión. De ser así hay excelentes posibilidades de que el paquete difundido haya seguido la mejor ruta desde el enrutador y, por tanto, sea la primera copia en llegar al enrutador.

La ventaja principal del reenvío por trayectoria invertida es que es razonablemente eficiente y fácil de poner en práctica. No requiere que los enrutadores conozcan los árboles de extensión, ni tiene la carga extra de una lista de destinos o un mapa de bits en cada paquete de difusión, como los tiene el direccionamiento multidestino. Tampoco requiere de mecanismos especiales para detener el proceso, como en el caso de la inundación.

En la **figura 3.8** se muestra un ejemplo del algoritmo de reenvío por trayectoria invertida. En la primera escala I envía Paquetes a F, H, J y N, como lo indica el segundo reglón del árbol. Cada uno de estos paquetes llega a I por la trayectoria preferida, como lo indica el círculo alrededor de la letra. En la segunda escala, se generan ocho paquetes, dos por cada uno de los enrutadores que recibieron un paquete

de la misma escala. Como resultado, los ochos llegan a enrutadores no sitiados previamente, y todos menos uno llegan a través de la línea preferida. De los nuevos paquetes generados en la tercera escala, sólo dos llegan por la trayectoria preferida (a C y L), así que sólo éstos generan paquetes posteriores. Tras cinco escalas y 24 paquetes, termina la difusión, en comparación con cuatro escalas y 14 paquetes si se hubiera seguido exactamente el árbol de descenso.

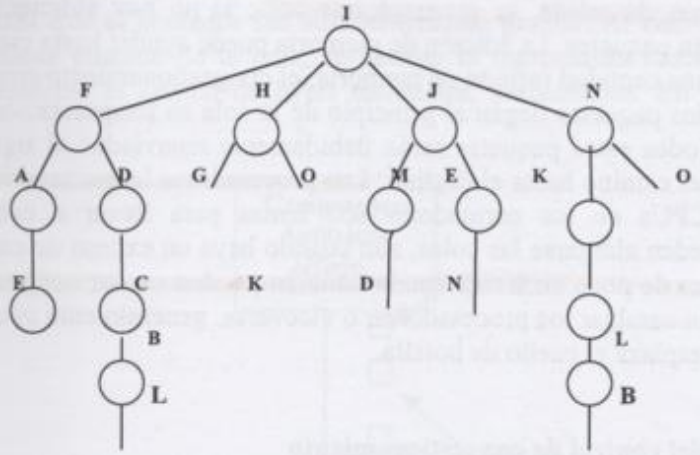


FIGURA 3.8: Algoritmo de Reenvío por Trayectoria Invertida.

3.11. Congestión

Cuando hay demasiados paquetes en la subred, o en parte de ella, hay una degradación del desempeño. Esta situación se llama congestionamiento. El congestionamiento puede ocurrir por varias razones; si repentinamente comienzan a llegar cadenas de paquetes por tres o cuatro líneas de entrada y todos necesitan la misma línea de salida, se generará una cola; si no hay suficiente memoria para contenerlos a todos, se perderán paquetes. La adición de memoria puede ayudar hasta cierto punto, puesto que si los enrutadores tienen una cantidad infinita de memoria, el congestionamiento empeora en lugar de mejorar, ya que para cuando los paquetes llegan al principio de la cola su temporización ha terminado y se han enviado duplicados. Todos estos paquetes serán debidamente reenviados al siguiente enrutador, aumentando la carga en todo el camino hasta el destino. Los procesadores lentos también pueden causar congestionamientos; si las CPUs de los enrutadores son lentas para llevar a cabo las tareas de administración requeridas, pueden alargarse las colas, aún cuando haya un exceso de capacidad de línea. De la misma manera, las líneas de poco ancho de banda también pueden causar congestionamientos. La modernización de las líneas sin cambiar los procesadores, o viceversa, generalmente ayuda un poco, pero con frecuencia simplemente desplaza el cuello de botella.

3.11.1. Principios generales del control de congestionamiento

Las herramientas para llevar a cabo el control del ciclo abierto, incluyen: decidir cuando aceptar tráfico nuevo, decidir cuando descartar paquetes, y cuáles, y tomar decisiones de calendarización en varios puntos de la red. Todas tienen en común el hecho de que toman decisiones independientemente del estado actual de la red.

En contraste, las soluciones de ciclo cerrado se basan en el concepto de un ciclo de realimentación. Este enfoque tiene tres partes cuando se aplica el control de congestionamiento:

1. Supervisar el sistema para detectar cuándo y dónde ocurren congestionamientos.
2. Pasar esta información a lugares en los que puedan llevar a cabo acciones.
3. Ajustar la operación del sistema para corregir el problema.

3.11.2. Algoritmos de control de congestionamiento

3.11.2.1. Algoritmo de cubeta con goteo

Conceptualmente, cada *host* está conectado a la red, mediante una interfaz que contiene un goteo, es decir, una cola finita interna. Si llega un paquete a la cola cuando está llena, se descarta el paquete. En otras palabras, si uno o más procesos del *host* tratan de enviar paquetes cuando ya está en cola la cantidad máxima, se descarta el paquete sin más. Este arreglo, puede incorporarse en el *hardware* de la interfaz, o simularse a través del sistema operativo del *host*.

La implementación de este algoritmo es fácil. La cubeta con goteo consiste en una cola finita. Al llegar un paquete, si hay espacio en la cola, se agrega a ella; de otro modo se descarta. En cada pulso de reloj se transmite un paquete.

La cubeta con goteo que usa conteo de bits se implementa casi de la misma manera. En cada pulso se inicia un contador en *n*. Si el primer paquete de la cola tiene menos bytes que el valor actual del contador, se transmite y se disminuye el contador en esa cantidad de bytes. Pueden enviarse paquetes adicionales mientras que el contador sea suficientemente grande. Al caer el contador por debajo de la longitud del siguiente paquete de la cola, se detiene la transmisión hasta el siguiente pulso, en cuyo momento se sobrescribe el conteo de bytes residuales, perdiéndose. En la **figura 3.9** se ilustra este algoritmo:

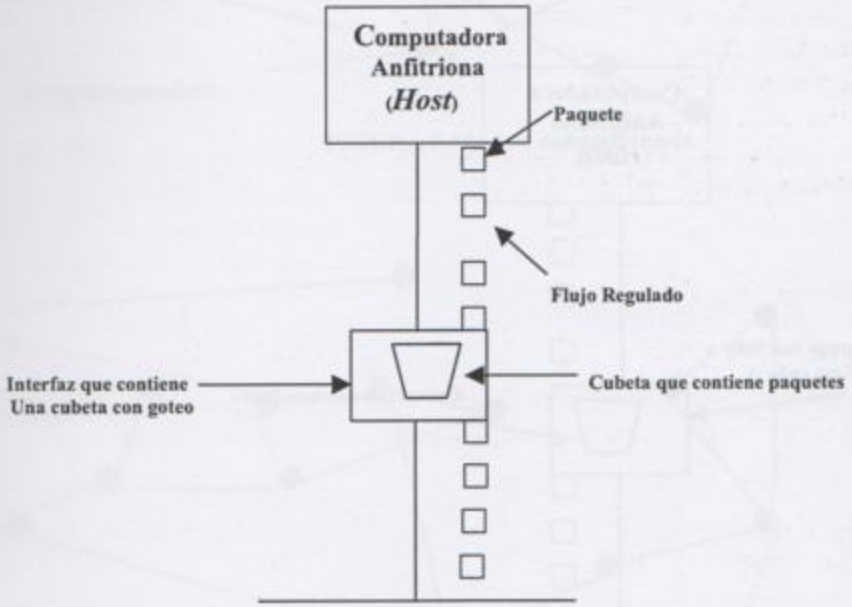


FIGURA 3.9: Algoritmo de Cubeta con Goteo.

3.11.2.2. Algoritmo de cubeta con ficha

El algoritmo de cubeta con goteo impone un patrón de salida rígido a la tasa promedio, sin importar la cantidad de ráfagas que tenga el tráfico. En muchas aplicaciones es mejor permitir que la salida se acelere un poco al llegar ráfagas grandes, por lo que se necesita un algoritmo más flexible, de preferencia uno que nunca pierda datos.

El algoritmo de cubeta con ficha, es uno de estos algoritmos. En este algoritmo, la cubeta con goteo contiene fichas, generadas por un reloj a razón de una ficha cada Δt *seg*. En la **figura 3.10** vemos una cubeta que contiene tres fichas, con cinco paquetes esperando ser transmitidos. Para transmitir un paquete, el transmisor debe capturar y destruir una ficha.

Este algoritmo ofrece una forma diferente de conformación del tráfico que el algoritmo de cubeta con goteo. Este último no permite que los *hosts* inactivos acumulen permisos para enviar posteriormente ráfagas grandes. El algoritmo de cubeta con fichas, sí permite el ahorro, hasta el tamaño máximo de la cubeta, *n*.

Otra diferencia entre los dos algoritmos, es que el algoritmo de cubeta con ficha descarta las ficha cuando la cubeta se llena, pero nunca descarta los paquetes. En contraste, el algoritmo de cubeta co goteo descarta los paquetes cuando las cubetas están llenas.

Los algoritmos de cubeta con goteo y cubeta con fichas pueden servir para regular el tráfico ent los enrutadores, de la misma manera en que se usan para regular la salida de un *host*.

La implementación del algoritmo básico de las cubetas con fichas simplemente es una variable que cuenta fichas. El contador se incrementa en uno cada ΔT y disminuye en uno cada vez que se env un paquete. Al llegar a cero el contador, ya no se puede enviar más paquetes. En la variante del conteo d bits, se incrementa el contador en k bytes cada ΔT y disminuye en la longitud de cada paquete enviado. E esencia lo que hace el algoritmo de cubeta con ficha, es permitir ráfagas a una longitud máxima regulada

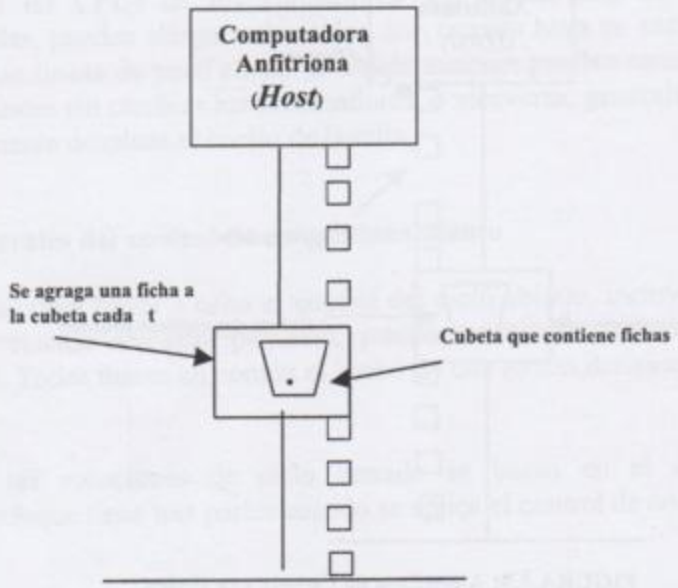


FIGURA 3.10: Algoritmo de Cubeta con Ficha.

3.11.2.3. Especificaciones de flujo

La conformación del tráfico es más efectiva cuando el transmisor, el receptor y la subred están d acuerdo. Para ponerse de acuerdo, es necesario especificar el patrón de tráfico de una manera precisa.

Tal arreglo se llama especificación de flujo, y consiste en una estructura de datos que describ tanto el patrón de tráfico interpolado como la cantidad de servicio deseado por las aplicaciones. Un especificación se puede aplicar tanto a los paquetes enviados por circuito virtual como a una secuencia d datagramas enviados entre un origen y un destino.

3.11.2.4. Control de congestionamiento en las subredes de circuitos virtuales

Unas de las técnicas que se usa ampliamente para evitar que empeoren los congestionamientos el control de admisión. La idea es sencilla: una vez que sea detectado el congestionamiento, no establecen circuitos virtuales nuevos hasta que haya desaparecido el problema.

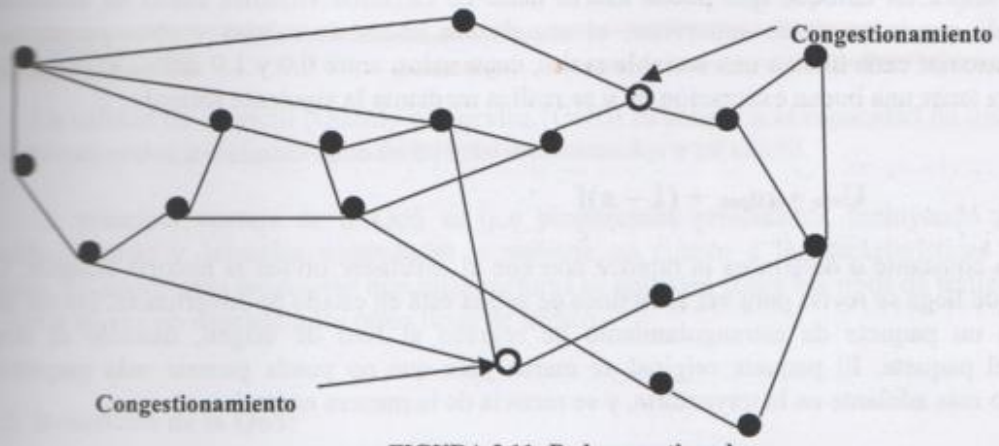


FIGURA 3.11: Red congestionada.

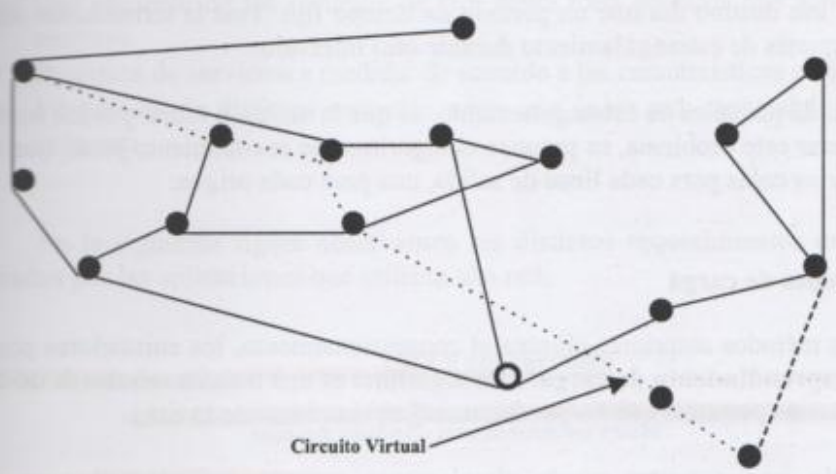


FIGURA 3.12: Circuito Virtual.

Un enfoque alternativo es permitir el establecimiento de nuevos circuitos virtuales, pero enrutando cuidadosamente dichos circuitos por otras rutas que no tienen problemas.

Otra estrategia que tiene que ver con los circuitos virtuales es negociar un acuerdo entre el *host* y la subred al establecer un circuito virtual. Este arreglo normalmente especifica el volumen y la forma del tráfico, la cantidad de servicio requerida y otros parámetros.

Para cumplir con su parte del acuerdo, la subred típicamente reserva servicios a lo largo de la trayectoria al establecerse el circuito. De esta manera es poco probable que ocurran congestionamientos en los circuitos virtuales nuevos porque está garantizada la disponibilidad de todos los servicios necesarios durante todo el tiempo. Una de las desventajas de hacerlo todo el tiempo es que se tiende a desperdiciar recursos

3.11.2.5. Paquetes de estrangulamiento

Veamos ahora un enfoque que puede usarse tanto en circuitos virtuales como en subredes de datagramas. Cada enrutador puede supervisar, el uso de sus líneas de salidas y otros recursos. Por ejemplo, puede asociar cada línea a una variable real *u*, cuyo valor, entre 0.0 y 1.0 refleja el uso reciente de esa línea. Para tener una buena estimación de *u* se realiza mediante la siguiente fórmula:

$$U_{nvo} = au_{ant} + (1 - a)f$$

Donde la constante *a* determina la rapidez con que el enrutador olvida la historia anterior. Cada paquete nuevo que llega se revisa para ver si su línea de salida está en estado de advertencia. De ser así, el enrutador envía un paquete de estrangulamiento de regreso al *host* de origen, dándole el destino encontrado en el paquete. El paquete original se marca para que no pueda generar más paquetes de estrangulamiento más adelante en la trayectoria, y se reenvía de la manera normal.

Al recibir el paquete de estrangulamiento, el *host* de origen está obligado a reducir el tráfico que envía al destino especificado en un X %. Dado que otros paquetes destinados al mismo lugar probablemente ya están encamino y generan nuevos paquetes de estrangulamiento, el *host* deberá ignorar los paquetes que se refieran a ese destino durante un período de tiempo fijo. Tras la terminación de ese período, el *host* espera más paquetes de estrangulamiento durante otro intervalo.

Un problema con el uso de paquetes de estrangulamiento, es que la acción a tomar por los *hosts* de origen es voluntaria. Para superar este problema, se propuso el algoritmo de encolamiento justo, que hace que los enrutadores, tengan varias colas para cada línea de salida, una para cada origen.

3.11.2.6. Desprendimiento de carga

Cuando ninguno de los métodos anteriores elimina el congestionamiento, los enrutadores pueden sacar la artillería pesada: el **desprendimiento de carga**. Este algoritmo es una manera rebuscada de decir que, al inundarse los enrutadores de paquetes que no pueden manejar, simplemente lo tiran.

El enrutador abrumado por paquetes puede simplemente escoger paquetes al azar para desprenderse de ellos, pero normalmente pueden hacer algo mejor. El paquete a descartar puede depender de las aplicaciones que se están ejecutando. En la transferencia de archivos vale más un paquete viejo que uno nuevo. En un archivo con 12 paquetes, deshacerse del paquete 6 podría requerir la retransmisión de los paquetes 7 al 12, y deshacerse del 10 podría requerir la retransmisión sólo del paquete 10 al 12.

Para poner en práctica una política inteligente de desprendimiento, las aplicaciones deben marcar sus paquetes con clases de prioridades para indicar su importancia.

Otra opción es permitir que los *hosts* excedan los límites especificados en el acuerdo negociado al establecer el circuito virtual, pero sujetos a la condición de que el exceso de tráfico se marque con prioridad baja. Tal estrategia no es mala, porque hace uso más eficiente de los recursos ociosos, permitiendo a los *hosts* su uso siempre y cuando nadie más esté interesado, pero sin establecer un derecho sobre ellos cuando los tiempos se vuelven difíciles.

3.12. Calidad de Servicio en Redes

3.12.1. Introducción

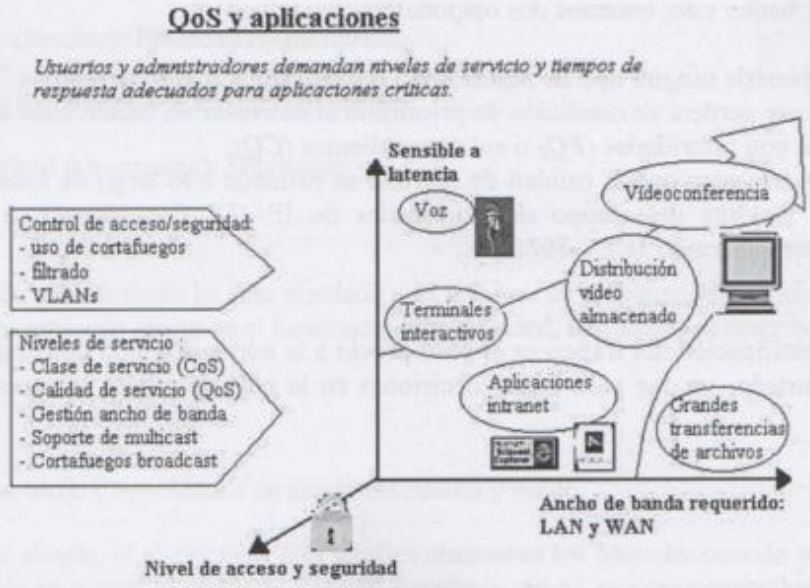
La calidad de servicio (Quality of Service (QoS)) se refiere a la capacidad de una red de proveer servicios mejorados a distintos tipos de tráfico, seleccionados a tal efecto.

La principal ventaja de la QoS es que proporciona prioridades, incluyendo ancho de banda dedicado, retardo y latencias controladas y mejoras en cuanto a las características de pérdidas de paquetes. Es importante asegurarse que estas mejoras se apliquen sobre los tipos de tráfico seleccionados, pero que a su vez no degrade a los otros tipos de tráfico

3.12.2. Beneficios de la QoS:

- Control sobre los recursos de red: ancho de banda, facilidades de acceso WAN, servidores, bases de datos, etc.
- Uso eficiente de los recursos de red: sobre todo aquellos que son críticos para la misión de la empresa.
- Provisión de servicios a medida: de acuerdo a las características solicitadas por los clientes.
- Integración de distintos servicios sobre una única red: respetando las características propias de cada uno.

En la siguiente figura observamos los distintos requerimientos que poseen los flujos de datos generados por las aplicaciones que utilizan una red:



3.12.3. Arquitectura básica de la QoS

Fundamentalmente la QoS se obtiene priorizando un flujo de determinado tráfico sobre otros flujos, los cuales en caso de congestión en un nodo, son atendidos con diferentes políticas durante su estancia en las colas de espera.

Esto se puede lograr con diferentes herramientas; la tarea de la gestión de la QoS es seleccionar las apropiadas para cada caso en particular, ya que algunas se adaptan mejor que otras a determinados tipos de tráficos

No obstante existen otras acciones que mejoran el desempeño final de la red, y por lo tanto mejoran la calidad percibida por los usuarios de la red.

La arquitectura de la QoS consta de tres piezas básicas:

a) Identificación de los tipos de tráfico y coordinación de los elementos de red que intervengan en la determinación de una QoS de extremo a extremo
b) Definición de los elementos de QoS (programación de tareas en una cola de espera, política de servicio en dicha cola, herramientas de tráfico, etc)
c) Control, gestión y medición de las características dinámicas del tráfico de extremo a extremo.

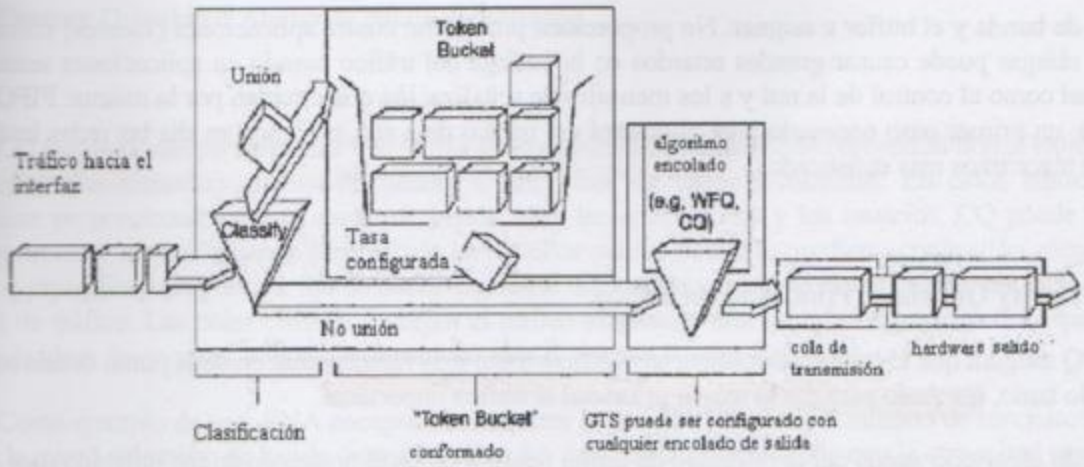
a) Identificación y marcado de los tipos de tráfico para QoS

Para proveer servicio preferencial a determinado tipo de tráfico primero hay que identificarlo, diferenciándolo del resto. Algunas de las herramientas que tenemos son las listas de control de acceso (ACL), el enrutamiento basado en políticas, etc.

Una vez hecho esto, tenemos dos opciones:

1. No ponerle ningún tipo de marca extra (clasificación que se denomina "de un salto") ya que el paquete perderá su condición de prioritario al atravesar un router. Esto se da cuando se utilizan colas con prioridades ***(PQ)*** o colas por clientes ***(CQ)***.
2. Marcarlo para que la calidad de servicio se extienda a lo largo de toda la red. Esto se realiza con los bits del campo de prioridades de IP ***(IP Precedence)***, o con los mecanismos contemplados en **IEEE 802.1p**

Esta identificación del tráfico es el paso previo a la administración de congestión que veremos en el siguiente apartado, ya que para tomar decisiones en la cola de espera se necesita que el tráfico esté marcado.



b) Administración de la Congestión

Debido a la naturaleza a ráfagas del tráfico de voz, video o datos, éste a menudo excede la capacidad del enlace. El router tiene dos alternativas a adoptar:

a) Almacenar todo el tráfico en una sola cola de espera e ir despachándolo en la medida que lo permita el enlace con la política de FIFO, o
b) Almacenar los paquetes en diferentes colas de espera y tratar a cada una en forma distinta, según las distintas herramientas de administración de colas

Detallaremos algunas de ellas:

1. FIFO (First-in, First-out): Primero en entrar, primero en salir de la cola.
2. PQ (Priority Queuing): Prioridad encolamiento.
3. CQ (Custom Queuing): A la medida del cliente.
4. WFQ (Weighted fair queuing): Ponderado.

Cada algoritmo de encolamiento ha sido diseñado para resolver un problema específico del tráfico de la red, obteniendo así un determinado efecto en el funcionamiento de la red, tal y como se describe en cada uno de ellos.

1. FIFO (First-in, First-out): Capacidades de almacenamiento y envío.

En su forma más simple, el algoritmo FIFO implica almacenar los paquetes cuando se congestiona la red y expedirlos, teniendo en cuenta el orden de llegada, cuando la red no está tan congestionada. FIFO es el algoritmo por defecto, por lo que no requiere ninguna configuración, sin embargo tiene varios defectos. El más importante es que no toma decisiones sobre la prioridad de los paquetes, es el orden de llegada el que determina

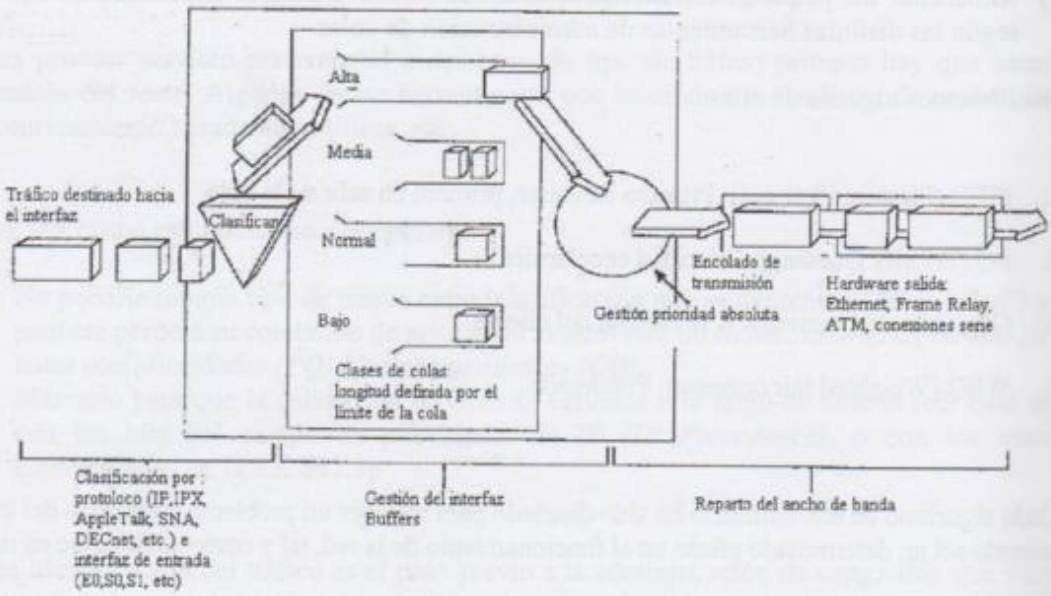
el ancho de banda y el buffer a asignar. No proporciona protección contra aplicaciones (fuentes) corruptas. El tráfico a ráfagas puede causar grandes retardos en la entrega del tráfico basado en aplicaciones sensibles a l tiempo, así como al control de la red y a los mensajes de señalización que circulan por la misma. FIFO fue, en definitiva, un primer paso necesario para el control del tráfico de a red, pero hoy en día las redes inteligentes necesitan algoritmos más sofisticados.

2. PQ (Priority Queuing): Priorizando el tráfico.

PQ asegura que el tráfico importante sea administrado más rápidamente en cada punto donde se utilice. Fue, por lo tanto, diseñado para dar la mayor prioridad al tráfico importante.

Este algoritmo puede dar la prioridad de forma flexible según el protocolo de red utilizado (por ejemplo IP, IPX, o AppleTalk), el interfaz entrante, el tamaño del paquete, la dirección fuente y/o destino, y mucho más.

En PQ cada paquete es colocado en una de las cuatro colas de prioridad –alta, media, normal, baja- basándose en la prioridad ya asignada, asignándose prioridad normal para aquellos paquetes que no tengan ninguna prioridad asignada, tal y como se puede ver en la figura posterior. Como vemos, durante la transmisión el algoritmo concede un tratamiento preferencial a las colas de mayor prioridad sobre las de menor prioridad.



Algoritmo PQ. Encolamiento basado en prioridad de paquetes.

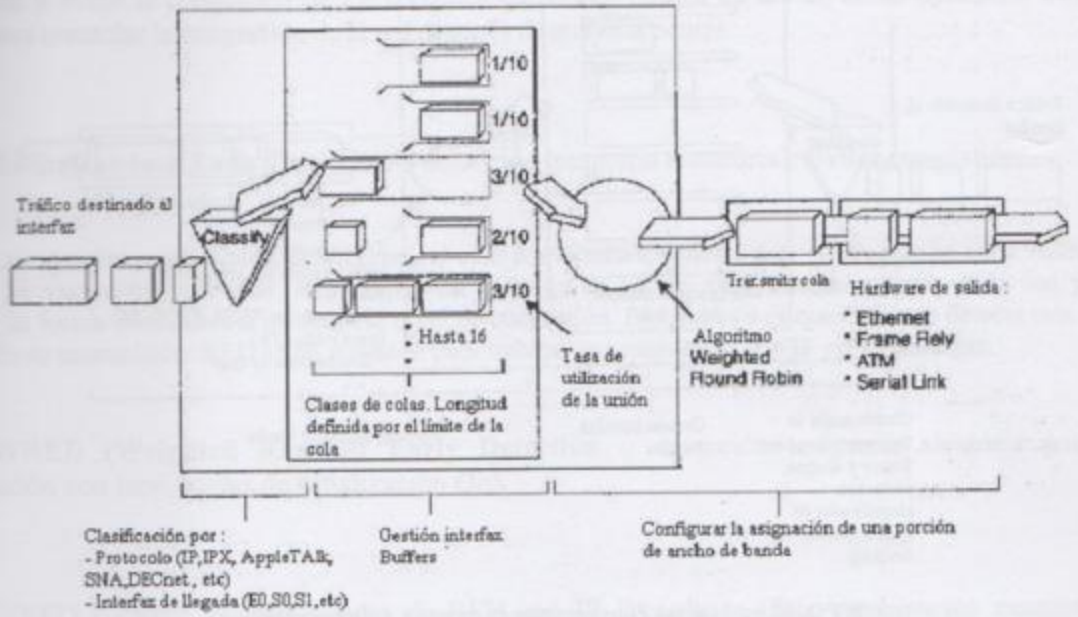
PQ es útil para cerciorarse de que el tráfico que atraviesa varias conexiones WAN y es considerado crítico consiga un tratamiento prioritario.

Actualmente, además, este algoritmo usa una configuración estática, no adaptándose así automáticamente a los requisitos cambiantes de las redes.

CQ (Custom Queuing): Ancho de banda garantizado

CQ fue diseñado para permitir que varias aplicaciones u organizaciones compartan la red, entre aquellas aplicaciones que necesiten anchos de bandas o requisitos de latencia mínimos. En estos entornos debe compartirse proporcionalmente el ancho de banda entre las aplicaciones y los usuarios. CQ puede utilizarse para proporcionar ancho de banda garantizado en aquellos puntos donde se produzca congestión, asegurando a un tráfico específico una porción fija de ancho de banda disponible y dejando el tráfico restante para cualquier otro tipo de tráfico. Las colas clientes manejan el tráfico asignando una cantidad específica del espacio de la cola a cada clase de paquete, aplicando posteriormente el sistema Round-Robin.

Como ejemplo de uso, SNA encapsulado requiere la garantía de un nivel mínimo de servicio. Se podría reservar la mitad del ancho de banda disponible para los datos SNA, permitiendo que la otra mitad sea utilizada por otros protocolos como IP e IPX.



Algoritmo CQ. Maneja el tráfico asignando una cantidad específica de espacio de la cola a cada clase de paquetes y sirviéndolas hacia 17 colas aplicando Round-Robin.

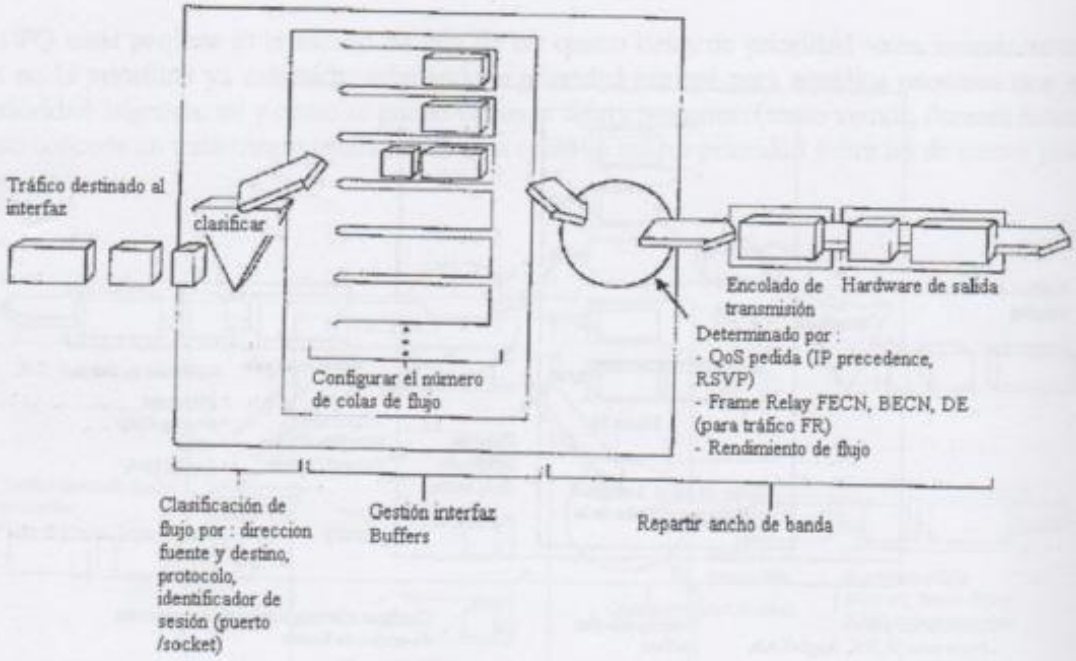
El algoritmo de encolamiento coloca los mensajes en una de las 17 colas (la cola 0 se utilizada para almacenar mensajes de sistema como mantenimiento, señalización, etc.) y se vacía con prioridad pesada. Los servicios de encaminamiento van desde la cola 1 a la 16 según el orden asignado por Round-Robin, desencolando un byte de cada cola por cada ciclo.

Esto asegura que ninguna aplicación (o grupo de aplicaciones) logre una mayor proporción de capacidad global cuando la línea se encuentre bajo presión. Como PQ, CQ se configura estáticamente y no se adapta automáticamente a las condiciones cambiantes de las redes.

4. WFQ (Weighted fair queuing): Algoritmo para redes inteligentes

Para situaciones en las que es deseable proporcionar un tiempo de respuesta consistente a cualquier tipo de usuarios sin necesidad de aumentar el ancho de banda de forma excesiva, entonces la solución es WFQ. Es un algoritmo de encolamiento basado en el flujo que realiza dos tareas simultáneamente: situa el tráfico interactivo a principio de la cola para reducir el tiempo de respuesta y permite así compartir el resto del ancho de banda entre flujos que requieren gran ancho de banda.

WFQ asegura que las colas no se quedarán sin ancho de banda, proporcionando a ese tráfico un servicio predecible. Así mismo, las ráfagas de tráfico de bajo volumen –la mayoría del tráfico- reciben servicio preferencial, transmitiéndolas rápidamente. Las ráfagas de tráfico de gran volumen compartirán la capacidad restante de forma proporcional entre ellos, como muestra la siguiente figura.



WFQ. Si hay varias conversaciones de gran volumen activas sus velocidades de transferencia y periodos entre llegadas se hacen más predecibles.

WFQ ha sido diseñado para minimizar en esfuerzos al configurar, adaptándose automáticamente a las condiciones cambiantes del tráfico de la red.

WFQ es eficaz pues permite que se pueda asignar cualquier cantidad de ancho de banda para flujos de tráfico de baja prioridad si no está presente ningún flujo de alta prioridad. Esto es diferente del multiplexado por división en el tiempo (TDM) que simplemente mide el ancho de banda y permite que este no se utilice si no está presente un determinado tipo de tráfico. WFQ, además, trabaja con las técnicas IP Precedence y RSVP para proporcionar QoS diferenciada así como servicios garantizados.

Este algoritmo también trata el problema de la variabilidad del atraso durante la transmisión. Si hay múltiples conversaciones de alto volumen activas, sus tasas de transferencia, así como sus periodos de llegada se hacen más predecibles. WFQ refuerza algoritmos como el SNA Control de Enlace Lógico (LLC) y el control

de congestión del Protocolo de Control de Transmisión (TCP), obteniendo como resultado una expedición y un tiempo de respuesta más predecible para cada uno de los flujos activos, tal y como muestran las siguientes gráficas.

Gestión de las colas de espera

Debido a que el tamaño de una cola de espera no es infinito, ésta se puede llegar a saturar y con ello, desbordar. Esto significa que cualquier paquete extra que llegue será desechado, incluso si es un paquete de alta prioridad de servicio. Para que esto no suceda tenemos dos opciones:

a) Asegurarnos que la cola tenga un tamaño suficiente como para que no se sature nunca
b) Intentar una detección temprana de la saturación para desechar antes los paquetes de baja prioridad que los de alta prioridad. Esto se conoce como Weighted early random detect (WRED)

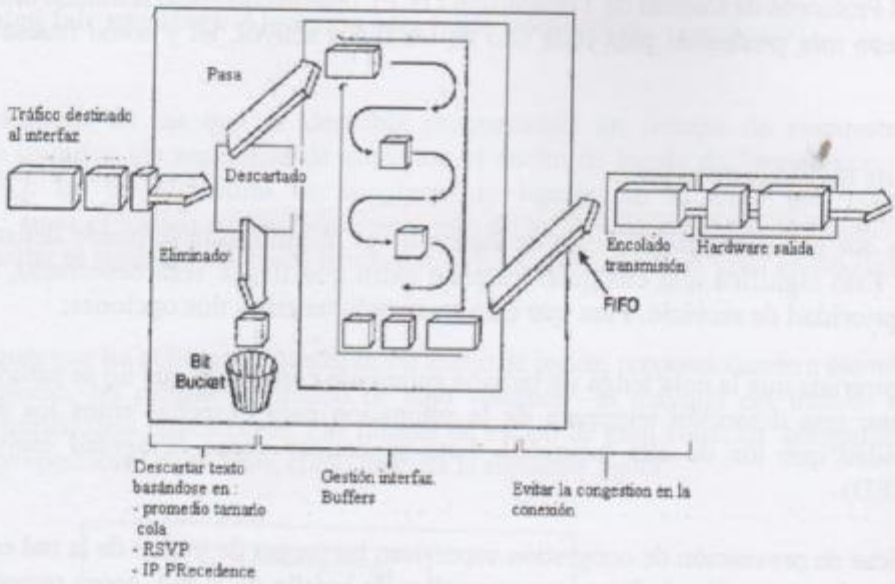
Las técnicas de prevención de congestión supervisan las cargas de tráfico de la red en un esfuerzo por anticiparse y evitar la congestión de los comunes cuellos de botella de la red, como opuesto a técnicas que operan para controlar la congestión de la red después de que esta ocurre.

RED (Random Early Detection o detección temprana aleatroria): Evitar congestión.

Los algoritmos de detección temprana al azar son diseñados para evitar la congestión entre redes antes de que esta se vuelva un problema. RED supervisa la carga de tráfico en diferentes puntos de la red y descarta paquetes de forma estocástica si aumenta el nivel de congestión. El resultado es que la fuente detecta esta situación, retardando su transmisión. RED se ha diseñado para trabajar en entornos TCP e IP principalmente.

WRED (Weighted Random Early Detection o detección temprana aleatoria ponderada): Cooperación con tecnologías de señalización QoS

WRED combina las capacidades de RED con IP Precedence. Esta combinación mantiene tráfico preferencial que maneja como paquetes de prioridad más altos. Puede selectivamente desechar el tráfico de menor prioridad cuando el interfaz empieza a congestionarse y proporciona características de gestión distintas para las diferentes clases de servicio. Pero WRED también permite RSVP, ofreciendo servicios integrados de QoS de carga controlada.



WRED proporciona un método que descarta estocásticamente paquetes si la congestión aumenta.

Eficiencia del enlace

Algunas veces es problemática la demora introducida por la serialización de los paquetes en la interfaz de salida. Por ejemplo para una aplicación de voz que deba esperar a que un paquete de 1500 Bytes salga por una línea de 56 kbps, la demora sería:

Packet size:	1500-Bytes × 8 bits/Byte = 12,000 bits
Line rate:	56,000 bps
Resultado:	12,000 bits/56,000bps = 0.214 sec o 214 mseg.

¡Algo inadmisible para la aplicación de voz ...! Incluso antes de que el paquete deje el router

Para mejorar esto podemos fragmentar el paquete más grande e intercalar un paquete de voz con uno de datos, logrando así que la demora en la serialización se minimice para el paquete de voz.

3.12.4. Gestión de la QoS

La gestión de la QoS se desarrolla en las siguientes etapas:

- Paso 1: se trazan las características del tráfico en la red y se determinan las condiciones ideales de QoS
- Paso 2: Se implementan las técnicas de gestión para los tipos de tráfico y las condiciones ideales determinadas en el paso anterior
- Paso 3: se evalúan los resultados, para verificar si se obtienen las respuestas esperadas

EJERCICIOS SOBRE DIRECCIONAMIENTO IP

Ejercicios propuestos

1) Decir que tipo de direcciones son (A, B o C)

3.3.3.3
230.23.2.1
100.1.1.1
190.2.234.210
210.0.0.1
90.4.3.2

2.1). Decir de a que clase pertenecen las siguientes direcciones

131.12.12.5
8.1.1.6
4.15.2.2

2.2) ¿Cuál es la mascara de subred por defecto para cada clase?

3) Indicar de estos números IP cuales pertenecen a las mismas redes

140.128.200.1
150.128.300.3
140.128.200.255
140.129.250.1
140.128.190.221
140.128.30.30
140.128.120.120
140.128.60.1

con las siguientes subredes:

255.255.255.192
255.255.192.0
255.255.248.0

4) Si tenemos una dirección de clase C, y 200 hosts separados en 3 redes, ¿cuál seria una mascara de subred apropiada para implementar?

5) ¿Cuál es la máscara más apropiada para implementar en un enlace serial?

6) Indicar cuál de las siguientes direcciones IP corresponden a una red dividida en subredes con 62 host en cada una:
213.45.45.33
200.10.0.128
215.14.97.129
198.0.45.77

Ejercicios Resueltos

1.-A que clase de red pertenecen las siguientes direcciones?
Indique si es posible que parte de la dirección es de red y que parte de host.

202 . 100 . 35 . 21	Clase C
191 . 146 . 201 . 120	Clase B
10 . 8 . 1 . 100	Clase A (Privada)

2.-Dar los 3 primeros bits del primer octeto de una dirección IP de una red clase "C". 110

Dar los 2 primeros bits del primer octeto de una dirección IP de una red clase "B". 10

Dar todos los bits del primer octeto del máximo número de red que puede tener una red clase "A".
01111111

3.-Completar la siguiente tabla para una red clase "B"

Cantidad de bits tomados prestados		Cantidad de subredes utilizables	Cantidad de hosts utilizables en c/u de las subredes	Cant. TOTAL de hosts utilizables
0	255.255.0.0	---------	---------	65534
1	255.255.128.0	---------	---------	65534
2	255.255.192.0	2	16382	32764
3	255.255.224.0	6	8190	49140
4	255.255.240.0	14	4094	57316
5	255.255.248.0	30	2046	61380
6	255.255.252.0	62	1022	63364
7	255.255.254.0	128	510	65280
8	255.255.255.0	254	254	64516
9	255.255.255.128	510	126	64260
10	255.255.255.192	1022	62	63364
11	255.255.255.224	2046	30	61380

12	255.255.255.240	4094	14	57316
13	255.255.255.248	8190	6	49140
14	255.255.255.252	16382	4	65528
15	255.255.255.254	---------	---------	---------
16	255.255.255.255	---------	---------	---------

4.-Decir si es posible cuantos hosts podrá haber en c/u de las subredes para c/u de las siguientes máscaras y/o cuantas subredes se podrán tener:

255 . 255 . 240 . 0 No es posible, ya que no sabemos la clase

255 . 240 . 0 . 0 14 subredes de 1.048.574 hosts c/u

255 . 255 . 255 . 240 No es posible, ya que no sabemos la clase

5.-Sabiendo que las siguientes son direcciones de subredes, decir cual es la cantidad mínima de bits que se tomaron prestados.

114 . 200 . 1 . 0 16 bits

114. 208 . 2 . 0 15 bits

114. 1 . 3 . 0 16 bits

114. 0 . 4 . 0 14 bits

Unidad 4

Capa de transporte (TCP)

Capa de Aplicación

Internet

Objetivos

- Describir el funcionamiento de los protocolos TCP y del UDP y sus principales aplicaciones
- Explicar la Internet y los servicios que ella brinda
- Describir el funcionamiento de la transferencia y acceso de archivos en una red de computadoras.
- Estudiar el concepto de servidor de nombres de dominio (DNS). y cómo funciona.
- Especificar qué es el correo electrónico, e-mail, conocer sus características principales.
- Explicar qué es la WWW (*Worl Wide Web*), el lado del cliente, el lado del servidor y protocolo que utiliza.
- Explicar qué se entiende por gestión de redes
- Describir el funcionamiento del protocolo simple de administración de redes (SNMP)
- Desarrollar las aplicaciones de una red IP para el transporte de diversos servicios (Voz, datos, video)
- Analizar los inconvenientes que ello presenta y los criterios para dar respuesta a dichos inconvenientes (QoS)

4.1. Internet

Internet puede ser definida como una **red de redes de computadoras de alcance mundial**. Las redes de computadoras que se encuentran interconectadas van desde grandes instalaciones gubernamentales hasta redes universitarias; las que mantienen las organizaciones sin fines de lucro, y las de las corporaciones.

Internet nació en 1969 como un proyecto de la Agencia de Proyectos de Investigación de Defensa Avanzados de EEUU (DARPA). La base del proyecto era la necesidad de intercambio informativo entre los investigadores y científicos militares, ubicados en sitios apartados. Esta red, llamada Arpanet, fue construida para estudiar técnicas para la provisión de comunicación robusta y segura independiente de los proveedores.

En 1975, la Arpanet fue convertida desde una red experimental a una red operacional y la responsabilidad de administración fue dada a la DCA (Agencia de Comunicaciones de Defensa), cuyo nombre fue cambiado luego por DISA (Agencia de Sistemas de Información de Defensa).

El protocolo básico TCP/IP fue desarrollado después que la red se transformó en operacional. Éste fue adoptado como estándar militar en 1983. En este año la Arpanet fue dividida en Milnet, la parte clasificada de la Red de Defensa (DDN) y una Arpanet más pequeña. El término Internet fue usado para referirse a la red completa, Milnet más Arpanet. En 1990, la Arpanet dejó de existir formalmente, pero actualmente **Internet** es más grande y comprende redes en todo el mundo.

Como ya se vio, el término red significa dos o más computadoras conectadas entre sí. Si bien existen muchas razones para conectar dos o más computadoras, desde el punto de vista de **Internet** tenemos:

- Permitir que las personas se comuniquen.
- Compartir recursos.

En cuanto al primer punto, se pueden mantener mensajes con otras personas que usan redes conectadas a Internet. En cuanto al segundo, en Internet se comparten recursos de información más que dispositivos de *hardware*.

El hilo común que enlaza la enorme **Internet** es el *software* de red **TCP/IP**. Éste es un grupo de protocolos de comunicación que define cómo los diferentes tipos de computadores hablan entre sí. Este conjunto lleva el nombre de dos de los principales protocolos: **TCP (Protocolo de Control de Transmisión)** y el **IP (Protocolo de Internet)**. No obstante a ello, existen en este grupo muchos otros protocolos.

¿Qué significa estar en Internet?

Una máquina está en Internet si opera con la pila de protocolos de TCP/IP, tiene una dirección de IP y es capaz de enviar paquetes de IP a todas las demás máquinas de Internet. La mera capacidad de enviar y recibir correo electrónico no es suficiente, pues éste se distribuye a muchas redes fuera de Internet. Sin embargo, el asunto pierde claridad en cierta forma por el hecho de que muchas

computadoras personales tienen la capacidad de llamar a un proveedor de servicios de Internet mediante un módem, recibir la asignación de una dirección IP temporal y enviar paquetes IP a otras *hosts* de Internet. Tiene sentido considerar que tales máquinas están en Internet mientras están conectadas al enrutador del proveedor de servicio.

4.1.1. Tipos de acceso

4.1.1.1. Protocolo SLIP (IP de Línea en Serie)

Es el más viejo de los protocolos; fue diseñado en 1984 para conectar estaciones de trabajo *Sun* a Internet a través de una línea de discado usando un módem. Es muy sencillo, la estación sólo envía paquetes IP en bruto a través de la línea, con un byte indicador especial (0xC0) al final para delimitar el marco. Si el byte indicador ocurre dentro del paquete IP, se usa una forma de relleno de caracteres, enviándose la secuencia de dos bytes (0xDB, 0xDC) en su lugar. Si ocurre 0XDB dentro del paquete IP, también se rellena. Algunas implementaciones de SLIP agregan un byte indicador tanto al principio como al final de cada paquete IP enviado.

Las versiones más recientes efectúan cierta compresión de encabezados TCP e IP. Lo que hacen es aprovechar el hecho de que los paquetes consecutivos con frecuencia tienen muchos campos de encabezado en común; se comprimen omitiendo aquellos campos que son iguales a los campos correspondientes del paquete IP previo. Es más, los campos que sí difieren no son enviados en su totalidad, sino como incrementos del valor previo.

NO CONGESTIONA LA RED.

Aunque aun se utiliza ampliamente, SLIP tiene algunos problemas serios:

MIENTRAS MAS ABAJO SE DETECTE LA FALLA, MEJOR.

- Primero, SLIP no efectúa detección o corrección de errores, por lo que es responsabilidad de las capas superiores detectar y recuperar marcos perdidos, dañados o fusionados.

- Segundo, SLIP no reconoce IP. Con el crecimiento de Internet para abarcar redes que no usan IP como su lenguaje nativo (por ejemplo, las LAN Novell), esta restricción se vuelve cada vez más grave.

  JUNTA PAQUETES // NO DETECTA

- Tercero, cada lado debe conocer por adelantado la dirección IP del otro; ninguna de las dos direcciones puede asignarse dinámicamente durante el establecimiento del enlace. Dada la escasez actual de direcciones IP, esta limitación es un problema importante, pues es imposible dar a cada usuario casero de Internet una dirección única de IP.

- Cuarto, SLIP no proporciona ninguna forma de verificación de autenticidad, por lo que ninguna parte sabe realmente con quién está hablando. Con líneas arrendadas éste no es un problema, pero con líneas de discado sí lo es.

- Quinto, SLIP no un estándar aprobado de Internet, por lo que existen muchas versiones diferentes (e incompatibles). Esta situación no simplifica la interconexión.

4.1.1.2. Protocolo PPP (Protocolo Punto a Punto)

Para mejorar la situación, se estableció un protocolo de enlace de datos para líneas punto a punto que resolviera todos estos problemas y que pudiera volverse un estándar oficial de Internet.

El PPP realiza detección de errores, reconoce múltiples protocolos, permite la negociación de direcciones de IP en el momento de la conexión, permite la verificación de autenticidad (a trav´ces de los protocolos PAP y CHAP) y tiene muchas mejoras respecto a SLIP. Aunque muchos proveedores de servicios de Internet aun reconocen tanto SLIP como PPP, el futuro claramente está en PPP, no sólo en las líneas por discado sino también en las líneas arrendadas de enrutador a enrutador.

PPP proporciona tres cosas:

- Un método de enmarcado que delinea sin ambigüedades el final de un marco y el inicio del siguiente. El formato de marco también maneja la detección de errores.
- Un protocolo de control de enlace para activar líneas, probarlas, negociar opciones y desactivarlas ordenadamente cuando ya no son necesarias. Este protocolo se llama **LCP (Protocolo de Control de Enlace)**.
- Un mecanismo para negociar opciones de capa de red con independencia del protocolo de red usado. El método escogido consiste en tener un **NCP (Protocolo de Control de Red)** distinto para cada capa de red reconocida.

El formato de marco de PPP se escogió de modo que fuera muy parecido al formato de marco de HDLC. (Ver **figura 4.1**) La diferencia principal entre ellos es que el primero está orientado a caracteres, no a bits. En particular, PPP, como SLIP, usa el relleno de caracteres en las líneas por discado con módem. Por lo que los marcos tienen un número entero de bytes.

Byte	1	1	1	1 o 2	Variable	2	1
	Indicador 01111110	Dirección 11111111	Control 00000011	Protocolo	Carga útil	CRC	Indicador 01111110

FIGURA 4.1: Formato de marco completo PPP para el modo operación sin numeración.

Todos los marcos PPP comienzan con el byte **indicador** estándar de HDLC (01111110), que se rellena si ocurre dentro del campo carga útil. Luego viene el campo de **dirección**, al que siempre se le asigna el valor binario 11111111 para indicar que todas las estaciones deben aceptar el marco. El empleo de este valor evita tener que asignar direcciones de enlace de datos.

Este campo ve seguido del campo de **control**, cuyo valor predeterminado es 00000011. Este valor indica un marco sin número. En otras palabras, PPP no proporciona por omisión transmisión confiable usando números de secuencia y acuses. En ambientes ruidosos, como los de las redes inalámbricas, se puede usar el modo numerado para transmisión confiable.

Dado que los campos de **dirección** y **control** son constantes en la configuración predeterminada, LCP proporciona los mecanismos necesarios para que las dos partes negocien una opción que simplemente los omita por completo y ahorre dos bytes por marco.

La tarea del campo **protocolo** es indicar la clase de paquete que está en el campo de **carga**. Se definen códigos para LCP, NCP, IP, IPX, Apple Talk y otros protocolos. Los protocolos que comienzan con un bit 0 son protocolos de capa de red. Los que comienzan con un bit 1 se usan para negociar otros protocolos. El tamaño por omisión del campo de **protocolo** es de 2 bytes, pero puede negociarse su disminución a 1 byte usando LCP.

El campo de **carga útil** es de longitud variable, hasta algún máximo negociado. Si la longitud no se negocia con LCP durante el establecimiento de la línea, se usa una longitud predeterminada de 1500 bytes. De ser necesario se puede incluir un relleno después de la carga.

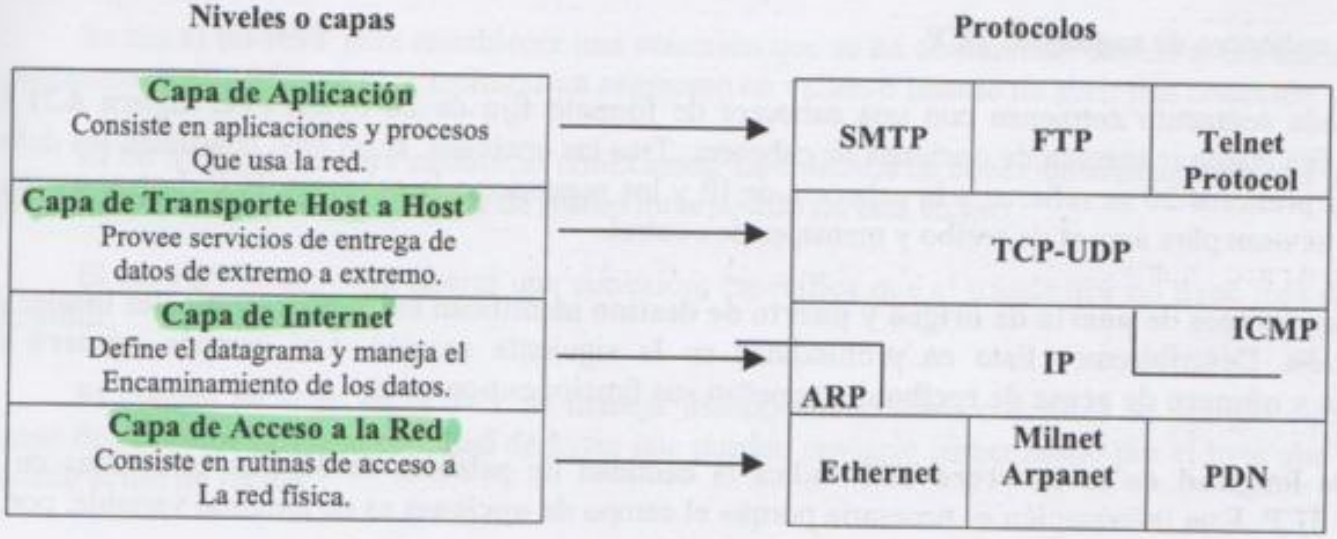
Luego se encuentra el campo **suma de comprobación**, que normalmente es de 2 bytes, pero puede negociarse una suma de comprobación de 4 bytes.

En resumen, PPP es un mecanismo de enmarcado multiprotocolo adecuado para usarse a través de módems, líneas de serie de bits HDLC, SONET y otras capas físicas. Maneja detección de errores, negociación de errores, compresión de encabezados y, opcionalmente, transmisión confiable con marcos HDLC.

4.1.3. Arquitectura de Internet

Ésta está basada sobre una visión de comunicaciones que involucra tres agentes: **procesos, hosts y redes**. Los procesos son las entidades fundamentales que se comunican. Un ejemplo es una operación de transferencia de archivos. Los procesos se ejecutan sobre los *hosts*, los cuales a menudo pueden soportar procesos múltiples simultáneos.

Los *hosts* son conectados por redes y los datos a ser intercambiados son transmitidos por la red desde uno a otro *host*. (Ver **figura 4.2**)



SMTP: Protocolo Simple de Transferencia de Correo.
FTP: Protocolo de Transferencia de Archivos.
UDP: Protocolo de Usuario de Datagrama.
ARP: Protocolo de Resolución de Dirección.
ICMP: Protocolo de Control de Mensajes de Internet.

FIGURA 4.2: Niveles y sus protocolos.

4.2. Protocolo TCP (Protocolo de Control de Transporte)

De los dos protocolos de la capa de transporte, el protocolo TCP proporciona un servicio de comunicación que forma un circuito, es decir, que el flujo de datos entre el origen y el destino parece que sea continuo. TCP proporciona un circuito virtual el cual es llamado una conexión.

Al contrario que los programas que utilizan UDP, los que utilizan el TCP tienen un servicio de conexión entre los programas llamados y los que llaman, chequeo de errores, control de flujo y capacidad de interrupción.

La entidad TCP transmisora y receptora intercambian datos en forma de segmentos. Un **segmento** consiste en una cabecera TCP fija de 20 bytes (más una parte opcional) seguida de cero o más bytes de datos.

El *software* de TCP decide el tamaño de los segmentos: puede acumular datos de varias escrituras para formar un segmento, o dividir los datos de una escritura en varios segmentos. Un segmento demasiado grande para transitar por una red puede dividirse en varios segmentos mediante un enrutador. Cada segmento nuevo recibe sus propias cabeceras TCP e IP, por lo que la fragmentación en los enrutadores aumenta la carga extra total.

El protocolo básico usado por las entidades TCP es el **protocolo de ventana corrediza**. Cuando un transmisor envía un segmento, también inicia un temporizador. Cuando llega el segmento a destino, la entidad TCP receptora devuelve un segmento (con datos, si existen, de otro modo sin ellos) que contiene un número de acuse de recibo igual al siguiente número de secuencia que espera recibir.

Si el temporizador del transmisor expira antes de la recepción del acuse de recibo, el transmisor envía de nuevo el segmento.

4.2.1. La cabecera de segmento TCP

Cada segmento comienza con una cabecera de formato fijo de 20 bytes. (Ver **figura 4.2**) La cabecera fija puede ir seguida de opciones de cabecera. Tras las opciones, si las hay, continúan los datos, donde los primeros 20 se refieren a la cabecera de IP y los segundos a la cabecera TCP. Los segmentos sin datos se usan para acuses de recibo y mensajes de control.

Los campos de **puerto de origen** y **puerto de destino** identifican los puntos terminales locales de la conexión. Describiremos Esto en profundidad en la siguiente sección. Los campos **número de secuencia** y **número de acuse de recibo** desempeñan sus funciones normales.

La **longitud de la cabecera** TCP indica la cantidad de palabras de 32 bits contenidas en la cabecera TCP. Esta información es necesaria porque el campo de **opciones** es de longitud variable, por lo que la cabecera también.

A continuación viene un campo de 6 bits que no se usa. Luego vienen seis banderas de 1 bit.

El **apuntador urgente (URG)** sirve para indicar un desplazamiento en bytes a partir del número actual de secuencia en el que se encuentran datos urgentes. El bit **ACK** se establece en 1 para indicar que el **número de acuse de recibo** es válido. Si el **ACK** es 0, no contiene un acuse de recibo.

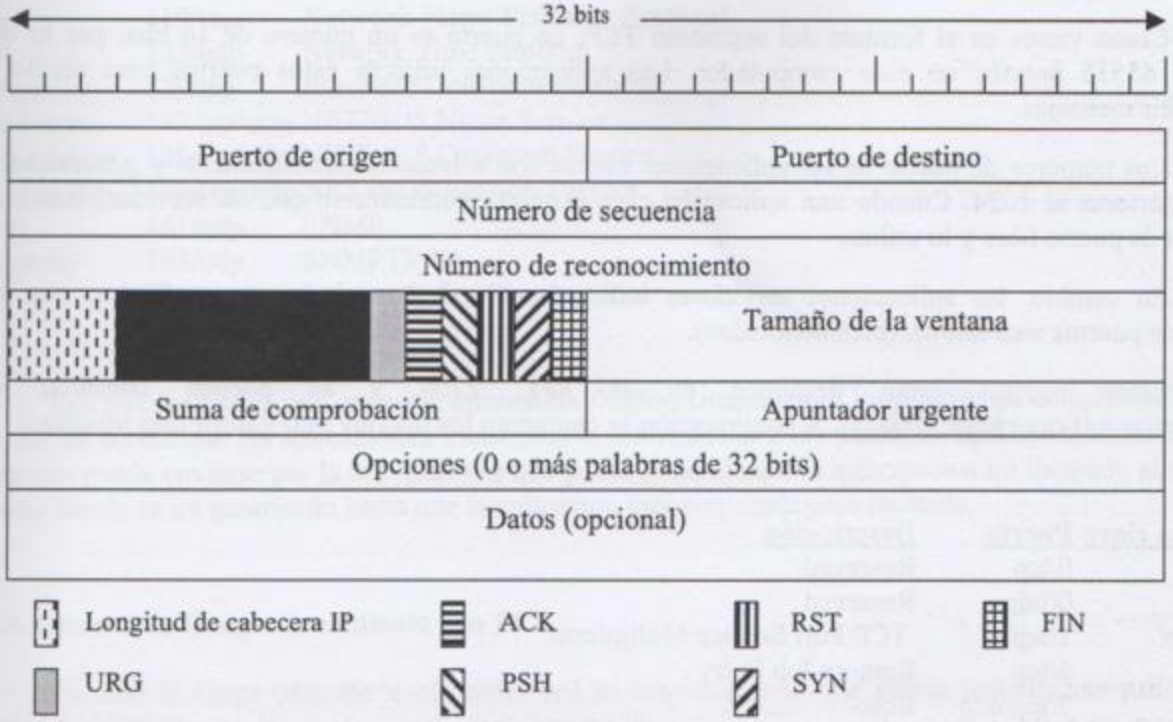


FIGURA 5.64: Cabecera de TCP.

El bit **PSH** indica datos empujados. Por este medio se solicita atentamente al receptor entregar los datos a la aplicación a su llegada y no ponerlos en *buffer* hasta la recepción de un *buffer* completo.

Se usa el bit **RST** para restablecer una conexión que se ha confundido debido a una caída de *host* u otra razón; también sirve para rechazar un segmento no válido o intento de abrir una conexión.

El bit **SYN** se usa para establecer conexiones. La solicitud de conexiones tiene SYN = 1 y ACK = 0 para indicar que el campo de acuse de recibo incorporado no está en uso.

El bit **FIN** se usa para liberar una conexión; especifica que el transmisor no tiene más datos que transmitir.

El control de flujo en el TCP se maneja usando una ventana corrediza de tamaño variable. El campo de **ventana** indica la cantidad de bytes que pueden enviarse comenzando por el byte que ya se ha enviado acuse de recibo.

El campo **suma de comprobación** es una suma de comprobación de la cabecera, los datos y una pseudocabecera conceptual.

El campo de **opciones** se diseñó para contar con una manera de agregar características extra no cubiertas por la cabecera normal. La opción más importante es la que permite que cada *host* especifique la carga útil TCP máxima que está dispuesto a aceptar.

4.2.2. Números de puertos TCP

Como vimos en el formato del segmento TCP, un puerto es un número de 16 bits, por lo que existen 65536 puertos en cada computador. Las aplicaciones utilizan estos puertos para recibir y transmitir mensajes.

Los números de puerto de las aplicaciones cliente son asignados dinámicamente y generalmente son superiores al 1024. Cuando una aplicación cliente quiere comunicarse con un servidor, busca un número de puerto libre y lo utiliza.

En cambio, las aplicaciones servidoras utilizan unos números de puerto prefijados: son los llamados puertos *well-known* (bien conocidos).

Estos puertos están definidos en la *RFC 1700* y se pueden consultar en http://www.ietf.org/rfc/rfc1700.txt. A continuación se enumeran los puertos *well-known* más usuales:

Palabra clave	Puerto	Descripción
	0/tcp	Reserved
	0/udp	Reserved
Tcpmux	1/tcp	TCP Port Service Multiplexer
Rje	5/tcp	Remote Job Entry
Echo	7/tcp/udp	Echo
Discard	9/tcp/udp	Discard
systat	11/tcp/udp	Active Users
daytime	13/tcp/udp	Daytime
Qotd	17/tcp/udp	Quote of the Day
chargen	19/tcp/udp	Character Generator
ftp-data	20/tcp	File Transfer [Default Data]
ftp	**21/tcp**	**File Transfer [Control]**
telnet	**23/tcp**	**Telnet**
smtp	**25/tcp**	**Simple Mail Transfer**
time	37/tcp/udp	Time
nameserver	42/tcp/udp	Host Name Server
nicname	43/tcp/udp	Who Is
domain	**53/tcp/udp**	**Domain Name Server**
Bootps	67/udp/udp	Bootstrap Protocol Server
tftp	69/udp	Trivial File Transfer
Gopher	70/tcp	Gopher
finger	79/tcp	Finger
www-http	**80/tcp**	**World Wide Web HTTP**
dcp	93/tcp	Device Control Protocol
Supdup	95/tcp	SUPDUP
hostname	101/tcp	NIC Host Name Server
iso-tsap	102/tcp	ISO-TSAP
Gppitnp	103/tcp	Genesis Point-to-Point Trans Net
rtelnet	107/tcp/udp	Remote Telnet Service
pop2	109/tcp	Post Office Protocol - Version 2
pop3	**110/tcp**	**Post Office Protocol - Version 3**
Sunrpc	111/tcp/udp	SUN Remote Procedure Call

auth	113/tcp	Authentication Service
sftp	115/tcp/udp	Simple File Transfer Protocol
nntp	**119/tcp**	**Network News Transfer Protocol**
Ntp	123/udp	Network Time Protocol
pwdgen	129/tcp	Password Generator Protocol
Netbios-ns	137/tcp/udp	NETBIOS Name Service
Netbios-dgm	138/tcp/udp	NETBIOS Datagram Service
Netbios-ssn	**139/tcp/udp**	**NETBIOS Session Service**
snmp	161/udp	SNMP
Snmptrap	162/udp	SNMPTRAP
Irc	194/tcp	Internet Relay Chat Protocol

Los puertos tienen una memoria intermedia *(buffer)* situada entre los programas de aplicación y la red. De tal forma que las aplicaciones transmiten la información a los puertos. Aquí se va almacenando hasta que pueda enviarse por la red. Una vez que pueda transmitirse, la información irá llegando al puerto destino donde se irá guardando hasta que la aplicación esté preparada para recibirla.

4.2.3. Control de Congestionamiento con TCP

Cuando la carga ofrecida a cualquier red es mayor que la que puede manejar, se genera un **congestionamiento**. La Internet no es ninguna excepción.

En teoría, puede manejarse el congestionamiento aprovechando un principio de física: la ley de conservación de los paquetes. La idea es no inyectar un paquete nuevo en la red hasta que salga uno viejo (es decir, se entregue). El TCP intenta lograr esta meta manipulando dinámicamente el tamaño de la ventana.

Hoy día, la pérdida de paquetes por errores de transmisión es relativamente rara debido a que los troncales de larga distancia son de fibra (aunque las redes inalámbricas son otra historia). En consecuencia, la mayoría de las terminaciones de temporización en Internet se deben a congestionamientos.

Antes de analizar la manera en que el TCP reacciona al congestionamiento, se describirá primero lo que hace para evitar que ocurra. Al establecer una conexión, se tiene que seleccionar un tamaño de ventana adecuado. El receptor puede especificar una ventana con base en su tamaño de *buffer*. Si el transmisor se ajusta a su tamaño de ventana, no ocurrirán problemas por desbordamiento de *buffers* en la terminal receptora, pero aun pueden ocurrir debido a congestionamientos internos de la red.

La solución de Internet es aceptar que existen dos problemas potenciales (capacidad de la red y capacidad del receptor) y manejarlos por separado. Para ello, cada transmisor mantiene dos ventanas: la ventana que ha otorgado el receptor y una segunda ventana, la **ventana de congestionamiento**; cada una refleja la cantidad de bytes que puede enviar el transmisor. La cantidad de bytes que pueden enviarse es la cifra menor de las dos ventanas.

Al establecer una conexión, el transmisor asigna a la ventana de congestionamiento el tamaño de segmento máximo usado por la conexión; entonces envía un segmento máximo. Si se recibe el acuse de recibo de este segmento antes de terminar el temporizador, el transmisor agrega el equivalente en bytes de

auth	113/tcp	Authentication Service
sftp	115/tcp/udp	Simple File Transfer Protocol
nntp	**119/tcp**	**Network News Transfer Protocol**
Ntp	123/udp	Network Time Protocol
pwdgen	129/tcp	Password Generator Protocol
Netbios-ns	137/tcp/udp	NETBIOS Name Service
Netbios-dgm	138/tcp/udp	NETBIOS Datagram Service
Netbios-ssn	**139/tcp/udp**	**NETBIOS Session Service**
snmp	161/udp	SNMP
Snmptrap	162/udp	SNMPTRAP
Irc	194/tcp	Internet Relay Chat Protocol

Los puertos tienen una memoria intermedia *(buffer)* situada entre los programas de aplicación y la red. De tal forma que las aplicaciones transmiten la información a los puertos. Aquí se va almacenando hasta que pueda enviarse por la red. Una vez que pueda transmitirse, la información irá llegando al puerto destino donde se irá guardando hasta que la aplicación esté preparada para recibirla.

4.2.3. Control de Congestionamiento con TCP

Cuando la carga ofrecida a cualquier red es mayor que la que puede manejar, se genera un **congestionamiento**. La Internet no es ninguna excepción.

En teoría, puede manejarse el congestionamiento aprovechando un principio de física: la ley de conservación de los paquetes. La idea es no inyectar un paquete nuevo en la red hasta que salga uno viejo (es decir, se entregue). El TCP intenta lograr esta meta manipulando dinámicamente el tamaño de la ventana.

Hoy día, la pérdida de paquetes por errores de transmisión es relativamente rara debido a que los troncales de larga distancia son de fibra (aunque las redes inalámbricas son otra historia). En consecuencia, la mayoría de las terminaciones de temporización en Internet se deben a congestionamientos.

Antes de analizar la manera en que el TCP reacciona al congestionamiento, se describirá primero lo que hace para evitar que ocurra. Al establecer una conexión, se tiene que seleccionar un tamaño de ventana adecuado. El receptor puede especificar una ventana con base en su tamaño de *buffer*. Si el transmisor se ajusta a su tamaño de ventana, no ocurrirán problemas por desbordamiento de *buffers* en la terminal receptora, pero aun pueden ocurrir debido a congestionamientos internos de la red.

La solución de Internet es aceptar que existen dos problemas potenciales (capacidad de la red y capacidad del receptor) y manejarlos por separado. Para ello, cada transmisor mantiene dos ventanas: la ventana que ha otorgado el receptor y una segunda ventana, la **ventana de congestionamiento**; cada una refleja la cantidad de bytes que puede enviar el transmisor. La cantidad de bytes que pueden enviarse es la cifra menor de las dos ventanas.

Al establecer una conexión, el transmisor asigna a la ventana de congestionamiento el tamaño de segmento máximo usado por la conexión; entonces envía un segmento máximo. Si se recibe el acuse de recibo de este segmento antes de terminar el temporizador, el transmisor agrega el equivalente en bytes de

un segmento a la ventana de congestionamiento para hacerla de dos segmentos de tamaño máximo, y envía dos segmentos. A medida que se reconoce cada uno de estos segmentos, se aumenta el tamaño de la ventana de congestionamiento en un segmento máximo.

La ventana de congestionamiento sigue creciendo exponencialmente hasta ocurrir una terminación de temporización o alcanzar el tamaño de la ventana receptora. La idea es que, si las ráfagas de 1024, 2048 y 4096 bytes funcionan bien, pero una ráfaga de 8192 produce una terminación de temporización, la ventana de congestionamiento debe establecerse en 4096 para evitar el congestionamiento. Mientras el tamaño de la ventana de congestionamiento permanezca en 4096, no se enviará una ráfaga de mayor longitud, sin importar la cantidad de espacio de ventana otorgada por el receptor.

Este algoritmo se llama **arranque lento**, pero no es lento en lo absoluto; es exponencial, y se requiere que todas las implementaciones de TCP lo manejen.

Veamos ahora el algoritmo de control de congestionamiento de Internet, el cual usa un tercer parámetro, el **umbral**, inicialmente de 64 K, además de las ventanas de recepción y congestionamiento. Al ocurrir una terminación de temporización, se establece el umbral en la mitad de la ventana de congestionamiento actual, y la ventana de congestionamiento se restablece a un segmento máximo.

Luego se usa el arranque lento para determinar lo que puede manejar la red, excepto que el crecimiento exponencial termina al alcanzar el umbral. A partir de ese punto, las transmisiones exitosas aumentan linealmente la ventana de congestionamiento (en un segmento máximo por ráfaga) en lugar de uno por segmento.

En efecto, este algoritmo está suponiendo que probablemente es aceptable recortar la ventana de congestionamiento a la mitad, y luego aumentarla gradualmente a partir de ahí.

4.2.4. Interfaces TCP

Existen dos tipos de interfaces entre la conexión TCP y los otros programas. El primero es utilizar la pila de los programas de la capa de red. Como en esta capa solo esta el protocolo IP, el interface lo determina este protocolo. El segundo tipo es el interfaz del programa de usuario. Este interface puede variar segun el sistema operativo, pero en general tiene las siguientes caracteristicas.

El interface envuelve el programa de usuario llamando a una rutina que introduce entradas en una estructura de datos llamada el bloque de control de transmision (TCB). Las entradas se realizan inicialmente en la pila de *hardware* y transferidas al TCB por medio de una rutina de sistema. Estas entradas permiten al TCP asociar un usuario con una conexión particular, de modo que pueda aceptar comandos de un usuario y mandarlos a otro usuario en la otra parte de la conexión. TCP utiliza unos identificadores unicos para cada parte de la conexión. Esto se utiliza para recordar la asociacion entre dos usuarios. Al usuario se le asigna un nombre de conexión para utilizarlo en futuras entradas del TCB.

Los identificadores para cada estremo de la conexión se llaman **sockets.**

El socket local se construye concatenando la direccion IP de origen y el número de puerto de origen. El socket remoto se obtiene concatenando la direccion IP de destino y el número de puerto de destino.

El par de sockets de una conexión forman un único número en Internet. El UDP tiene los mismos sockets, pero no los recuerda. Esta es las diferencia entre un protocolo orientado a conexión y otro a no conexión. A continuacion se explican los comandos más usuales:

- ***Open***: Inicia una conexión o comienza a escuchar un socket. El usuario tiene un nombre de conexión local que actua como un puntero dentro del TCB.
- ***Send***: El comando *Send* manda datos del *buffer* especificado.
- ***Receive***: El comando *Receive* es un mensaje de error si el nombre local proporcionado no es utilizado antes con el comando *Open*.
- ***Close***: El comando *Close* hace que se cierre una conexión. Se produce un error si la conexión especificada no ha sido abierta, o si no se tiene autorizacion para cerrar la conexión.
- ***Status***: El comando *Status* solo tiene una variable asociada, que es el nombre de la conexión.
- ***Abort***: El comando *Abort* hace que todos los comandos Send y Receive asociados al nombre de la conexión local se interrumpan. La entrada del usuario del TCB se elimina y se envia un mensaje especial de reinicio a la entidad del otro lado de la conexión.

El TCP recuerda el estado de cada conexión por medio del TCB. Cuando se abre una conexión, se efectua una entrada unica en el TCB. Un nombre de conexión se le asigna al usuario para activar los comandos de la conexión. Cuando se cierra una conexión se elimina su entrada del TCB.

CONTROL DE

4.2.5. Estados del TCP

TCB - BLOQUE DE TRANSMISION

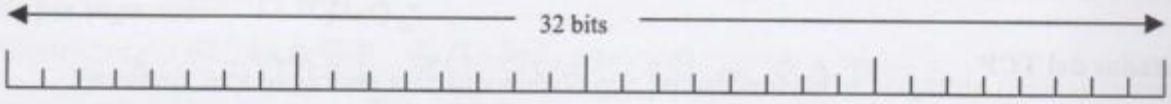
El inicio, mantenimiento y cierre de una conexión requiere que el TCP recuerde toda la información relativa a cada conexión. Esta información se almacena en una entrada para cada conexión dentro del TCB. Cuando se abre una conexión, la entrada en el TCB se realiza con todas las variables inicializadas con sus rexpectivos valores. Durante la conexión, la entrada del TCB es actualizada a medida que cambia la información. A continuacion se describen algunos de los estados del TCP:

- **0. CLOSED:** No existe, solo para referencia.
- **1. LISTEN:** Esperando solicitud de conexión de un TCP remoto.
- **2. SYN-SEN:** Esperando un mensaje de solicitud de conexión despues de haber enviado una solicitud de conexión.
- **3. SYN-RECEIVED:** Esperando confirmacion de una reconicimiento de solicitud de conexión, despues de haber enviado y recibido una solicitud de conexión.
- **4. ESTABLISHED:** Representa un a conexión abierta. Los datos recibidos pueden ser enviados a un protocolo de una capa superior. Este es el estado normal de la fase de transferencia de la conexión.
- **5. FIN-WAIT-1:** Esperando la solicitud de fin de conexión de un TCP remoto, o un reconocimiento de una solicitud de fin de transmision enviada anteriormente.
- **6. FIN-WAIT-2:** Esperando una solicitud de fin de conexión de un TCP remoto.

- **7. CLOSE-WAIT:** Esperando una solicitud de fin de conexión de un protocolo de una capa superior.
- **8. CLOSING:** Esperando el conocimiento de una solicitud de final de conexión de un TCP remoto.
- **9. LAST-ACK:** Esperando el conocimiento de una solicitud de final de conexión enviada anteriormente al TCP remoto.
- **10. TIME-WAIT:** Esperando el tiempo necesario para que el TCP remoto haya recibido el conocimiento de la solicitud del fin de conexión.

4.2.6. Protocolo UDP (Protocolo de Datos de Usuario)

El grupo de protocolos de Internet también maneja un grupo de protocolo de transporte sin conexiones, el UDP. Éste ofrece a las aplicaciones un mecanismo para enviar datagramas IP en bruto encapsulados sin tener que establecer una conexión. Muchas aplicaciones cliente-servidor que tienen una solicitud y una respuesta usan el UDP en lugar de tomarse la molestia de establecer y luego liberar una conexión.



Puerto de origen	Puerto de destino
Longitud UDP	Suma de comprobación UDP

FIGURA 5.65: La cabecera de UDP.

Un **segmento UDP** consiste en una **cabecera** de 8 bytes seguida de los **datos**. Los dos puertos de la cabecera sirven para lo mismo que en el TCP: para identificar los puntos terminales de las máquinas de origen y destino.

El campo de **longitud UDP** incluye la cabecera de 8 bytes y los datos.

La **suma de comprobación UDP** incluye la misma pseudocabecera de formato mostrada en la **figura 5.65**, la cabecera UDP y los datos UDP, rellenados a una cantidad par de bytes de ser necesario. Esta suma es opcional y se almacena como 0 si no se calcula.

4.3. DNS (Sistema de nombres de dominio)

Cuando miles de estaciones de trabajo se conectaron a la red, todos se dieron cuenta que este enfoque no podría seguir funcionando eternamente. Por una parte el archivo se volvería muy grande. Un problema aun más importante era que ocurrirían conflictos constantes con los nombres de los *hosts* y destinos de correos electrónicos con direcciones IP, a menos que los nombres se administraran centralmente, algo impensable en una red internacional enorme.

Para resolver estos problemas se inventó el **DNS**[38] (Sistema de Nombre de Dominio).

La esencia del DNS es la invención de un esquema de nombres jerárquicos basado en dominio y una base de datos distribuida para implementar este esquema de nombres. El DNS se usa principalmente para relacionar las direcciones de *hosts* y destinos de correo electrónico con las direcciones IP, pero también puede usarse con otros fines.

Muy brevemente, el funcionamiento del DNS es el siguiente: para relacionar un nombre con una dirección IP, un programa de aplicación llama a un procedimiento de biblioteca llamado resolvedor, pasándole el nombre como parámetro.

El resolvedor envía un paquete UDP[39](Protocolo de Datagramas de Usuario) a un servidor DNS local, que entonces busca el nombre y devuelve la dirección IP al resolvedor, que entonces lo devuelve al solicitante. Con la dirección IP, el programa puede establecer una conexión TCP[40](Protocolo de Control de Transmisión) con el destino, o enviarle paquetes UDP.

4.3.1. El espacio de nombres del DNS

La administración de un grupo grande y cambiante de nombres es un problema nada sencillo. En el sistema postal, la administración de los nombres se hace requiriendo letras para especificar (implícita o explícitamente) el país, estado o provincia, ciudad y calle, y dirección del destino destinatario.

Conceptualmente, la Internet se divide en varios cientos de **dominios** de nivel superior, cada uno de los cuales abarca muchos *hosts*.

Cada dominio se divide en subdominios, y éstos se dividen nuevamente. Todos estos dominios pueden representarse mediante un árbol, como se muestra en **figura 4.6.**

Las hojas de los árboles representan los dominios que no tienen subdominios (pero que, por supuesto, contienen máquinas). Un dominio de hoja puede contener un solo *host*, o puede representar una compañía de miles de *hosts*.

[38] En Inglés: Domain Name System.
[39] En Inglés: User Datagram Protocol.
[40] En Inglés: Transmission Control Protocol.

4.3. DNS (Sistema de nombres de dominio)

Cuando miles de estaciones de trabajo se conectaron a la red, todos se dieron cuenta que este enfoque no podría seguir funcionando eternamente. Por una parte el archivo se volvería muy grande. Un problema aun más importante era que ocurrirían conflictos constantes con los nombres de los *hosts* y destinos de correos electrónicos con direcciones IP, a menos que los nombres se administraran centralmente, algo impensable en una red internacional enorme.

Para resolver estos problemas se inventó el **DNS**[38] (Sistema de Nombre de Dominio).

La esencia del DNS es la invención de un esquema de nombres jerárquicos basado en dominio y una base de datos distribuida para implementar este esquema de nombres. El DNS se usa principalmente para relacionar las direcciones de *hosts* y destinos de correo electrónico con las direcciones IP, pero también puede usarse con otros fines.

Muy brevemente, el funcionamiento del DNS es el siguiente: para relacionar un nombre con una dirección IP, un programa de aplicación llama a un procedimiento de biblioteca llamado resolvedor, pasándole el nombre como parámetro.

El resolvedor envía un paquete UDP[39](Protocolo de Datagramas de Usuario) a un servidor DNS local, que entonces busca el nombre y devuelve la dirección IP al resolvedor, que entonces lo devuelve al solicitante. Con la dirección IP, el programa puede establecer una conexión TCP[40](Protocolo de Control de Transmisión) con el destino, o enviarle paquetes UDP.

4.3.1. El espacio de nombres del DNS

La administración de un grupo grande y cambiante de nombres es un problema nada sencillo. En el sistema postal, la administración de los nombres se hace requiriendo letras para especificar (implícita o explícitamente) el país, estado o provincia, ciudad y calle, y dirección del destino destinatario.

Conceptualmente, la Internet se divide en varios cientos de **dominios** de nivel superior, cada uno de los cuales abarca muchos *hosts*.

Cada dominio se divide en subdominios, y éstos se dividen nuevamente. Todos estos dominios pueden representarse mediante un árbol, como se muestra en **figura 4.6.**

Las hojas de los árboles representan los dominios que no tienen subdominios (pero que, por supuesto, contienen máquinas). Un dominio de hoja puede contener un solo *host*, o puede representar una compañía de miles de *hosts*.

[38] En Inglés: Domain Name System.
[39] En Inglés: User Datagram Protocol.
[40] En Inglés: Transmission Control Protocol.

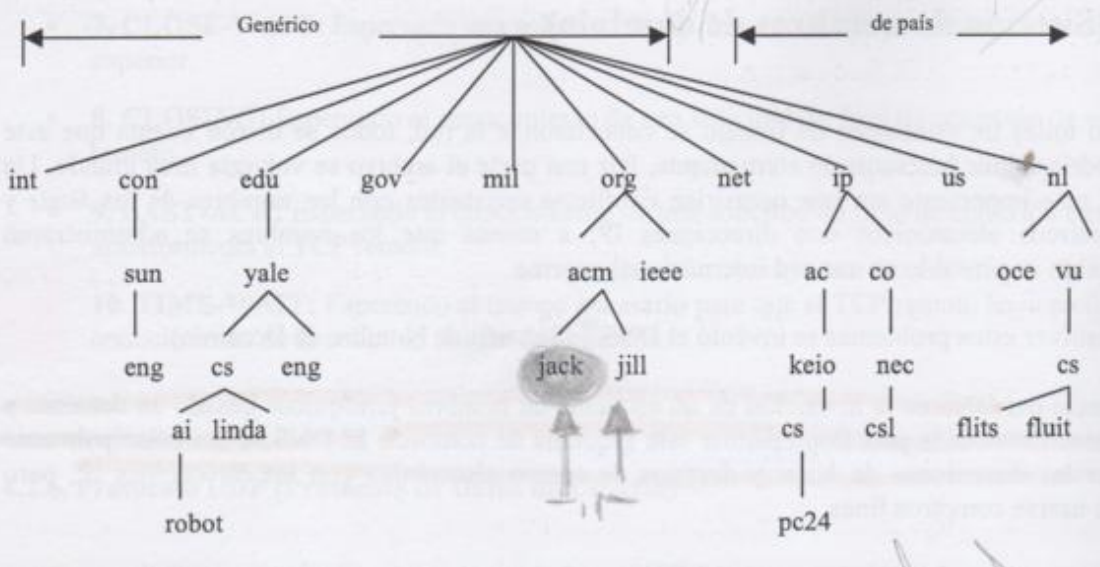


FIGURA 4.6: Árbol DSN.

Cada dominio se nombra por la trayectoria hacia arriba desde él a la raíz (sin nombre). Los componentes se separan por puntos.

Los nombres de los dominios pueden ser absolutos o relativos. Un nombre de dominio absoluto termina con un punto por ejemplo: *eng.sun.com.* Los nombres de dominio relativo tienen que interpretase en algún contexto para determinar de manera única su significado verdadero. En ambos casos, un dominio nombrado se refiere a un nombre específico del árbol y a todos los nodos por debajo de él.

Los nombres de dominio no hacen distinción entre las mayúsculas y las minúsculas por lo que *edu y EDU* significan la misma cosa. Los nombres de componentes pueden ser de hasta 63 caracteres de longitud, los nombres de trayectoria completa no deben exceder los 255 caracteres.

Para crear un dominio nuevo, se requiere el permiso del dominio donde se incluirá. Los nombres reflejan los limites organizacionales, no las redes físicas. Por ejemplo, si los Departamentos de Informática e Ingeniería Electrónica se ubican en el mismo edificio y comparten la misma LAN, de todas maneras pueden tener dominios diferentes.

4.3.2. Registros de recursos

Cada dominio, sea un *host* individual o un dominio de nivel superior, puede tener un grupo de registros de recursos asociados a él. En un *host* individual, el registro de recursos más común es simplemente una dirección IP, pero también existen muchos otros tipos de registros de recursos.

Cuando un resolvedor da un nombre de dominio al DNS, lo que recibe son los registros de recursos asociados a ese nombre. Por lo tanto la función real del DNS es relacionar los dominios de nombres con los registros de recursos.

Un registro de recursos tiene cinco tuplas. Aunque éstas se codifican en binario por cuestión de eficiencia, en la mayoría de las presentaciones los registros de recursos se dan como texto ASCII, una línea por registro de recurso. El formato que usaremos es el siguiente:

Nombre_dominio Tiempo_de_vida Tipo Clase Valor

- El **nombre_dominio:** indica en dominio al que pertenece este registro. Por lo tanto, este campo es la llave primaria de búsqueda usada para atender las consultas.
- El campo **tiempo_de_vida:** es una indicación de la estabilidad del registro.
- El campo **tipo:** indica el tipo de registro de que se trata.
- El campo **clase:** indica la clase de registro de que se trata.
- El campo **valor:** este campo puede ser un número, un nombre de dominio o una cadena ASCII.

4.3.3. Servidores de nombres

Cuando menos en teoría, un solo servidor de nombres podría contener la base de datos DNS completa y responder a todas las consultas sobre ella. En la práctica, este servidor estaría tan sobrecargado que sería inservible. Es más, si llegara a caerse, la Internet completa se vendría abajo.

Para evitar los problemas asociados a tener una sola fuente de información, el espacio de nombres DNS se divide en **zonas** no traslapantes.

Una manera posible de dividir el espacio de nombres, es como se muestra en la **figura 4.7**. Cada zona contiene una parte del árbol y también contiene servidores de nombres que contienen la información de autorización correspondiente a esa zona. Normalmente una zona tendrá un servidor de nombres primarios, que obtiene su información de un archivo en su disco, y uno o más nombres de servidores secundarios, que obtienen su información del servidor de nombres primario.

Para asegurar su confiabilidad, algunos servidores de ciertas zonas pueden situarse fuera de la zona.

El lugar donde se colocan los límites de las zonas dentro de una zona es responsabilidad del administrador de esa zona. Esta decisión se toma en gran medida basada en la cantidad de servidores de nombres deseados y su ubicación.

Cuando un resolvedor tiene una consulta frente a un nombre de dominio, la pasa a uno de nombres de servidores locales. Si el dominio que se busca cae bajo la jurisdicción del servidor de nombres, devuelve los registros de recursos autorizados. Un **registro autorizado** es uno que viene de la autoridad que administra el registro y por lo tanto siempre es correcto. Los registros autorizados contrastan con los registros en caché, que podrían no estar actualizados.

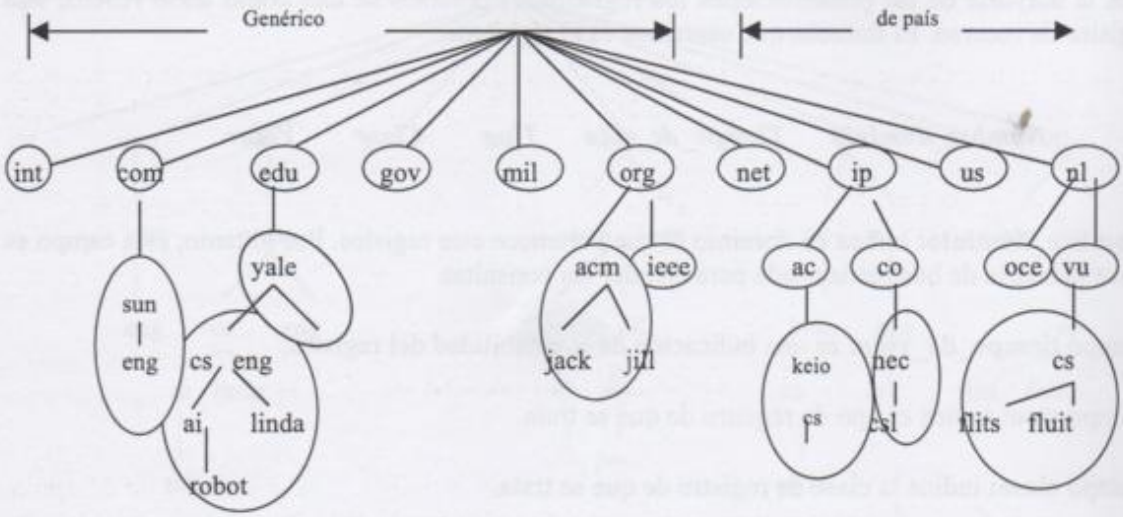


FIGURA 4.7: División de los espacios de los nombres.

Por otro lado, si el dominio es remoto y no hay información disponible localmente, sobre el dominio solicitado, el servidor de mensajes envía un mensaje de consulta para el dominio solicitado al servidor de nombres del nivel superior. Para hacer más claro este proceso, considere el ejemplo de la **figura 4.8**. Aquí, un resolvedor de *flits.cs.vu.nl* quiere saber la dirección IP del *host linda.cs.yale.edu.* En el paso 1 se envía una consulta al servidor de nombre local, *cs.vu.nl.* Esta consulta contiene el nombre del dominio buscado, el tipo (*A*) y la clase (*IN*).

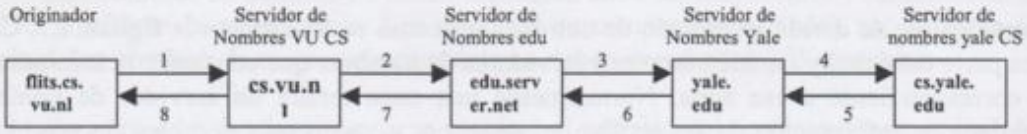


FIGURA 4.8: Manera en que un resolvedor busca un nombre remoto en ocho pasos.

Supongamos que el servidor de nombres local nunca ha tenido una consulta para este nombre antes, y no sabe nada sobre él; puede preguntar a algunos otros servidores de nombres cercanos, pero si ninguno de ellos sabe nada, enviará un paquete UDP al servidor *edu* indicado en su base de datos (**figura 4.8**), *edu.server.net.* Es improbable que este servidor sepa la dirección de *linda.cs.yale.edu* y probablemente tampoco sabe la de *cs.yale.edu*, pero debe conocer a todos sus hijos, por lo que envía su solicitud al servidor de nombres de *yale.edu* (paso 3). A su vez, éste reenvía la solicitud a *cs.yale.edu* (paso 4), que debe tener los registros de recursos autorizados. Puesto que cada solicitud es de un cliente a un servidor, el registro de recursos solicitado regresa a través de los pasos 5 a 8.

Una vez que estos registros regresan al servidor de nombres *cs.vu.nl*, son ingresados en caché ahí, para el caso que se necesiten después. Sin embargo, esta información aquí almacenada no es autorizada, puesto que los cambios hechos en *cs.yale.edu* no se propagan a todos los cachés del mundo que puedan saber sobre ella. Por esta

razón, las entradas de caché no deben vivir demasiado tiempo. Esta es la razón de que el campo tiempo de vida se incluya en cada registro de recurso.

Vale la pena mencionar que el método de consultas aquí descrito se conoce como **consulta recurrente**, puesto que cada servidor no tiene toda la información solicitada sale a encontrarla en algún lado y luego la informa.

También vale la pena indicar que, cuando un cliente DNS no recibe una respuesta antes de terminar su temporizador, normalmente intentará otro servidor la siguiente vez.

4.4. SNMP[41] (Protocolo sencillo de administración de redes)

El SNMP proporcionó una manera sistemática de supervisar y administrar una red de cómputo. Esta estructura y su protocolo se implementaron ampliamente en los productos comerciales y se volvieron los estándares de facto para la administración de redes.

4.4.1. El modelo SNMP

El modelo SNMP de una red administrada consta de cuatro componentes:

1- Nodos administrados.

2- Estaciones administradas.

3- Información de administración.

4- Un protocolo de administración.

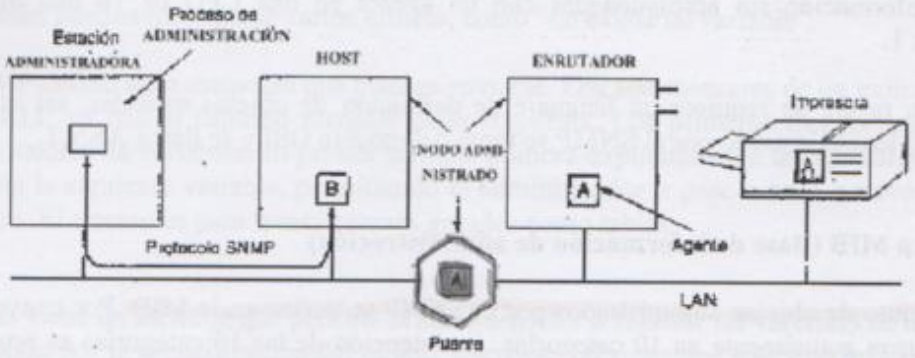


FIGURA 4.9: Componentes del modelo de administración SNMP.

Los nodos administrados pueden ser *hosts*, enrutadores, puentes, impresoras u otros dispositivos capaces de comunicar información de estado al mundo exterior. Para ser administrado directamente por el SNMP, un nodo debe ser capaz de ejecutar un proceso de administración SNMP llamado Agente SNMP. Todas las computadoras cumplen este requisito, al igual que una cantidad creciente de puentes, enrutadores y dispositivos periféricos

[41] En Inglés: Simple Network Management Protocol.

diseñados para uso en redes. Cada agente mantiene una base de datos local de variables que describen su estado e historia y que afectan su operación.

La administración de la red se hace desde **estaciones administradoras**, que son, de hecho, computadoras de propósito general que ejecuten un *software* de administración especial. La estación administradora contiene uno o más procesos que se comunican con los agentes a través de la red, emitiendo comandos y recibiendo respuestas. En este diseño, toda la inteligencia está en las estaciones administradoras, a fin de mantener los agentes tan sencillos como sea posible y minimizar su impacto en los dispositivos en los que se ejecutan. Muchas estaciones administradoras tienen una interfaz gráfica de usuario para que el administrador de la red pueda inspeccionar el estado de la red y emprenda acciones cuando se requieran.

Por lo tanto el SNMP describe con riguroso detalle la información exacta de cada tipo de agente que tiene que administrar y el formato con que éste tiene que proporcionarle los datos. La parte más grande del modelo SNMP es la definición de quién tiene que llevar el registro de qué y cómo se comunica esta información.

Muy brevemente, cada dispositivo mantiene una o más variables que describen su estado. En la documentación del SNMP, estas variables se llaman objetos, pero el término es engañoso porque no son objetos en el sentido de un sistema orientado a objetos, puesto que sólo tienen estados y no métodos. Sin embargo, el término está tan difundido que lo usaremos aquí. El conjunto de todos los objetos posibles de una red se da en la estructura de datos llamada MIB[42] (Base de información de administración) que mencionaremos más adelante.

4.4.2. ASN[43].1 (Notación de Sintaxis Abstracta 1)

El corazón del modelo SNMP es el grupo de objetos administrados por los agentes y leídos y escritos por la estación administradora. Para ser posible la comunicación multiproveedor, es esencial que estos objetos se definan de una manera estándar y neutral desde el punto de vista de los proveedores. Es más, se requiere una forma estándar de codificarlos para su transferencia a través de una red. Si bien las definiciones en C satisfarían el primer requisito, tales definiciones no definen una codificación de bits en el alambre de modo tal que una estación administradora de 32 bits *little endian* de complemento a 2 pueda intercambiar información sin ambigüedades con un agente en una CPU de 16 bits *big endian* de complemento a 1.

Por esta razón, se requiere un lenguaje de definición de objetos estándar, así como reglas de codificación. El lenguaje usado por el SNMP se toma del modelo OSI y se llama **ASN.1**.

4.4.3. La MIB (Base de información de administración)

El conjunto de objetos administrados por el SNMP se define en la MIB. Por conveniencia, estos objetos se agrupan actualmente en 10 categorías. La intención de las 10 categorías es proporcionar una base de lo que debe entender una estación administradora. Ciertamente se agregarán nuevas categorías y objetos en el futuro, y los proveedores están en libertad de definir objetos adicionales para sus productos. Las 10 categorías se definen en la **figura 4.10**.

[42] En Inglés: Management Information Base.
[43] En Inglés: Abstract Syntax Notation.

Grupo	# Objeto	Descripción
SYSTEM	7	Nombre, ubicación y descripción del equipo.
INTERFACES	23	Interfaces de red y su tráfico medio.
AT	3	Traducción de direcciones (desaprobada).
IP	42	Estadísticas de paquetes IP.
ICMP	26	Estadísticas sobre los paquetes ICMP recibidos.
TCP	19	Algoritmos, parámetros y estadísticas TCP.
UCP	6	Estadística de tráfico UCP.
EGP	20	Estadística de tráfico de protocolo de pasarela exterior.
TRANSMISION	0	Reservado para MIB de medio específico.
SNMP	29	Estadística de tráfico SNMP.

FIGURA 4.10: Grupos de objetos del MIB-II de Internet..

4.4.4. El Protocolo SNMP

La forma normal de uso del SNMP es que la estación administradora envíe una solicitud a un agente pidiéndole información o mandándole actualizar su estado de cierta manera. Idealmente la respuesta del agente simplemente es la información solicitada o la confirmación de que ha actualizado su estado según lo solicitado. Los datos se envían empleando la sintaxis de transferencia ASN.1. Sin embargo, también pueden informarse varios errores, como "no existe tal variable".

El SNMP define siete mensajes que pueden enviarse. Los seis mensajes de un indicador se ilustran en la **figura 4.11**, ya que el séptimo mensaje es la respuesta. Los primeros tres mensajes solicitan la devolución de valores de variables. El primer formato nombra explícitamente las variables que quiere. El segundo solicita la siguiente variable, permitiendo al administrador ir paso a paso a través de la MIB en orden alfabético. El tercero es para transferencias grandes como tablas.

Después viene un mensaje que permite al administrador actualizar las variables de un agente, hasta el límite permitido por la especificación del objeto, claro está, si sigue una solicitud informal que permite a un administrador indicarle a otro las variables que está manejando. Por último viene el mensaje enviado de un agente a un administrador cuando ha habido una interrupción.

Mensajes	Descripción
Get- request.	Solicita el valor de una o más variables.
Get-next-request.	Solicita la variable que sigue a ésta.
Get-bulk-request.	Obtiene una tabla grande.
Set-request.	Actualiza una o más variables.
Inform-request.	Mensaje de administrador o y administrador describiendo la MIB local.
Snmpv2-trap.	Informe de interrupciones de agente a administrador.

FIGURA 4.11: Seis mensajes del indicador.

4.5. Correo electrónico

El correo electrónico o *e-mail*, ha existido por más de dos décadas. Los primeros sistemas de correo electrónico consistían simplemente en protocolos de transferencia de archivos, con la convención que la primera línea de cada mensaje contenía la dirección del destinatario.

En esta sección proporcionaremos una vista panorámica de lo que pueden hacer los sistemas de correo electrónico y la manera en que están organizados. Normalmente consisten en dos subsistemas: los **agentes de usuario**, que permiten a la gente leer y enviar correo electrónico, y los **agentes de transferencia de mensaje**, que mueven los mensajes del origen al destino. Los agentes de usuarios son programas locales que proporcionan un método basado en comandos, basados en menúes o de interacción gráfica con el correo electrónico. Los agentes de transferencia de mensajes son por lo común *daemons* del sistema que operan en segundo plano y mueven correo electrónico a través del sistema.

Por lo común los sistemas de correo electrónico desempeñan cinco funciones básicas, como se describe a continuación.

- La **composición** se refiere al proceso de crear mensajes y respuestas.
- La **transferencia** se refiere a mover mensajes del originador al destinatario.
- La **generación del informe** tiene que ver con indicar al remitente lo que ocurrió con el mensaje.
- La **visualización** de los mensajes de entrada es necesaria para que la gente pueda leer su correo electrónico.
- La **disposición** es el paso final y se refiere a lo que el destinatario hace con el mensaje tras recibirlo.

La mayoría de los sistemas permiten a los usuarios crear buzones de correo *(mailboxes)* para almacenar el correo entrante.

El correo registrado es otra idea importante, para permitir al originador saber que su mensaje ha llegado. Como alternativa, podría desearse la notificación automática del correo que no se puede entregar. De cualquier modo, el originador debe tener algún control sobre el informe de lo ocurrido.

Otra característica avanzada son las copias al carbón, correo electrónico de alta prioridad, correo electrónico secreto (cifrado), destinatarios alternos por si el primario no está disponible y la capacidad de que las secretarias manejen el correo de su jefe.

Una idea clave de todos los sistemas modernos de correo electrónico es la distinción entre la envoltura y su contenido. La envoltura encapsula el mensaje, como dirección de destino, prioridad y nivel de seguridad, la cual es diferente del mensaje mismo. Los agentes de transporte del mensaje usan la envoltura para enrutar, al igual que la oficina postal.

El mensaje dentro de la envoltura contiene dos partes: la **cabecera** y el **cuerpo**. La cabecera contiene información de control para los agentes de usuario. El cuerpo es por completo para el destinatario humano.

4.5.1. El agente de usuario

Un agente de usuario normalmente es un programa que acepta una variedad de comandos para componer, recibir y contestar menajes, así como manipular los buzones de correo. Algunos agentes de usuario tienen una interfaz elegante operada por menúes o iconos que requieren un ratón (*mouse*), mientras que otros esperan comandos de un carácter desde el teclado. Funcionalmente, ambos son iguales.

4.5.2. Envío de correo electrónico

Para enviar un mensaje de correo electrónico, el usuario debe proporcionar el mensaje, la dirección de destino y posiblemente, algunos otros parámetros (prioridad o nivel de seguridad). El mensaje puede producirse con un editor de texto independiente, un programa de procesamiento de texto, o posiblemente, un editor de texto incorporado en el agente de usuario.

La mayoría de los sistemas de correo electrónico manejan listas de correo, por lo que un usuario puede mandar el mismo mensaje a un grupo de personas con un solo comando. Si la lista de correo se mantiene localmente, el agente usuario puede sencillamente enviar un mensaje por separado a cada destinatario. Sin embargo, si la lista se mantiene remotamente, entonces los mensajes se multiplicarán ahí.

4.5.3. Lectura del correo electrónico

Por lo común, al arrancar un agente de usuario, buscará en el buzón del usuario el correo electrónico recibido, antes de presentar otra cosa en la pantalla. Entonces puede anunciar la cantidad de mensajes en el buzón o presentar un resumen de una línea de cada uno y esperar un comando.

Como ejemplo de funcionamiento de un agente de usuario, veremos una situación típica de correo. Tras iniciar el agente de usuario, el usuario solicita un resumen de correo electrónico. Aparece entonces una pantalla como la **figura 4.12,** cada línea se refiere a un mensaje. En este ejemplo el buzón contiene ocho mensajes.

#	Indicadores	Bytes	Remitente	Asunto
1	k	1030	Asw	Cambios UNÍS.
2	ka	6348	Radia	Comentario sobre el material que me enviaste.
3	kf	4519	Amy. m. wong	Solicitud de información.
4		1236	Bal	Fecha límite para propuesta de subvención.
5		103620	Kaashoek	Texto de documento dcs.
6		1223	Emily. e	Apuntador a página de www
7		3110	Saniya	Informes de arbitraje sobre documentos.
8		1204	Drm	Re: visita de mis estudiantes.

FIGURA 4.12: Ejemplo de exhibición del contenido de un buzón.

Una vez que se han visualizado las cabeceras, el usuario puede ejecutar cualquiera de los comandos disponibles. Un conjunto típico se ilustra en la **figura 4.13**. Algunos de los comandos requieren un parámetro. El signo # significa que se espera el número de un mensaje o tal vez de varios mensajes. Como alternativa, puede utilizarse la letra "a" para referirse a todos los mensajes.

En los sistemas de correo electrónico diseñados para principiantes, cada uno de estos comandos típicamente está asociado a un icono de la pantalla, por lo que el usuario no tiene que recordar que "a" significa respuesta. En cambio, tiene que recordar que la pequeña imagen de una persona con su boca abierta significa respuesta y no visualizar mensaje.

Comando	Parámetro	Descripción
h	#	Presenta cabeceras en la pantalla.
c		Presenta cabecera actual únicamente.
t	#	Tipos de mensajes en la pantalla.
s	dirección	Envía mensaje.
f	#	Reenvía mensaje.
a	#	Contesta mensaje.
d	#	Borra mensaje.
u	#	Recupera mensajes previamente borrados.
m	#	Mueve mensajes a otro buzón.
k	#	Guarda mensaje tras salir.
r	buzón	Lee un buzón nuevo.
n		Va al siguiente mensaje y lo presenta.
b		Regresa al menaje previo y lo presenta.
g	#	Va a un mensaje específico pero no lo presenta.
e		Sale del sistema de correo y actualiza el buzón.

FIGURA 4.13: Comandos.

4.5.4. Formato de mensaje

4.5.4.1. RFC 822

Pasamos ahora de la interfaz del usuario al formato de los mensajes de correo electrónico. Los mensajes consisten en una envoltura primitiva, algunos campos de cabecera, algunas líneas en blanco y el cuerpo del mensaje. Cada campo de cabecera consiste en una sola línea de texto de ASCII que contiene el nombre del campo, dos puntos y para la mayoría de los campos un valor. El RFC 822 es un estándar viejo y no distingue claramente la envoltura de los campos de cabecera, como lo haría un estándar nuevo. En el uso normal el agente de usuario construye un mensaje y lo pasa al agente de transferencia de mensajes, quien entonces usa algunos de los campos de la cabecera para construir la envoltura, una mezcla un tanto anticuada de mensaje y envoltura.

Los principales campos de cabecera relacionados con el transporte del mensaje se listan en la **figura 4.14.** Además de estos campos, los mensajes RFC 822 también pueden conectar una variedad de campos de cabecera usados por los agentes de los usuarios o los destinatarios. Los más comunes se listan en la **figura 4.15.**

Cabecera	Significado
To	Direcciones de e-mail de los destinatarios primarios.
Cc	Direcciones de e-mail de los destinatarios secundarios.
bcc	Direcciones de e-mail para las copias al carbón ciegas.
from	Persona/s que crearon el mensaje.
sender	Dirección de correo electrónico del remitente.
received	Línea agregada por cada agente de transferencia en la ruta.
return-path	Puede usarse para identificar una trayectoria de regreso al remitente.

FIGURA 4.14: Campos de Cabecera.

Cabecera	Significado
date	Fecha y hora de envío del mensaje.
reply-to	Dirección de e-mail a la que deben enviarse las contestaciones.
messaged-id	Número único para referencia posterior para este mensaje.
in-reply-to	Identificación del mensaje a que éste responde.
references	Otros identificadores de mensajes pertinentes.
keywords	Claves seleccionadas por el usuario.
subject	Resumen de mensaje corto para exhibir en una línea.

FIGURA 4.15: Campos de cabecera RFC 822 relacionados con el transporte de mensajes.

El documento RFC 822 explícitamente indica que los usuarios pueden inventar cabeceras nuevas para su uso privado, siempre y cuando comiencen con la cadena X. Se garantiza que no habrá cabeceras futuras que comiencen con la cadena X, a fin de evitar conflictos entre las cabeceras oficiales y privadas.

4.5.4.2. MIME (Extensiones multipropósito de correo Internet)

En los primeros días de Arpanet, el correo electrónico consistía exclusivamente en mensajes de texto escritos en inglés y expresados en ASCII. En tal entorno, el RFC 822 hacía todo el trabajo: especificaba las cabeceras, pero dejaba el contenido en manos del usuario. Hoy día en la red mundial de Internet, este enfoque y no es adecuado. Los problemas incluyen envío y recepción de:

1. Mensajes en idiomas con acentos.
2. Mensajes en alfabetos no latinos.
3. Mensajes en idiomas sin alfabetos.
4. Mensajes que no contienen texto.

Se propuso una solución en el RFC 1341 y se actualizó el RFC 1521. Esta solución llamado MIME (Multipurpose Internet Mail Extensions) se usa ampliamente. Ahora la describimos.

La idea básica del MIME es continuar usando el formato RFC 822, pero agregar una estructura al cuerpo del mensaje y definir reglas de codificación para los mensajes no ASCII. Al no desviarse del 822, los mensajes MIME pueden enviarse usando los programas y protocolos de correo electrónico existentes. Todo lo que tiene que cambiarse son los programas transmisores y receptores, lo que pueden hacer los usuarios mismos.

El MIME define cinco nuevas cabeceras de mensaje, como se muestra en la **figura 4.16.**

Cabecera	Significado
mime-version	Identifica la versión de MIME.
content-description	Cadena de texto que describe el contenido.
content-id	Identificador único.
content-transfer-encoding	Cómo se envuelve el mensaje para su transmisión.
content-type	Naturaleza del mensaje.

FIGURA 4.16: Cabeceras RFC 822 agregadas por MIME.

4.5.5. Transferencia de mensajes

El sistema de transferencia de mensajes se ocupa de transmitir los mensajes del remitente al destinatario. La manera más sencilla de hacer esto es establecer una conexión de transporte de la máquina origen a la destino y sencillamente transferir el mensaje.

4.5.5.1. SMTP[44] (Protocolo sencillo de transferencia de mensajes)

En Internet, el correo electrónico se entrega al hacer que la máquina de origen establezca una conexión TCP con el puerto 25 de la máquina de destino. Escuchando en este puerto está un *daemon* de correo electrónico que habla con el SMTP. Este *daemon* acepta conexiones de entrada y copia mensajes de ellas a los buzones adecuados. Si no puede entregarse un mensaje, se devuelve al transmisor un informe de error que contiene la primera parte del mensaje que no pudo entregarse.

El SMTP es un protocolo ASCII sencillo. Tras establecer la conexión TCP con el puerto 25 de la máquina transmisora, operando como cliente, espera que la máquina receptora, operando como servidor, hable primero. El servidor comienza por enviar una línea de texto que proporciona su identidad e indica si está preparado o no para recibir correo. Si no lo está, el cliente libera la conexión y lo intenta después.

Si el servidor está dispuesto a aceptar el correo electrónico, el cliente anuncia de quién viene el mensaje, y a quién está dirigido. Si existe tal destinatario en tal destino, el servidor da permiso al cliente para transmitir el mensaje. Entonces el cliente envía el mensaje y servidor acusa su recibo. Si hay más correo electrónico, se envía ahora. Una vez que todo el correo electrónico ha sido intercambiado en ambas direcciones, se libera la conexión.

4.5.5.2. Pasarelas de correo electrónico

El correo electrónico usando SMTP funciona mejor cuando tanto el transmisor como el receptor están en Internet y pueden manejar conexiones TCP entre el transmisor y el receptor. Sin embargo, muchas máquinas que no están en Internet, también quieren recibir y transmitir correo electrónico de instalaciones de Internet. Por ejemplo, muchas compañías intencionalmente no quieren estar en Internet por razones de seguridad. Algunas de ellas incluso se aíslan de Internet levantando muros de seguridad (*firewalls*) entre ellas mismas y la Internet.

Ocurre otro problema cuando el transmisor habla sólo RFC 822 y el otro sólo habla un protocolo de correo X.400 o alguno patentado, específico del proveedor. Dado que estos dos mundos difieren en cuanto al formato de mensajes y los protocolos, es imposible la comunicación directa.

Ambos de problemas se resuelven usando pasarelas de correo electrónico. Supongamos un caso en que un *host* 1 sólo habla TCP/IP RFC 822, mientras que otro *host* 2 habla sólo TP4 y X.400 de OSI. No obstante, pueden intercambiar mensajes utilizando pasarelas de correo electrónico. El procedimiento es que el *host* 1 establece una conexión TCP con la pasarela y luego usa SMTP para transferir un mensaje 1 ahí. El *daemon* de la pasarela pone el mensaje en el buffer de mensajes destinados al *host* 2. Después se

[44] En Inglés: Simple Mail Transfer Protocol.

establece una conexión TP4 con el *host* 2 y el mensaje 2 se transfiere usando el equivalente OSI del SMTP. Todo lo que tiene que hacer el proceso de la pasarela es extraer los mensajes entrantes de una cola y depositarlos en otra.

4.5.5.3. Entrega final

Hasta ahora, hemos supuesto que todos los usuarios trabajan en máquinas capaces de enviar y recibir correo electrónico. Con frecuencia esta situación es falsa. Por ejemplo, en muchas compañías los usuarios trabajan en PCs de escritorio que no están en Internet y que son incapaces de recibir o enviar correo electrónico fuera de la compañía. En cambio, la compañía tiene uno o más servidores de correo electrónico que pueden enviar y recibir correo electrónico. Para enviar o recibir correo electrónico, una PC debe hablar con un servidor de correo electrónico usando alguna de clase de protocolo de entrega.

Un protocolo sencillo usado para traer correo electrónico de un buzón remoto es el **POP3** (Protocolo de Oficina Postal), que se define en el RFC 1225. Tiene comandos para que un usuario establezca una sesión, termine, obtenga mensajes y los borre.

Un protocolo más refinado es el **IMAP** (Protocolo Interactivo de Acceso a Correo), que se define en el RFC 1064. IMAP se diseñó para ayudar al usuario que tiene varias computadoras, tal vez una estación en la oficina, una PC en casa y una computadora portátil para el camino.

Un tercer protocolo de entrega es el **DMSP** (Protocolo de Sistema de Distribución de Correo), que es parte del sistema PCMAIL, y se describe en el RFC 1056. Éste no supone que todo el correo electrónico está en un servidor, como el POP3 y el IMAP. En cambio permite a los usuarios descargar correo del servidor a una estación de trabajo, PC o portátil y luego desconectarse. El correo electrónico puede leerse y contestarse estando desconectado. Al ocurrir una reconexión después, el correo electrónico se transferirá y el sistema se resincroniza.

4.5.6. Confidencialidad en el correo

Cuando un mensaje de correo electrónico se envía, entre dos sitios distantes, generalmente transitará por docenas de máquinas en el camino. Cualquiera de éstas puede leer y registrar el mensaje para su uso posterior, entonces la confiabilidad es inexistente. En las siguientes secciones estudiaremos dos sistemas de correo electrónico seguros de amplio uso, PGP y PEM.

4.5.6.1. PGP[45] (Bastante buena confidencialidad)

PGP es un paquete completo de seguridad de correo electrónico que proporciona confidencialidad, validación de identificación, firmas digitales y compresión, todo de una forma fácil de usar. Es más, el paquete completo, incluido el código fuente, se distribuye sin cargo por Internet, boletines electrónicos y redes comerciales.

El PGP intencionalmente usa algoritmos criptográficos existentes en lugar de crear nuevos; se basa en gran medida en el RSA[46], el IDEA[47] (Ver unidad 6) y MD5, todos algoritmos que han resistido

[45] En Inglés: Pretty Good Privacy.
[46] Rivest Shamir Adleman, creadores del algoritmo.

análisis extensos de colegas y no fueron diseñados ni infundidos por ninguna agencia gubernamental que estuviera tratando de debilitarlos. Para la gente que tiende a descodificar del gobierno, esta propiedad es un gran punto a favor.

El PGP maneja compresión de texto, secretos y firmas digitales, y también proporciona amplios recursos de manejo de claves. El PGP maneja tres longitudes de clave RSA. Es responsabilidad del usuario elegir la adecuada. Las longitudes son:

1. Casual (384 bits) puede ser descifrada hoy día por gente por grandes presupuestos.
2. Comercial (512 bits) podría ser descifrable por organizaciones de tres iniciales.
3. Militar (1024) indescifrable.

La administración de claves ha recibido mucha atención en el PGP, puesto que es el talón de Aquiles de todos los sistemas de seguridad. Cada usuario mantiene localmente dos estructuras de datos: un anillo de claves privadas y un anillo de claves públicas. El anillo de claves privadas contiene una o más pares de claves privada-clave pública personales. El anillo de claves públicas contiene claves públicas de los corresponsales del usuario; se requieren para cifrar las claves de mensajes asociadas a cada mensaje. Cada entrada del anillo de claves públicas contiene no sólo la clave pública, sino también su identificador de 64 bits y una indicación del nivel de confianza del usuario en la clave.

4.5.6.2. PEM[48] (Correo con confidencialidad mejorada)

En contrate con el PGP, que inicialmente fue asunto de una sola persona, nuestro segundo ejemplo en PEM es un estándar oficial de Internet y se describe en cuatro RFC: el RFC 1421 al RFC 1424. De manera muy general, en PEM cubre el mismo territorio que el PGP: confidencialidad y validación de identificación para sistemas de correos electrónicos basados en el RFC 822. Sin embargo, tienen algunas diferencias respecto al PGP en cuanto a enfoque y tecnología. A continuación describiremos el PEM y luego haremos las comparaciones con el PGP.

Asunto	PGP	PEM
¿Maneja cifrado?	Si	Si
¿Maneja validación de identificación?	Si	Si
¿Maneja no repudio?	Si	Si
¿Maneja compresión?	Si	No
¿Maneja canonización?	No	Si
¿Maneja listas de correo?	No	Si
¿Usa codificación base 64?	Si	Si
Algoritmo actual de cifrado de datos.	IDEA	DEs
Longitud de clave para cifrado de datos (bits).	128	56
Algoritmo actual para administración de claves	RSA	RSA o DES
Longitud de clave para la administración de clave	384/512/1024	Variable

[47] En Inglés: International Data Encryption Algorithm.
[48] En Inglés: Privacy Enhanced Mail.

Espacio de nombres de usuario.	Definido por usuario.	x.400
¿Se ajusta al x.509?	No	Si
¿Hay que confiar en alguien?	No	Si (ipra)
Certificación de claves.	Ad hoc.	Jerarquía ipra/pca/ca
Revocación de claves.	Fortuita.	Mejor
¿Pueden los espías leer los mensajes?	no	no
¿Pueden los espías leer las firmas?	no	si
¿Estándar Internet?	no	si
Diseñado por.	Equipo pequeño.	Comité de estándares.

FIGURA 4.20: Algunas de las semejanzas y diferencias entre el PGP y el PEM.

Los mensajes enviados usando el PEM primero se convierten en una forma canónica para que puedan tener las mismas convenciones de espacios blancos y el uso de retorno de carro y avance de línea. Esta transformación se lleva a cabo para eliminar los efectos de los agentes de transferencia de mensajes que modifican los mensajes que no son de su gusto. Sin canonización, tales modificaciones pueden afectar las dispersiones de los mensajes en sus destinos.

A continuación, se calcula una dispersión del mensaje usando MD2 o MD5. No es opcional, como en PGP. Después se cifra la concatenación de la dispersión y el mensaje usando DES[49]. En vista de las debilidades conocidas de una clave de 56 bits, esta selección es ciertamente sospechosa. El mensaje cifrado puede entonces codificarse con codificación base 64 y transmitirse al destinatario. Las listas de correo se reconocen explícitamente.

Como el PGP, cada mensaje se cifra con una clave de una sola vez que se incorpora en el mensaje. La clave puede protegerse mediante un RSA o un DES triple usando un EDE. En la práctica, todos usan RSA, por lo que nos concentraremos en él. De hecho, tenemos que hacerlo: el PEM no indica cómo se debe hacer la administración de la clave con DES.

La administración de las claves en el PEM es más estructurada. Las claves se certifican mediante autoridades certificadoras que producen certificados indicando el nombre del usuario, su clave pública y la expiración de la clave. Cada certificado tiene un número de serie único que lo identifica. Los certificados incluyen una dispersión MD5 firmada por la clave privada de la autoridad certificadora.

El PGP tiene un esquema parecido, pero tiene un problema: ¿debe creer un usuario en la autoridad certificadora?. El PEM resuelve este problema certificando las autoridades certificadoras, usando lo que se llama PCA[50] (Autoridades de Certificadoras de Políticas). Éstas por su parte son certificadas por el IPRA[51] (Autoridad de Registro de Políticas de Internet), que es el máximo árbitro sobre quién es bueno y quién es malo.

Cada PCA debe definir una política oficial en el momento de registrarse y archivarla con la IPRA. Estas declaraciones deben ser firmadas por el IPRA y hacerse públicas. Otra PCA podría aceptar registros

[49] En Inglés: Data Encryption Standard.
[50] En Inglés: Policy Certification Authorities.
[51] En Inglés: Internet Policy Registration Authority.

por correo electrónico de complementos extraños. Al hacer públicas las declaraciones de políticas, los usuarios tienen una base para decidir en qué autoridades deben confiar. No se ha tomado ninguna medida para asegurar que las políticas realmente se pongan en práctica.

Se contemplan tres tipos autoridades certificadoras. Una **autoridad organizacional** puede emitir certificados para sus empleados. La mayoría de las compañías operan su propia autoridad. Una **residencial** operará en nombre de ciudadanos comunes, de manera parecida a los proveedores de servicios de Internet, que proporcionan servicio a cualquiera que está dispuesto a pagarlo. Por último, hay un esquema planeado para cada **registro anónimo**. Con todas estas autoridades certificadoras por ahí, debe quedar clara la necesidad de que las PCA las vigilen de cerca. Aunque es rígidamente jerárquico y burocrático, este esquema tiene la ventaja respecto del PGP de hacer potencialmente práctica la revocación de certificados. Se requiere la revocación de un certificado si un usuario quiere cambiar su clave pública. La evocación se logra cuando un usuario dice a la autoridad certificadora que su clave pública está comprometida (o posiblemente al revés). La autoridad certificadora entonces agrega el número de serie del certificado que ha dejado de ser válido a una lista de certificados revocados, lo firma y distribuye la lista para todo el mundo.

4.6. World Wide Web

La World Wide Web es un armazón arquitectónico para acceder a los documentos vinculados distribuidos en miles de máquinas de toda la Internet; en cinco años, pasó de ser una manera de distribuir datos sobre física de alta energía a la aplicación que millones de personas piensan que es "La Internet". Su enorme popularidad se deriva del hecho que tiene una interfaz gráfica atractiva que es fácil de usar por los principiantes y proporciona un enorme cúmulo de información sobre casi cualquier tema concebible, desde aborígenes hasta zoología.

La Web, también conocida como WWW, comenzó en 1989 en el CERN (Centro Europeo de Investigación Nuclear). El CERN tiene varios aceleradores en el que los científicos de los países europeos participantes llevan a cabo investigaciones sobre física de partículas. La Web surgió de la necesidad de que estos grandes grupos de investigadores, dispersos internacionalmente, colaboraran usando un conjunto siempre cambiante de informes, planos, dibujos, fotos y otros documentos.

En las siguientes secciones describiremos la Web desde el punto de vista del usuario y, especialmente su funcionamiento interno. Puesto que la Web básicamente es un sistema cliente servidor, estudiaremos tanto el lado del cliente como el lado del servidor.

4.6.1. Del lado del cliente

Desde el punto de vista del usuario, la Web consiste en un enorme conjunto a nivel mundial de documentos generalmente llamados páginas. Cada página puede contener vínculos (apuntadores), con otras páginas relacionadas en cualquier lugar del mundo. Los usuarios pueden seguir un vínculo, lo que los lleva a la página apuntada. Este proceso puede repetirse indefinidamente, posiblemente atravesando miles de páginas vinculadas al hacerlo. Se dicen que las páginas que apuntan a otras páginas usan hipertexto.

Las páginas se ven mediante un programa llamado visor (*browser*); Internet Explorer y Netscape Navigator son dos de los más populares. El visor obtiene la página solicitada, interpreta el texto y los

comandos de formateo que contiene y exhibe la página adecuadamente formateada en la pantalla. En **figura 4.24 (a)** se da un ejemplo. Al igual que muchas páginas de la WEB, ésta comienza con un título, contiene cierta información y termina con el correo electrónico del encargado del mantenimiento de la página. Las cadenas de texto que son vínculos a otras páginas, llamadas hipervínculos (*hyperlinks*), se resaltan, ya sea mediante subrayado, presentación en un color especial, o ambas cosas. Para seguir un vínculo, el usuario coloca el cursor en el área resaltada, y la selecciona. Aunque existen visores no gráficos, como Lynux, no son tan comunes como los visores gráficos. También se están desarrollando visores basados en voz.

La mayoría de los visores tienen muchos botones y características que simplifican la navegación en la Web.

Las páginas también pueden almacenarse en disco o imprimirse. Además de tener texto normal (no subrayado) e hipertexto (subrayado), las páginas de la Web también pueden contener iconos, dibujos de líneas, mapas y monografías. Cada uno de éstos puede vincularse (opcionalmente) con otra página. En al caso de imágenes, como fotografías y mapas, la página que se trae a continuación puede depender de la parte de la imagen en donde se hizo clic.

No todas las páginas pueden visualizarse en forma convencional. Por ejemplo, algunas páginas consisten en pistas de audio, fragmentos de video o ambas cosas. El resultado de mezclar páginas de video con otros medios se llama hipermedia. Algunos visores pueden presentar, todos los tipos de hipermedia, pero otros no; en vez de ello revisan un archivo de configuración para ver la manera de manejar los datos recibidos.

Algunas páginas de Web contienen formas que solicitan información al usuario. Las aplicaciones típicas para estas formas son la búsqueda de elementos proporcionados por el usuario en una base de datos, la colocación de pedido de un producto y la participación en una encuesta de opinión. Otras páginas Web contienen páginas que le permiten a los usuarios hacer clic en ellos para exhibir acercamientos u obtener información sobre alguna zona geográfica.

Para ser *host* de un visor de la Web, una máquina debe estar directamente en Internet o por lo menos, tener una conexión SLIP[52] o PPP[53] con un enrutador u otra máquina conectada directamente a Internet. Este requisito existe porque la manera en que un visor trae una página, es estableciendo una conexión TCP con la máquina en donde se encuentra la página, y luego enviando un mensaje a través de la conexión solicitando la página. Un visor no funcionará si no puede establecer una conexión TCP a una máquina arbitraria de Internet.

4.6.2. Del lado del servidor

Cada instalación de la Web, tiene un proceso servidor que escucha en el puerto TCP 80, esperando conexiones entrantes de los clientes. Tras establecerse una conexión, el cliente envía una solicitud y el servidor envía una respuesta. Después se libera una conexión. El protocolo que define las solicitudes y respuestas legales se llama HTTP (Protocolo de transferencia de hipertexto).

[52] IP de Línea en Serie. En Inglés: Serial Line Internet Protocol.
[53] Protocolo Punto a Punto. En Inglés: Point to Point Protocol.

Los pasos que se ejecutan entre el clic del usuario y la presentación de la página son los siguientes:

1. El visualizador determina el URL[54] (viendo lo que se seleccionó).
2. El visualizador solicita al DNS la dirección IP.
3. El DNS contesta.
4. El visualizador establece una conexión TCP con el puerto 80.
5. A continuación, el visualizador emite un comando GET.
6. El servidor envía el archivo.
7. Se libera la conexión TCP.
8. El visualizador presenta todo el texto del archivo.
9. El visualizador trae y presta todas las imágenes del archivo.

4.6.3. HTTP[55] (Protocolo de transferencia de hipertexto)

El protocolo estándar de transferencia de la Web es el HTTP. Cada iteración consiste en una solicitud ASCII seguida de una respuesta tipo MIME RFC 822. Aunque es muy común el uso del TCP para la conexión de transporte, no es requerido formalmente por el estándar. Si las redes ATM, se vuelven lo bastante confiables, las solicitudes y respuestas http podrían transportarse igualmente mensaje AAL 5.

Este protocolo consiste en dos elementos bastante diferentes: el grupo de visualizadores a los servidores y el grupo de respuesta en el otro sentido. Aunque el HTTP se diseñó para usarse en la Web, ha sido intencionalmente más general de lo necesario con miras de aplicaciones futuras orientadas a objetos. Por esta razón, la primera palabra de la línea de solicitud completa es sencillamente el nombre del método (comando) a ejecutar en la página Web. Los métodos interconstruidos se listan en la **figura 4.26**.

Método	Descripción
Get	Solicita leer una página web.
Head	Solicita leer la cabecera una página web.
Put	Solicita almacenar una página web.
-post	Adiciona a un recurso nombrado.
Delete	Elimina la página web.
Link	Conecta dos recursos existentes.
Unlink	Rompe una conexión existente entre dos recursos.

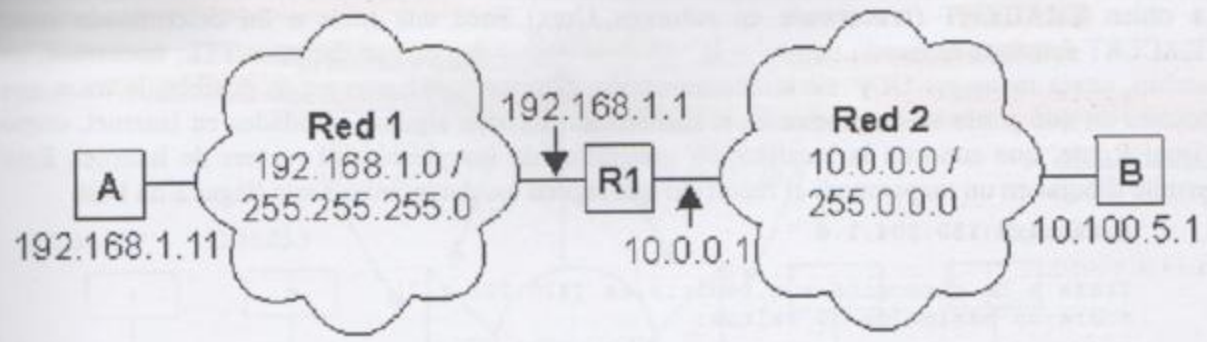
FIGURA 4.26: Métodos de solicitud HTTP interconstruidos.

[54] Localizador de uniforme de recursos. En Inglés: Uniform Resource Locator.
[55] [55] En Inglés: HiperText Trasnfer Protocol.

ÍNDICE

UNIDAD 1:
Arquitectura de Redes **11**
1.1. Concepto de Red de Telecomunicación 12
1.2. Red Informática 12
1.3. Componentes de una Red de Computadoras 14
1.4. Ventajas de las Redes 15
1.5. Aplicaciones de las Redes 15
1.6. Ejemplos de Redes de Telecomunicación 16
1.6.1. La Red Telefónica 16
1.6.2. La red de CATV 16
1.7. Concepto de Teleinformática 20
1.7.1. Evolución de los Sistemas Telemáticos 20
1.8. Clasificación de las Redes de Telecomunicación 21
1.8.1. De acuerdo con el Tipo de Transmisión 21
1.8.2. De acuerdo con su propiedad 22
1.8.3. De acuerdo con el Tipo de Tráfico 23
1.8.4. De acuerdo a su Cobertura Geográfica 23
1.9. Estructura de una red de computadoras 25
1.9.1. Estructura de una LAN 25
1.9.2. Estructura de una WAN 26
1.10. Topologías de Redes 27
1.10.1. Topologías Físicas 27
1.11. Red Corporativa 34
1.12. Estandarización de redes 37
1.12.1. Necesidad de la estandarización 37
1.12.2. Tipos de Estándares existentes 38
1.12.3. Quién es quién en el mundo de las Telecomunicaciones 38
1.12.4. Quién es quién en el mundo de los Estándares Internacionales 40
1.12.5. Quién es quién en el mundo de los Estándares de Internet 42
1.13. Arquitectura de Redes 44
1.13.1. Modelo de referencia OSI 44
1.13.2. Modelo TCP/IP 52
Preguntas de Repaso a la Unidad 1 55
Bibliografía de la Unidad 1 59

UNIDAD 2:
Capa de Acceso de Host a Red **61**
2.1. Concepto de Red de Área Local 62
2.2. Elementos de una red LAN 62
2.2.1. Enlace de comunicaciones 63




```
A>ping 10.100.5.1
```

- `Respuesta`. El cableado entre A y B, las tarjetas de red de A, R1 y B, y la configuración IP de A, R1 y B están correctos. El router R1 permite el tráfico de datagramas IP en los dos sentidos.
- `Tiempo de espera agotado`. Comprobar el host B y el cableado entre R1 y B. Para asegurarnos que el router R1 está funcionando correctamente haremos `A>ping 192.168.1.1`
- `Host de destino inaccesible`. Comprobar el router R1 y la configuración IP de A (probablemente la puerta de salida no sea 192.168.1.1). Recordemos que la puerta de salida (*gateway*) de una red es un host de su propia red que se utiliza para salir a otras redes.
- `Error`. Probablemente estén mal instalados los protocolos TCP/IP del host A. Probar `A>ping 127.0.0.1` para asegurarse.

En el caso producirse errores de comunicación en una red de redes con más de un router (Internet es el mejor ejemplo), se suele utilizar el comando PING para ir diagnosticando los distintos routers desde el destino hasta el origen y descubrir así si el fallo es responsabilidad de la red de destino, de una red intermedia o de nuestra red.

Mensajes ICMP de tiempo excedido

Los datagramas IP tienen un **campo TTL** (tiempo de vida) que impide que un mensaje esté dando vueltas indefinidamente por la red de redes. El número contenido en este campo disminuye en una unidad cada vez que el datagrama atraviesa un router. Cuando el TTL de un datagrama llega a 0, éste se descarta y se envía un mensaje ICMP de tipo 11 (*Time Exceeded*) para informar al origen.

Los mensajes ICMP de tipo 11 se pueden utilizar para hacer una traza del camino que siguen los datagramas hasta llegar a su destino. ¿Cómo? Enviando una secuencia de datagramas con TTL=1, TTL=2, TTL=3, TTL=4, etc... hasta alcanzar el host o superar el límite de saltos (30 si no se indica lo contrario).

El primer datagrama caducará al atravesar el primer router y se devolverá un mensaje ICMP de tipo 11 informando al origen del router que descartó el datagrama. El segundo datagrama hará lo propio con el segundo router y así sucesivamente. Los mensajes ICMP recibidos permiten definir la traza.