UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

MANUAL DE REDES

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO MECÁNICO ELECTRICISTA

P R E S E N T A:

JUAN GABRIEL QUILLO DUARTE

MÉXICO, ESTADO DE MÉXICO **2009**

*A MIS PADRES **IRENE** Y **RAMON** QUE ME DIERON LA DICHA DE HABER VENIDO A ESTE MUNDO.*
*MI ESPOSA **VIRGINIA** QUE SIEMPRE HA ESTADO CONMIGO.*
*A MIS HIJOS **RAMON** Y **FRANCISCO** QUE SON LA FUENTE DE SALIR ADELANTE SIEMPRE.*
*A MIS HERMANOS **GUADALUPE**, **PABLO**, **MIGUEL** Y **CARMEN** QUE SIEMPRE HEMOS ESTADO UNIDOS Y LOS EGUIREMOS POR MUCHOS AÑOS MAS.*
*Y ATODOS MIS **AMIGOS** QUE ME ALENTARON A SEGUIR ADELAMNTE SIEMPRE.*

SABIENDO QUE JAMAS EXISTIRA, UNA FORMA DE AGRADESER UNA VIDA DE LUCHA, SACRIFICIO Y ESFUERXO CONSTANTES, SOLO DESEO QUE COMPRENDAN QUE EL LOGRO MIO ES SUYO, QUE MIE SFUERZO ES INSPIRADO EN USTEDES Y QUE SON MI UNICO IDEAL.

CON RESPETO Y ADMIRACION.

JUAN GABRIEL QUILLO DUARTE.

MANUAL DE REDES

2.1.2.4.4.2.-Análisis de la Inductancia.
2.1.2.4.4.3.-Fuerza de Atracción.
2.1.3.-Plan de Numeración.
2.1.4.-Códigos de Marcación.
2.1.5.-Red Externa.
2.1.6.-Red Troncal.
2.1.7.-Red Principal.
2.1.8.-Red Directa.
2.1.9.-.Red Secundaria.
2.1.10.-Cajas de Distribución.
2.1.11.-Pupinización.
2.1.11.1.-Bobinas de Pupinización.
2.1.11.2.-Normas de Aplicación.
2.1.12.-Conmutación.
2.1.13.-Señalización.
2.1.13.1.-Señalización de Abonado.
2.1.13.2.-Señalización entre centrales.
2.1.13.2.1.-Señalización en Circuito.
2.1.13.2.2.-Señalización por Inversión en la Batería.
2.1.13.2.3.-Señalización E&M.
2.1.13.3.-Señalización a Corriente Alterna.
2.1.13.3.1.-Señalización dentro de Banda.
2.1.13.3.1.1.-Señalización por Impulsos.
2.1.13.3.1.2.-Señalización en Directa.
2.1.13.3.2.-Señalización Fuera de Banda.
2.1.13.4.-Señalización de Línea.
2.1.13.5.-Señalización de Registro.
2.1.13.6.-Señalización Multifrecuencia.
2.1.7.-Introducción al Dimensionamiento de Centros de Conmutación.
2.1.7.1.-Sistemas de Pérdida y Sistemas de Espera.
2.1.7.2.-Fórmula de Bernoulli.
2.1.7.3.- Fórmula de Poisson.
2.1.7.4.-Cantidades y Unidades de la Teoría de Tráfico.
2.1.7.5.-Generación de Tráfico.
2.1.7.6.-Hora de Máximo Tráfico.
2.1.7.7.-Fórmula de Erlang.
2.1.7.7.1.-Grupos de Troncales de Accesibilidad Completa.
2.1.7.7.2.-Grupos de Troncales de Accesibilidad Limitada.
2.1.7.8.-Redes de Conmutación de Varias Etapas.
2.1.7.9.-Características de los Sistemas de Retardo.
2.1.8.-Servicios Ofrecidos por la Red Telefónica Básica.
2.1.8.1.-Telefonía Básica.
2.1.8.1.1.-Números de Servicio.
2.1.8.2.-Telefonía Pública.
2.1.8.3.-Línea Multiservicio.
2.1.8.4.-Servicios Suplementarios Selectivos, (CLASS).
2.1.8.5.-Servicios de Teleconferencia.
2.1.8.5.1.-Audioconferencia Básica.
2.1.8.5.2.-Audioconferencia de Calidad Especial.
2.1.8.5.3.-Multiconferencia.
2.1.8.5.4.-Teleconferencia Audiográfica.
2.1.8.6.-Pictogramas y Símbolos para Ayudar a los Usuarios del Servicio Telefónico.
2.1.8.6.1.-Pictogramas para Ayudar a la Identificación de la Información.
2.1.8.6.2.-Pictogramas para Ayudar en la utilización de un Servicio Público.
2.1.8.6.3.-Pictogramas para Ayudar A la Identificación de los Servicios Ofrecidos a los Abonados Telefónicos.

2.2.-Evolución de las Redes Telefónicas.
2.3.-PCM y TDM.
2.3.1.-Introducción.
2.3.2.-Teorema del Muestreo.
2.3.3.-Sistema Básico de Transmisión.
2.3.4.-Muestreo.
2.3.5.-Cuantificación.
2.3.5.1.-Ruido de Cuantificación.
2.3.5.2.-Curva de Cuantificación Lineal.
2.3.6.-Codificación.
2.3.6.1.-Codificación de los Pulsos PAM en una Palabra de 8 Bits.
2.3.7.-Período y velocidad de Muestreo.
2.3.8.-Multiplexación TDM de los Canales Telefónicos.
2.3.9.-Decodificación de las Señales PCM.
2.3.10.-Formación de Sistemas PCM de Jerarquía Superior.
2.4.-Las primeras Redes de Datos.
2.4.1.-Concepto de MODEM.
2.4.1.1.-Introducción.
2.4.1.2.-Tipos de Módems.
2.4.1.2.1.-Externos.
2.4.1.2.2.-Internos.
2.4.1.3.-Velocidad de Transmisión.
2.4.1.3.1.-Limitación Física de la Velocidad de Transmisión en la Línea Telefónica.
2.4.1.3.2.-Velocidades y Estándares.
2.4.1.4.-Estándares de Modulación.
2.4.1.5.-Interfaces.
2.4.1.6.-Codificación de la Información.
2.4.1.7.-Estándares de la Corrección de Errores.
2.4.1.8.-Estándares de la Compresión de Datos.
2.4.1.9.-Conexión RS-232 entre la PC y el Modem.
2.4.1.10.-Control de Flujo.
2.4.1.11.-Comandos de Control del Modem.
2.4.1.12.-Modo de Operación.
2.4.1.13.-. Nuevas Tecnologías.
2.4.1.13.1.- Nuevas Tecnologías de Módems a 56Kbps.
2.4.1.13.2.- Módems Inalámbricos, Tendencias de los Módems PCS.
2.4.2.-Aparición de los sistemas Cliente-Servidor.
2.4.2.1.-Introducción.
2.4.2.2.-Arquitectura Cliente-Servidor.
2.4.2.3.-El Cliente.
2.4.2.3.1.-Uso del Front-End.
2.4.2.3.2.-Herramientas del Front-End.
2.4.2.4.-El Servidor.
2.4.2.4.1.-Procedimientos Almacenados.
2.4.2.4.2.-Hardware del Servidor.
2.4.2.5.-Ventajas de la Arquitectura Cliente-Servidor.
2.4.2.6.-Implantación de Aplicaciones Cliente-Servidor.
2.4.2.7.-Servidores Especializados.
2.4.2.7.1.-Servidores de Archivos e Impresión.
2.4.2.7.2.-Servidores de Aplicaciones.
2.4.2.7.3.-Servidores de Correo.
2.4.2.7.4.-Servidores de fax.
2.4.2.7.5.-Servidores de Comunicaciones.
2.4.2.7.6.-Servidores de Directorio.
2.4.3.-Aparición de la Aplicación de Conmutación de paquetes en Protocolos.
2.4.4.-SNA.

2.4.4.1.-Introducción
2.4.4.2.-Conceptos Generales.
2.4.4.3.-Topología.
2.4.4.4.-Niveles de SNA.
2.4.4.5.-Comparación entre los Niveles OSI y SNA.
2.4.4.6.-Sesiones.
2.4.4.7.-Formato de Datos.
2.4.4.7.1.-Flujo Normal y Flujo Expedito.
2.4.4.7.2.-Modos de Transacción.
2.4.4.8.-Protocolos.
2.4.4.9.-TCP/IP o SNA.
2.4.4.10.-Link Station.
2.4.4.11.-Multisystem Networking Facility (MSNF)
2.4.4.12.-Modename, Límite de Sesión y Clases de Servicios.
2.4.4.13.-CNOS y Sesiones Límite.
2.4.5.-X.25.
2.4.5.1.-Introducción.
2.4.5.2.-Seguridad.
2.4.5.3.-Niveles en X.25.
2.4.5.3.1.-El Nivel Físico
2.4.5.3.2.-El Nivel de Enlace (LAP-B)
2.4.5.3.3.-El Nivel de Red.
2.4.5.3.3.1.-Introducción.
2.4.5.3.3.2.-Circuitos Virtuales.
2.4.5.3.3.3.-Protocolo.
2.4.5.3.3.4.-Número de Canal Lógico (NLC).
2.4.5.3.3.4.1.-Estado de los Canales Lógicos.
2.4.5.3.3.5.-PDU's en el Nivel de Red.
2.4.5.4.-Formato del Paquete.
2.4.5.4.1.-El Bit D.
2.4.5.4.2.-El Bit M.
2.4.5.4.3.-Paquetes A y B.
2.4.5.4.4.-El Bit Q.
2.4.5.4.5.-Establecimiento de Conexiones.
2.4.5.4.5.1.-Comunicación Establecida.
2.4.5.4.5.2.-Paquete de Petición de llamada, Llamada Entrante.
2.4.5.4.5.3.-Paquete de Llamada Aceptada y de Comunicación Establecida.
2.4.5.4.5.4.-Intercambio de Datos.
2.4.5.4.5.5.-Paquete de datos.
2.4.5.4.5.6.-Paquete de Supervisión.
2.4.5.4.5.7..-intercambio de Datos Acelerados.
2.4.5.4.6.-Reinicio y Rearranque de Conexiones.
2.4.5.4.6.1.-Reinicio.
2.4.5.4.6.2.-Rearranque.
2.4.5.4.7.-Liberación de Conexiones.
2.4.5.4.7.1.-Petición/Indicación de Liberación.
2.4.5.4.7.2 Confirmación de Liberación por parte del DTE/DCE.
2.4.5.5.-Procedimiento Multienlace.
2.4.5.6.-Normas Auxiliares de X.25.
2.4.5.7.-Principios de control de flujo.
2.4.5.8.-Facilidades en X.25.
2.4.5.9.-Otros estándares y niveles.
2.4.5.9.1.-El PAD.
2.4.5.9.2.-X.28.
24.5.9.3.-X.29.

3.-INICIO DE LA EVOLUCION TECNOLÓGICA.
3.1.-Evolución de los Medios.
3.2.-ISDN.
3.2.1.-Introducción.
3.2.2.-Ventajas.
3.2.3.-Servicios.
3.2.4.-Canales.
3.2.5.-Grupos de Funcionales y Puntos de Referencia.
3.2.5.1.-Grupos funcionales.
3.2.5.2.-Puntos de Referencia.
3.2.6.-Protocolo de Señalización.
3.3.-FDDI.
3.3.1.-Introducción.
3.3.2.-Tecnología.
3.3.3.-Niveles del Modelo OSI.
3.3.4.-Trama FDDI.
3.3.5.-Gestión de Fallos.
3.4.-Sonet.
3.4.1.-Introducción.
3.4.2.-Características.
3.4.2.1.-Red DE elementos de Sonet.
3.4.3.-Estructura del Marco Sonet STS-1.
3.4.3.1.-Multiplexaje en Sonet.
3.4.3.2.-Estructura del formato de la trama Sonet.
3.4.3.2.1.-Estructura de la trama STS-1.
3.4.3.2.2.-Estructura del SPE.
3.4.3.2.3.-Estructura de la trama STS-N.
3.4.3.2.4.-Overheads en Sonet.
3.5.-Frame Relay.
3.5.1.-Introducción.
3.5.2.-Circuitos Virtuales.
3.5.3.-Formato de la Trama Frame Relay.
3.5.4.-Formato de la Trama LMI.
3.5.5.-Mecanismos de Control de Saturación.
3.5.6.- Estandarización.
3.5.7.- Ventajas y Desventajas.
3.5.8.- Aplicaciones.

4.-NORMAS Y ESTANDARES DE REDES.
4.1.-Función de los Estándares en las Redes.
4.2.-Origen de los Estándares.
4.2.1.-La Influencia de la Comunidad Empresarial.
4.2.2.-La influencia de la Comunidad Técnica.
4.3.-Organizaciones de Estandarización.
4.3.1.-Organización Internacional de Estandarización (ISO).
4.3.1.1.-Objetivos de la ISO en Comunicaciones entre Equipos.
4.3.1.2.-El Modelo de Referencia de Interconexión OSI.
4.3.1.3.-Una Arquitectura por Niveles.
4.3.1.4.-Relación entre los Niveles del Modelo OSI.
4.3.1.5.-Paquetes de Datos y el Modelo OSI.
4.3.1.5.1.-Direccionamiento de Paquetes.
4.3.1.5.2.-Como Dirigir los Paquetes.
4.3.2.-El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).
4.3.2.1.-El Estándar IEEE 802.x.
4.3.2.2.-El Proyecto 802.
4.3.2.3.-Mejoras sobre el Modelo OSI.

6.3.2.-Servicios que se pueden ofrecer con un sistema de comunicación xDSL.
6.3.3.-Tipos de xDSL.
6.3.3.1.-ADSL.
6.3.3.2.-HDSL.
6.3.3.3.-VDSL.
6.3.3.4.-RADSL.
6.3.3.5.-SDSL.
6.4.-MPLS
6.4.1.-Introducción.
6.4.2.-Marco Teórico.
6.4.2.1.-Orígenes de MPLS.
6.4.2.2.-Funcionamiento de MPLS.
6.4.3.-El camino hacia la Convergencia de Niveles: IP sobre ATM.
6.4.4.-Un Paso más en la Convergencia hacia IP: Conmutación IP
6.4.5.-Ideas Preconcebidas sobre MPLS.
6.4.6.-Descripción Funcional de MPLS.
6.4.7.-Aplicaciones de MPLS.
6.4.7.1.-Ingeniería de Tráfico.
6.4.7.2.-Clase de Servicio (CoS).
6.4.7.3.-Redes Privadas Virtuales (VPN'S)
6.4.7.4.-Diez Razones para Migrar a MPLS/VPN.
6.5.-TCP/IP
6.5.1.-Introducción.
6.5.2.-Arquitectura de Protocolos TCP/IP.
6.5.3.-Conjunto de Protocolos TCP/IP.
6.5.4.-Descripción del Uso General de TCP/IP.
6.5.5.-Principales Protocolos de Internet.
6.5.6.-Direcciones IP.
6.5.6.1.-Clases de Redes.
6.5.6.2.-Subredes.
6.5.6.3.-Tipos de Subnetting.
6.5.6.3.1.-Subnetting Estático.
6.5.6.3.1.1.-Ejemplo de Subnetting Estático.
6.5.6.3.2.-Subnetting de Longitud Variable.
6.5.6.3.3.-Mezclando Subnetting Estático y de Longitud Variable.
6.5.6.4.-Encaminamiento IP con Subredes.
6.5.6.5.-Obteniendo una Máscara de Subred.
6.5.6.6.-Direccionando Routers y Host Multi-Homed.
6.5.6.7.-Direcciones IP Especiales.
6.5.6.8.-Unicasting, Broadcasting y Multicasting.
6.5.6.8.1.-Broadcasting.
6.5.6.8.2.-Multicasting.
6.5.7.-Protocol Internet.
6.5.7.1.-El Datagrama IP.
6.5.7.1.1.-Formato del Datagrama IP.
6.5.7.1.2.-Fragmentación.
6.5.7.1.3.-Opciones de Encaminamiento del Datagrama IP.
6.5.7.1.4.-IT (Internet Timestamp).
6.5.7.2.-Encaminamiento IP.
6.5.7.3.-Destinos Directos e Indirectos.
6.5.7.4.-Tabla de Encaminamiento IP.
6.5.7.5.-Algoritmo de Encaminamiento IP.
6.5.8.-DNS (Domain Name System).
6.5.8.1.-El Espacio de Nombres Jerárquico.
6.5.8.2.-FQDN (Fully Qualified Domain Names).
6.5.8.3.-Dominios Genéricos.

6.5.8.4.-Dominio de Países.
6.5.8.5.-Mapeando Nombres de Dominio a Direcciones IP.
6.5.8.6.-Mapeando Direcciones IP a Nombres de Dominio Consultas con Punteros.
6.5.8.7.-Otros Usos para el DNS.
6.5.9.-ARP (Address Resolution Protocol)
6.5.9.1.-Descripción de ARP.
6.5.9.2.-Concepto Detallado de ARP.
6.5.9.2.1.-Generación del Paquete ARP.
6.5.9.2.2.-Recepción del Paquete ARP.
6.5.9.2.3.-ARP y Subredes.
6.5.9.2.3.1.-Concepto de Proxy ARP.
6.5.10.-RARP (reverse Address Resolution Protocol).
6.5.10.1.-Concepto de RARP.
6.5.11.-ICMP (Internet Control Messenge Protocol).
6.5.11.1.-Mensajes ICMP.
6.5.11.2.-Echo (8) y Echo Reply (0).
6.5.11.3.-Destination Unreeachable (3).
6.5.11.4.-Source Quench (4).
6.5.11.5.-Redirect.
6.5.11.6.-Router Advertisement (9) y Router Solicitation (10).
6.5.11.7.-Time Exceeded.
6.5.11.8.-Parameter Problem (12).
6.5.11.9.-Timestamp Request (13) y Timestamp Reply (14).
6.5.11.10.-Information Request (15) e Information Reply (16).
6.5.11.11.-Address Mask Request (17) y Address Mask Reply (18).
6.5.11.12.-Aplicaciones para ICMP.
6.5.11.13.-ICMP para la Versión 6 de IP.
6.5.12.-UDP (User Datagram Protocol).
6.5.12.1.-Puertos.
6.5.12.2.-Formato del Datagrama UDP.
6.5.12.3.-Interfaz de Programación de Aplicación de UDP.
6.5.13.-TCP (transfer Control Protocol).
6.5.13.1.-Zócalos.
6.5.13.2.-Conceptos de TCP.
6.5.13.3.-El Principio de la Ventana.
6.5.13.4.-El Principio de la Ventana Aplicado a TCP.
6.5.13.5.-Formato del Mensaje en TCP.
6.5.13.6.-Reconocimientos y Retransmisiones.
6.5.13.7.-Intervalos de Timeout Variable.
6.5.13.8.-Establecimiento de una Conexión TCP.
6.5.13.9.-Segmentos TCP Transportados en Datagramas IP.
6.5.13.10.-API en TCP.
6.5.14.-Telnet.
6.5.14.1.-Funcionamiento de Telnet.
6.5.14.2.-NVT (Network Virtual Terminal).
6.5.14.3.-Opciones de Telnet.
6.5.14.4.-Estructura de Comandos de Telnet.
6.5.14.5.-Negociación de Opciones.
6.5.14.6.-Comandos Básicos de Telnet.
6.5.15.-TFTP (Trivial File Transfer Protocol).
6.5.15.1.-Uso de TFTP.
6.5.15.2.-Descripción del Protocolo TFTP.
6.5.15.3.-Paquetes TFTP.
6.5.15.4.-Modos de Transferencia.
6.5.16.-FTP (File Transfer Protocol).
6.5.16.1.-Descripción de FTP.

6.5.16.2.-Operaciones de FTP.
6.5.16.2.1.-Conexión a un Host Remoto.
6.5.16.2.2.-Selección de un Directorio.
6.5.16.2.3.-Listado de Ficheros Disponibles para una Transferencia.
6.5.16.2.4.-Especificación del Modo de Transferencia.
6.5.16.2.5.-Copia de Ficheros.
6.5.16.2.6.-Finalización de la Sesión de Transferencia.
6.5.16.3.-Códigos de Respuesta.
6.5.16.4.-Ejemplo de una Sesión.
6.5.16.5.-FTP Anónimo.
6.5.17.-SMTP (Simple Mail Transfer Protocol).
6.5.17.1.-Funcionamiento de SMTP.
6.5.17.1.1.-Formato de la Cabecera.
6.5.17.1.2.-Intercambio de Correo SMTP.
6.5.17.2.-SMTP y el DNS.
6.5.17.3.-Servidor de Correo POP (Post Office Protocol).
6.5.17.3.1.-Direccionando Buzones en Servidores.
6.5.17.3.2.-Gateways SMTP.
6.5.18.-SNMP (Simple Network Management Protocol).
6.5.18.1.-SMI (Structure and Identification of Management Information).
6.5.18.2.-MIB (Management Information Protocol)-
6.5.18.2.1.-Descripción.
6.5.18.3.-SNMP.
6.5.18.4.-CMOT (Common Management Information Protocol Over TCP/IP).
6.5.18.5.-El DPI de SNMP (SNMP Distributed Programming Interface).
6.5.18.6.-SNMPv2 (SNMP Versión 2).
6.5.18.6.1.-Entidad SNMpv2.
6.5.18.6.2.-Entorno de Gestión (SNMPv2 Party o EG).
6.5.18.6.3.-GetBulkRequest.
6.5.18.6.4.-Inform Request.
6.5.18.7.-El MIB para SNMPv2.
6.5.18.8.-eg del MIB (Party MIB).
6.5.18.8.1.-MIB Manager-Manager.
6.5.18.9.-SAPP (Single Authentification and Privacy Protocol).
6.5.18.10.-El Nuevo Modelo Administrativo.
6.6.-WIRELESS.
6.6.1.-Antecedentes
6.6.2.-Concepto de Telefonía Móvil.
6.6.3.-Concepto de Internet, El Modelo World Wide Web.
6.6.4.-Marco Teórico.
6.6.4.1.-Concepto de WAP.
6.6.4.2.-Descripción de WAP.
6.6.4.3.-Modelo WAP.
6.6.5.-Arquitectura WAP.
6.6.5.1.-Capa de Aplicación (WAE).
6.6.5.2.-Capa de Sesión (WSP).
6.6.5.3.-Capa de Transacciones (WTP).
6.6.5.4.-Capa de Seguridad (WTLS).
6.6.5.5.-Capa de Transporte (WPD).
6.6.6.-Uso y Aplicaciones de WAP.
6.6.6.1.-Aplicación de Telefonía Inalámbrica.
6.6.6.1.1.-Vistazo General a la Arquitectura.
6.6.6.1.2.-Los Agentes de Usuario WTA y WAE.
6.6.6.1.3.-Servidor WAT.
6.6.6.1.4.-Servicios WAT.
6.6.6.1.5.-Iniciación de Servicios WAT.

C2.2.1.-Direcciones Global Unicast.
C3.-Paquetes.
C3.1.-Cabeceras Extendidas.
C3.1.1.-Orden de las Cabeceras.
C3.2.-Fragmentación.
C4.-IPv6 y el Sistema de Nombres de Dominio.
C5.-IPSec.
C5.1.-El Problema de la Seguridad en Internet.
C5.2.-Seguridad en IPv6.
C5.3.-Calidad de Servicio (QoS).
C5.4.-Servicios Ofrecidos por IPSec.
C5.5.-Protocolos Usados por IPSec.
C6.-Despliegue.
C6.1.-Mecanismos de Transición a IPv6.
C6.2.-Ventajas.
C6.3.-Desventajas.

D.-VoIP
D1.-Conceptos.
D1.1.-Introducción.
D1.2.-Definición.
D1.3.-Como se Usa La VoIP.
D1.4.-Elementos de la VoIP.
D1.5.-Características de la VoIP.
D1.6.-Protocolos de VoIP.
D1.7.-El Estándar de VoIP.
D1.8.-Pila de Protocolos en VoIP.
D1.9.-Arquitectura de Red.
D1.10.-Calidad De Servicio.
D1.11.-Aplicaciones de VoIP
D1.12.-Inicios de la Tecnología de VoIP.
D1.12.1.-Inicios.
D1.12.2.-El Mercado de Servicios De VoIP: es tan sólo el comienzo.
D1.12.3.-Las Primeras Barreras.
D1.12.4.-El Mercado Decide.
D1.12.5.-Comparación de VoIP y Telefonía Tradicional.
D1.12.6.-Telefonía Tradicional.
D1.12.6.1.-Arquitectura de una Central Telefónica.
D1.12.6.2.-Procesamiento de Llamadas.
D1.12.6.3.-Conexión Entre Centrales.
D1.12.6.4.-Ruteo, Señalización y Protocolos.
D1.12.6.4.1.-Codificación de la Voz.
D1.12.6.4.2.-Señalización.
D1.12.6.4.3.-Ejemplo de Conexión VoIP Usando IP.
D1.12.6.4.4.-Conexión de Muchas Computadoras.
D1.12.6.4.5.-Implementaciones.
D1.12.6.4.6.-PBX.
D1.13.-Ventajas y Desventajas que Presenta la Solución de VoIP con Respecto a la Telefonía Tradicional.
D1.13.1.-Ventajas.
D1.13.2.-Desventajas.
D1.14.-Telefonía Sobre IP: Como Cambiarle la Cara a las Telecomunicaciones.
D1.15.-Como Funciona la VoIP.
D1.16.-La Promesa de VoIP: Mejorar la Calidad de la Voz.
D1.17.-La Voz Sobre Internet.
D1.18.-Una Línea para Dos Comunicaciones.

D.2.-Seguridad para Sistemas de VoIP.
D2.1.-Seguridad en las Comunicaciones IP.
D2.2.-Seguridad en el Protocolo VoIP.
D2.2.1.-Amenazas.
D2.2.2.-Spoofing.
D2.2.3.-Herramientas del Hacker.
D2.3.-Defenderse.
D2.4.-IPSec.
D2.4.1.-Los protocolos IPSec.
D2.4.1.1.-Cabecera de Autentificación (AH).
D2.4.1.2.-Carga de Seguridad Encapsulada (ESP).
D2.4.1.3.-El Protocolo IKE.
D2.4.2.-Firewalls.
D2.4.3.-Redes Privadas Virtuales.
D2.5.-Seguridad en los Sistemas de VoIP.
D3.-Presente y Futuro de las Comunicaciones IP.
D3.1.-Empresas Relacionadas con los Estándares VoIP.
D3.1.1.-3Com Corporation y Siemens Communication Networks.
D3.1.2.-Cisco.
D3.1.3.-Motorola
D3.2.-La Solución de VoIP de 3Com.
D3.2.1.-Gateway de VoIP.
D3.2.2.-Gatekeeper de VoIP.
D3.2.3.-Servidores de Backend.
D3.2.4.-Otras Soluciones de VoIp de 3Com.
D3.3.-Futuro de la Tecnología de VoIP.
D3.3.1.-Las Predicciones del Mercado.

8.-CONCLUSIONES.

9.-BIBLIOGRAFIA.

I.-INTRODUCCION

1.1 CONCEPTOS GENERALES DE REDES

1.2 DEFINICION DE RED

Una red es un conjunto de medios y equipos interconectados para proporcionar servicios de telecomunicación entre cierto número de ubicaciones. Una ubicación (fija o móvil) es conocida como punto de terminación de red o simplemente **PTR**. Así pues, podríamos ver una red como algo abstracto que ofrece un determinado servicio en puntos de terminación de red.

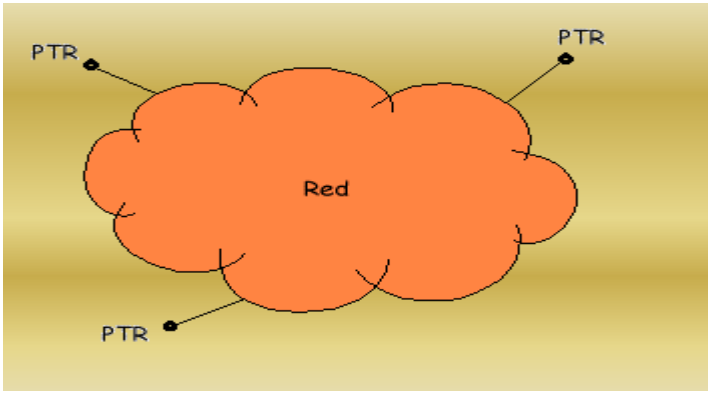


Figura 1 Red.

Dentro de esta especie de 'nube' que acabamos de dibujar existen normalmente recursos de transmisión y recursos de conmutación. Los recursos de transmisión más utilizados son los de tipo punto a punto dedicados y la conmutación se produce en nodos. Asociado a una red hay un operador, nombre que recibe quien gestiona u opera la red; es el encargado de reparar, extraer medidas, mantener la red, y a veces sacar un beneficio económico por la explotación de los servicios. Conviene aclarar también, la confusión que trae el término subred. Una subred no es una red de poca importancia, como podría dar a entender el prefijo **sub**. El modelo OSI llama subred a la infraestructura que acabamos de definir como red.

1.2.1 PARAMETROS.

Los parámetros más importantes que caracterizan una red son:

- **De servicio:**

  a) **Cadencia Efectiva (Cef).** También denominado Throughput o Caudal.-Es la cantidad de bps (bits por segundo) que se pueden introducir a la red en el punto de terminación de red (PTR), es decir, el ritmo al cual la red acepta información. La definición sólo habla de lo que ocurre en un extremo de la red, y no de la cantidad de bits que van de un extremo a otro de la red en un segundo. Por tanto, es importante no confundir que la cadencia sea 9,600bps con que 9,600 bits atraviesen la red en un segundo. Además, es necesario señalar que la **capacidad nominal** del enlace (**C**) y la cadencia no son lo mismo. `C` es toda la capacidad que brinda el enlace y como hay recursos compartidos en la red (enlaces y nodos), ocurre que Cef<C. Cef no es un valor determinista, puesto que depende del estado de la red, y por tanto es muy difícil de predecir.

  b) **El Retardo de tránsito (T).**-Es el tiempo que transcurre desde que la red recoge un bit en el punto de terminación de red origen hasta que se recibe en el PTR destino. Este tiempo T siempre será mayor que el tiempo de propagación de la señal. En principio Cef y T son dos magnitudes independientes; una tubería puede ser ancha y corta (Cef alto y T bajo), o larga y estrecha (Cef bajo y T alto). Suele ocurrir que si T es alto fuerza a que Cef sea pequeño, por las razones que se exponen a continuación. Al producto **Cef*T** se le llama **Memoria de la red**, y expresa el número de bits en tránsito, pues es la cantidad de información que ha salido del origen, pero no ha llegado a destino, luego está en la red. Para saber si un bit ha llegado bien y no hay que retransmitirlo, es necesario esperar un tiempo 2*T (o bien T1+T2 si los trayectos son asimétricos), llamado **Round Trip Delay (Retardo de ida y vuelta**); luego en el origen se han de almacenar al menos Cef*2T bits

para el caso en que se haya de retransmitir, y esto implica un uso de memoria muy grande si T y Cef son muy altos.

c) **La tasa de fallos**.-Se caracteriza por medio de la **Probabilidad de Error en bit** (**Pe**), esto es, la probabilidad de que un bit no llegue correctamente a su destino. Los fallos pueden ser debidos a pérdidas, corrupción, duplicación y desórdenes en bits o paquetes. Muchos de éstos son debidos a que el software de comunicaciones no puede responder ante todas las situaciones posibles, pues suele trabajar sobre complejos sistemas distribuidos. El uso de códigos reduce la tasa de fallos, pero no puede hacer nada si el sistema está indisponible, por ejemplo, si se caen los enlaces que conectan un nodo con el resto, dicho nodo está incomunicado.

d) **La Disponibilidad del Servicio.**-Viene determinada por el tanto por ciento del tiempo en que el servicio está funcionando (disponible). 100% es el límite ideal al que se debe intentar llegar.

e) **La Cobertura.-**Corresponde al área de alcance del servicio que proporciona la red. Es, en otras palabras, una enumeración de los puntos de terminación de red, dónde es posible usar la red. Un ejemplo de esto son los listines telefónicos que nos citan los puntos de terminación de red de la red telefónica básica, y por tanto implícitamente la cobertura de la red.

- **De Precio**:

El precio de los servicios de telecomunicación se compone generalmente de:

a) **Un alta.-**Precio que se paga por convertirse en usuario del servicio.

b) **Una factura mensual.-**Compuesta por una parte fija y por una parte variable .Ésta última se corresponde con la actividad desarrollada por el usuario, y puede depender de varios aspectos como el número de paquetes enviados, tiempo que está establecida la conexión, distancia de la comunicación, etc..

Existe una normativa europea que establece que los precios deben estar orientados a los costos. Esto quiere decir que, por ejemplo, para el alta y la parte fija mensual, los precios deben amortizar las inversiones, y que para la parte variable mensual debe pagar más el que más utiliza la red.

1.2.2 CLASIFICACION

Son muchos los criterios en función de los cuales podemos clasificar las redes. Aquí nos fijaremos sólo algunos de ellos, que son:

a) **Su objetivo empresarial.**-Las redes pueden ser **privadas** o **públicas**. Las primeras no buscan un beneficio económico sino una mejora en las herramientas de trabajo de una determinada empresa u organismo, mientras que las segundas sí persiguen ese beneficio. En otras palabras, sólo los usuarios de redes públicas se ven obligados a pagar por su utilización.

b) **Su cobertura.**-En virtud de la cobertura diferenciamos tres categorías:

- **LAN** (*L*ocal *A*rea *N*etwork): Redes de área local. Pueden abarcar una distancia de unos pocos metros (entorno de una habitación) o hasta cubrir un edificio, o como máximo unos pocos edificios cercanos entre sí (por ejemplo, el entorno de un campús universitario).
- **MAN** (*M*etropolitan *A*rea *N*etwork): Abarcan un área intermedia entre las LAN's y las WAN's. Se habla por tanto de ciudades como cobertura.
- **WAN** (*W*ide *A*rea *N*etwork): Es la red de mayor cobertura, llegando a cubrir el área de todo un país, un continente o incluso más.

c) **Sus características físicas:**

- **Sin tarjetas.-**Las estaciones que la forman se conectan entre sí a través de un puerto serie. Para ello se emplean unos puertos denominados multipuertos series.
- **Punto a Punto.**-La componen dos estaciones conectadas directamente entre sí. Es un tipo de red que se puede emplear con Windows sin necesidad de instalar ningún software especial para gestión de redes.

- **Entre Iguales.**-Es similar al anterior, con la diferencia de que este tipo de red intervienen dos o más estaciones que comparten la información entre ellos. Este tipo de red es muy utilizado bajo Windows.
- **Cliente-Servidor**.-Es el tipo de red más empleado. Esta compuesta por varias estaciones conectadas a un servidor.

1.2.3 COMPONENTES DE UNA RED

Los componentes de una red son, fundamentalmente, los siguientes:

- **Estaciones de Trabajo**.-Pueden ser de dos tipos:
  a) **Terminales Tontas**.-Denominadas de este modo porque usan todos los recursos del servidor, su sistema operativo y sus programas, es decir, los programas se ejecutan en el servidor. La terminal se compone básicamente de teclado y monitor (no tiene procesador propio), por ejemplo: las terminales del sistema AS/400 de IBM.
  b) **Estaciones con su Propio Sistema Operativo**.-Son estacione que se pueden trabajar también de forma independiente, por ejemplo: una PC.
- **Servidores**.-Un servidor es una estación central de una red, y es más potente que las estaciones a él conectadas. Dispone de un software especial que le permite trabajar como un servidor de red. Los servidores pueden ser de tres tipos:
  a) **De Información (Datos)**.-Mantienen los archivos en subdirectorios privados y compartidos para los usuarios de la red.
  b) **De Impresión**.-Gestionan las impresoras que tienen conectadas y permiten su uso por los diversos usuarios.
  c) **De Comunicaciones**.-Permiten enlazar diferentes redes de áreas locales.

  Aunque un mismo servidor, mediante el correspondiente software, puede desarrollar estas funciones simultáneamente, en redes de gran tamaño (a partir de 15 usuarios) es recomendable disponer de un servidor para cada tarea.
- **Usuario Final**.-Es la fuente o el destino del mensaje en la red; un usuario final no es necesariamente una persona, puede ser un programa de aplicación interactuando con otra aplicación, un usuario de terminal.
- **Ruta de Acceso**.-Es la conexión entre los dos usuarios finales que les permite a ellos comunicarse.
- **Nodo**.-Es una caja física que puede aceptar y redireccionar mensajes a lo largo de una ruta de acceso, puede ser una computadora o un controlador de terminal.

1.2.4 VENTAJAS DE LAS REDES

Las ventajas más importantes del trabajo en red son:

- Permite compartir periféricos de alto costo, tales como impresoras láser, a color, scaners, plotters.
- Evita la duplicidad de trabajos.
- Permite el uso de correo electrónico entre las estaciones.
- Permite sustituir a los mainframes (minicomputadoras), tales como el AS/400 de IBM.
- Permite el acceso de Internet.
- Cada usuario puede tener el nivel propio de seguridad y de acceso a los datos.
- Permitir la comunicación entre los elementos que conforman la red. Al estar interconectados diferentes estaciones pueden intercambiar información, datos o mensajes entre sí.
- La conexión entre dos estaciones, establece un canal permanente para la comunicación.

- Mayor fiabilidad.
- Ahorro de dinero.
- Flexibilidad de cambio ante fallos.
- La comunicación se puede establecer entre estaciones con diferente Sistema Operativo, usando sus respectivos protocolos.

1.2.5 FORMAS DE COMUNICACIÓN

- **Canales de Difusión**.-Hay un único canal de comunicación, que es compartido por todas las estaciones de la red. Maneja mensajes cortos llamados paquetes, estos son mandados por una estación y recibidos por otras, en contexto seguro. El paquete contiene una dirección que específica para quien es, cada estación cuando lo recibe, checa si es para ella, en caso afirmativo lo acepta, en caso contrario lo rechaza.
- **Punto a Punto**.-las redes contienen varias líneas que conectan estaciones, si dos de ellas desean comunicarse y no hay un canal directo que las una, lo realizan por medio de estaciones intermedias. Cada una de estas últimas recibe íntegramente el paquete y lo almacena esperando una línea libre de salida para retransmitirlo.

1.3 DEFINICION DE PROTOCOLO

Protocolo es un conjunto formal de convenciones y reglas, que establecen como las estaciones deben comunicarse a través de las redes, reduciendo al mínimo los errores de transmisión. Estos transmiten la información fragmentada, de esta manera ninguna transmisión, por grande que sea, monopoliza los servicios de red.

Un protocolo describe:

- El tiempo relativo al intercambio de mensajes entre dos sistemas de comunicaciones.
- El formato que el mensaje debe tener para el intercambio entre dos estaciones, que usan protocolos diferentes, se puedan establecer.
- Que acciones a tomar en caso de producirse errores.
- Las acciones hechas acerca del medio ambiente en el cual el protocolo se esta ejecutando.
- Los distintos protocolos determinan el contexto del Intercambio de Mensajes (correo electrónico), de las conexiones remotas (telnet), o la transferencia de archivos (FTP), entre otras actividades de las redes.
- Diferentes tipos de redes se pueden comunicar a pesar de sus diferencias, porque los protocolos de cada una de ellas proveen formas y métodos para la comunicación.
- Como las computadoras se identificarán unas a otras sobre una red.
- La forma que los datos deben tomar para ser transmitidos.

- Como la información debiera ser procesada una vez que llega a destino.

Los Protocolos también definen los procedimientos para el manejo de transmisiones o "paquetes" dañados o perdidos totalmente.

- IPX (para Novell NetWare).
- TCP/IP (para UNIX, Windows NT, Windows y otras plataformas).
- DECnet (para redes de computadoras DEC de Digital Equipment Corp.).
- AppleTalk (para computadoras Macintosh).
- NetBIOS/NetBEUI (para redes LAN Manager y Windows NT).

Son algunos de los tipos principales de protocolos de redes en uso.

Aunque cada protocolo de red es diferente, todos ellos son capaces de compartir un mismo cableado físico. Este método común de acceso a la red física permite a múltiples protocolos coexistir pacíficamente en el medio de red, y permite al constructor de la red el uso de equipamiento común para una variedad de protocolos. Este concepto es conocido como independencia del protocolo o **Protocol Independence** lo cual significa que los dispositivos son compatibles en las capas o niveles físico, **Physiscal Layer** y de vínculo de datos, **Data Link Layer**; permitiéndole al usuario correr muchos protocolos diferentes sobre el mismo medio. Debido a gran complejidad que conlleva la interconexión se ha tenido que dividir los procesos necesarios para realizar las conexiones en diferentes niveles. Cada nivel se ha creado para dar una solución a un tipo de problema particular dentro de la conexión. Cada nivel tendrá asociado un protocolo, el cual entenderá todas las partes que formen parte de la conexión.

1.4 DEFINICION DE CONMUTACIÓN

Hay dos técnicas de conmutación diferentes: conmutación de circuitos y conmutación de paquetes.

1.4.1 CONMUTACION DE CIRCUITOS

Cuando usted o su computadora hacen una llamada telefónica, el equipo de conmutación del sistema telefónico busca una trayectoria física de "cobre" (lo que incluye la fibra y la radio) que vaya desde su teléfono al del receptor. Esta técnica se llama conmutación de circuitos y se muestra de manera esquemática en la figura 2(a). Los rectángulos representan una oficina de conmutación de la portadora (oficina final, oficina de cargo, etc.). Cuando una llamada pasa por una oficina de conmutación, se establece una conexión física (en forma conceptual) entre la línea por la que llego la llamada y una de las líneas de salida, como indican las líneas punteadas. El modelo que se muestra en la figura 2(a) está altamente simplificado, porque partes de la trayectoria de "cobre" entre los dos teléfonos pueden ser enlaces de microondas en los cuales se multiplexan miles de llamadas. Sin embargo, la idea básica es válida: una vez que se ha establecido una llamada, existe una trayectoria dedicada entre ambos extremos y continuará existiendo hasta que termine la llamada. Una propiedad de la conmutación de circuitos es la necesidad de establecer una trayectoria de un extremo a otro antes de que se pueda enviar cualquier dato. Durante este intervalo de tiempo, el sistema telefónico está buscando una trayectoria de cobre, como se muestra en la Figura 3(a). En muchas aplicaciones de computadora son indeseables los tiempos de establecimiento largos. Al existir una trayectoria de cobre entre las partes en comunicación, una vez completado el establecimiento el único retardo de los datos es el tiempo de propagación de la señal Electromagnética, alrededor de 5mseg por cada 1,000km. Otra ventaja de la trayectoria establecida es que no hay peligro de congestión, aunque podría obtener una antes de establecerse la conexión debido a la falta de capacidad de conmutación o de troncal. Una estrategia de conmutación alterna es la conmutación de mensajes que se muestra en la figura 3(b). Cuando el emisor tiene un marco de datos para enviar, éste se almacena en la primera oficina de conmutación y después se reenvía, un salto a la vez. Cada marco se recibe en su totalidad, se inspecciona en busca de errores, y después se retransmite.

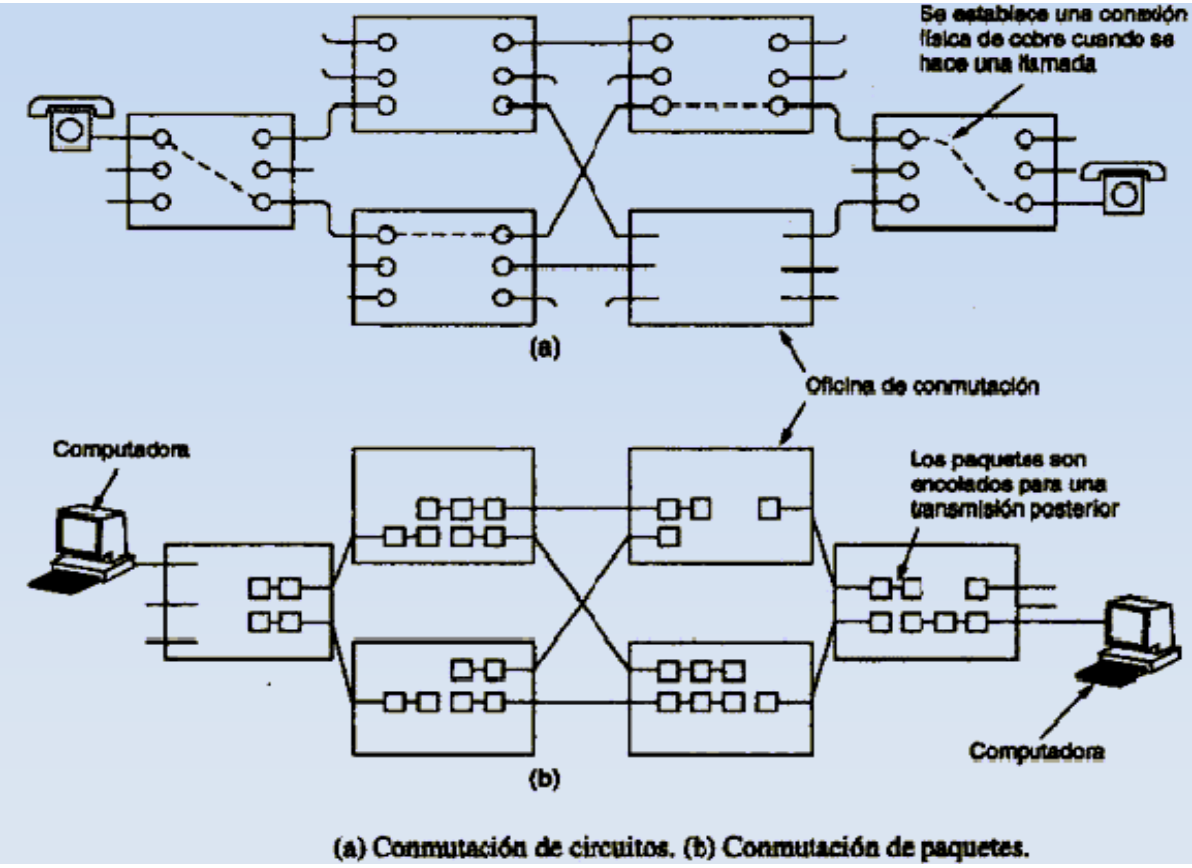
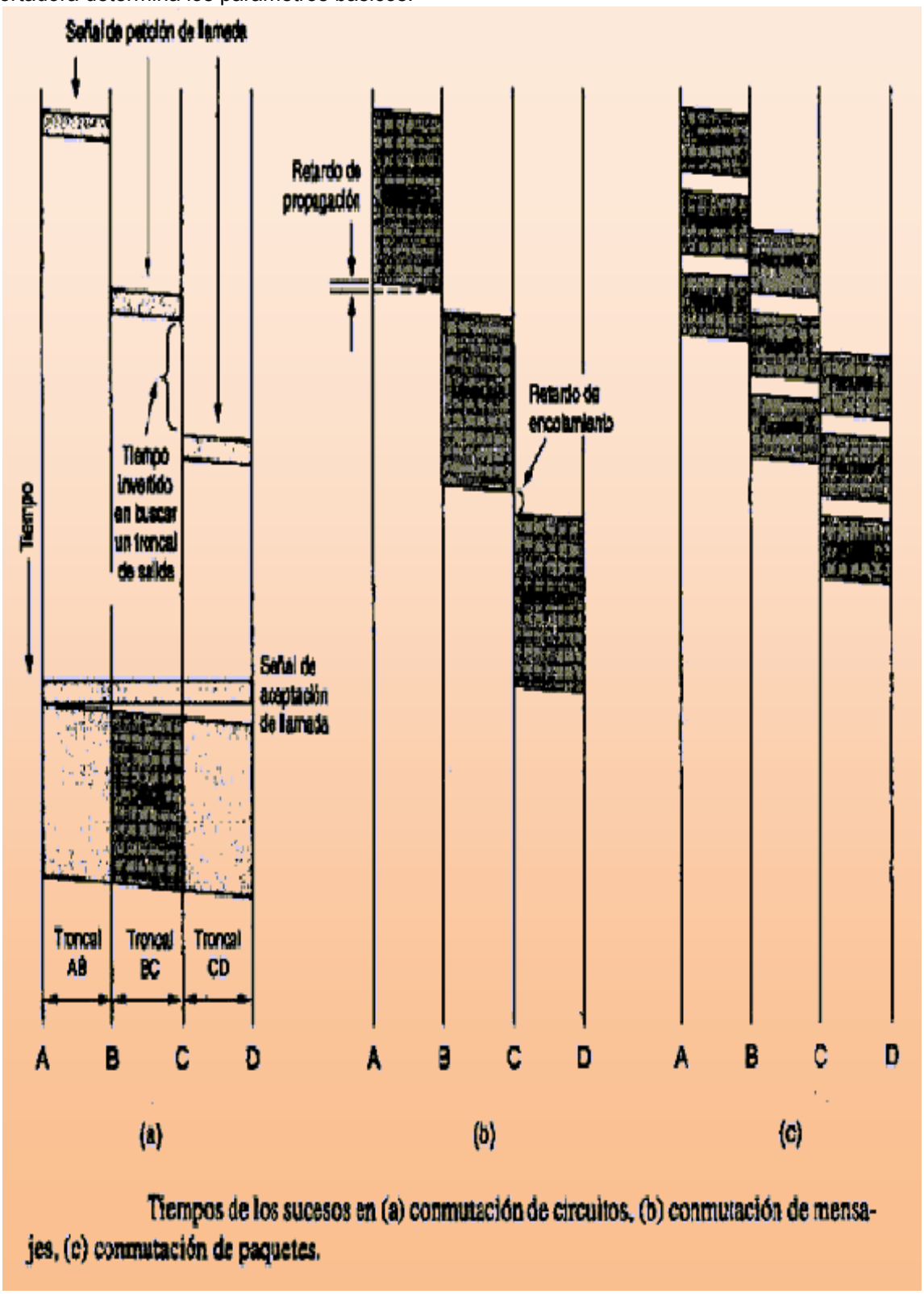


Figura 2 Conmutación de Circuitos

Con la conmutación de mensajes, no hay límite para el tamaño de los marcos, lo que significa que los ruteadores (en un sistema moderno) deben tener discos para almacenar en forma temporal los marcos largos. También significa que un sólo marco puede acaparar una línea de ruteador a ruteador durante minutos, lo que hace inútil la conmutación de mensajes para el tráfico interactivo. Para estos problemas se creó la conmutación de paquetes. Estas establecen un límite superior al tamaño del marco, lo que permite almacenar los paquetes en la memoria principal del ruteador en vez de hacerlo en disco. Al asegurarse de que ningún usuario pueda monopolizar una línea de transmisión durante mucho tiempo (milisegundos), las redes de conmutación de paquetes pueden manejar tráfico interactivo. En la figura 3(b) y 3(c) se muestra una ventaja adicional de la conmutación de paquetes sobre la conmutación de mensajes: el primer paquete de un mensaje de varios paquetes se puede reenviar antes de que el segundo haya llegado por completo, lo que reduce el retardo y mejora el rendimiento. La conmutación de circuitos y la de paquetes difieren en muchos aspectos. La diferencia clave es que la conmutación de circuitos reserva de manera estática por adelantado el ancho de banda requerido, mientras que la conmutación de paquetes lo adquiere y lo libera según se necesita. Con la conmutación de circuitos, cualquier ancho de banda que no se use en un circuito asignado se desperdicia. Con la conmutación de paquetes este ancho de banda se puede utilizar para transmitir otros paquetes de fuentes no relacionadas que van a destinos no relacionados porque los circuitos nunca son dedicados. Por otro lado, debido a que no hay circuitos dedicados, una crecida súbita en el tráfico de entrada puede saturar un ruteador, excediendo su capacidad de almacenamiento y provocando que pierda paquetes. En contraste con la conmutación de circuitos, cuando se usa la conmutación de paquetes resulta sencillo para los ruteadores efectuar conversiones de velocidad y de código. Sin embargo, en algunas redes de conmutación de paquetes éstos se pueden entregar a su destino en el orden equivocado, cosa que nunca puede suceder con la conmutación de circuitos. Otra diferencia es que la conmutación de circuitos es totalmente transparente. El emisor y el receptor pueden usar cualquier velocidad,

formato o método de encuadrado de bits que quieran. Con la conmutación de paquetes la portadora determina los parámetros básicos.



Tiempos de los sucesos en (a) conmutación de circuitos, (b) conmutación de mensajes, (c) conmutación de paquetes.

Figura 3

Esta transparencia es la que hace posible que coexista: voz, datos y fax dentro del sistema telefónico. Las diferencias en el algoritmo de cobro se resumen en la tabla 1.

Elemento	Conmutación de Circuitos	Conmutación de Paquetes
Trayectoria de "cobre" dedicada	Si	No
Ancho de banda disponible	Fijo	Dinámico
Puede desperdiciarse ancho de banda	Si	No
Transmisión de almacenamiento y reenvío	No	Si
Cada paquete sigue la misma ruta	Si	No
Establecimiento de llamada	Requerido	No es necesario
Cuando puede hacer congestión	Durante el establecimiento	En cada paquete
Cargos	Por minuto	Por paquete

Tabla 1

1.5 MEDIOS DE TRANSMISIÓN

Una parte importante en el diseño e instalación de una red es la correcta selección del medio físico apropiado al entorno existente. La adecuada selección del tipo de medio apropiado para cada caso, evitará costos de recableado, según vaya creciendo la red. Medio de transmisión es el sistema (físico o no) por el que viaja la información transmitida (datos, voz, audio) entre dos o más puntos distantes entre sí. Por el medio de transmisión viajan ondas electromagnéticas, que son las que realmente llevan la información. Se pueden distinguir básicamente dos tipos de medios:

- **Medios guiados***:* cuando las ondas están ligadas a algún tipo de medio físico: pares trenzados (UTP, STP, FTP), cables coaxiales, fibras ópticas.
- **Medios no guiados***:* cuando las ondas no están encauzadas (aire, mar, vacío): microondas terrestres, microondas satélite, infrarrojos, radio.
- **Medios Guiados.** A este grupo pertenecen todos aquellos medios en los que se produce un confinamiento de la señal. En estos casos la capacidad de transmisión (velocidad de transmisión Vt, o ancho de banda) depende de dos factores:
    - Distancia.
    - Tipo de enlace:
        - Punto-a-Punto.
        - Difusión.

Principalmente existen estos tipos: *pares trenzados, cable coaxial* y *fibra óptica.*

1.5.1 MEDIOS GUIADOS

1.5.1.1 MEDIOS MAGNETICOS

Una de las formas más comunes de transportar datos de una estación a otra es escribirlos en cinta magnética o disquetes. Una cinta estándar de vídeo de 8mm puede guardar hasta 7,000 gigabytes. Es probable que ninguna otra tecnología de transmisión pueda siquiera acercarse a la cinta magnética en rendimiento. Si vemos ahora el costo, y haciendo un pequeño análisis este representa 10 centavos de dólar por cada gigabyte. Ninguna portadora de red en el mundo puede competir con esto.

Nunca subestime el ancho de banda de una camioneta llena de cintas viajando por la carretera.

1.5.1.2 PAR TRENZADO

El medio de transmisión más viejo y todavía el más común es el par trenzado. Un par trenzado consiste en dos alambres de cobre aislados, por lo regular de 1mm de grueso. Los alambres se trenzan en forma helicoidal como en la figura 4, igual que una molécula de ADN.

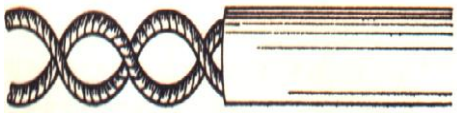


Figura 4

El propósito de torcer los alambres es reducir la interferencia eléctrica de pares similares cercanos (dos alambres paralelos constituyen una antena simple; un par trenzado no). Al trenzar los cables, se incrementa la inmunidad frente a interferencias electromagnéticas (interferencias y diafonía), dado que el acoplamiento entre ambos cables es mayor, de forma que las interferencias afectan a ambos cables de forma más parecida. Al cruzar los pares de hilos se consigue reducir el campo creado alrededor de los mismos, dado que la corriente inducida sobre cada uno de los cables se ve prácticamente cancelada por la corriente que circula por el otro hilo (de retorno) del par. Se pueden tender varios kilómetros de par trenzado sin necesidad de amplificación, pero se necesitan repetidoras para distancias mayores. El ancho de banda depende del grosor del cable y de la distancia, pero en muchos casos se pueden lograr varios Mbps durante algunos kilómetros. Es necesario que los cables tengan una impedancia característica bien definida para asegurar una propagación uniforme de las señales de alta velocidad a lo largo del cable, y para garantizar que la impedancia de los equipos que se conectan a la línea es la adecuada, de modo que pueda transferirse la máxima potencia de ésta. Cuando se conoce la impedancia característica de una línea con cierta precisión se puede diseñar una terminación adecuada que garantice la no reflexión de las señales (lo que da lugar a errores). Generalmente se tienen varios pares trenzados que se encapsulan con una cubierta protectora en un mismo cable, y a los que se denominan cables de pares apantallado figura 5. El aislante tiene dos finalidades: proteger de la humedad al cable y aislar los cables eléctricamente unos de otros. Comúnmente se emplea polietileno, PVC.

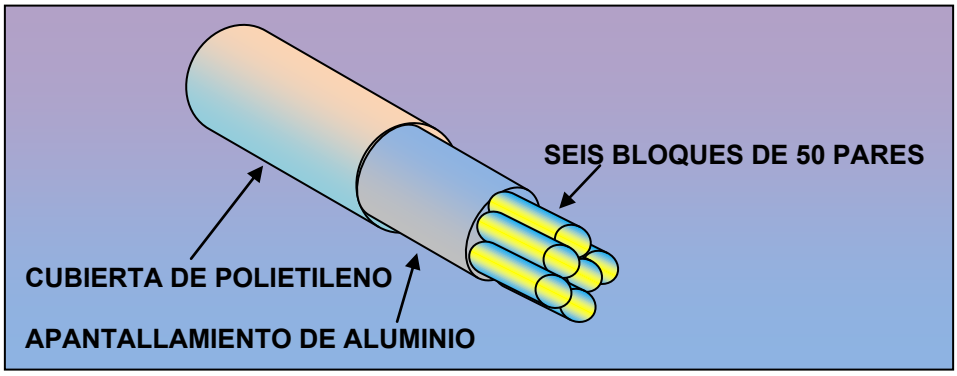


Figura 5

Los hilos empleados son de cobre sólido de 0.2 - 0.4mm de diámetro. El paso de torsión de cada cable puede variar entre una torsión por cada 7cm en los de peor calidad y 2 vueltas por cm en los de mejor calidad. Existen dos tipos de par trenzado:
UTP: Unshielded Twisted Pair (**Par trenzado sin apantallar**). Muy sensible a interferencias, tanto exteriores como procedentes de pares adyacentes. Es muy flexible y se suele utilizar habitualmente en telefonía. Su impedancia característica es de 100ohms. La norma EIA/TIA 568 los divide en varias categorías, destacando:

- **Categorías 1 y 2**: Son cables de telefonía y datos a baja velocidad (hasta 4Mbps).
- **Categoría 3**: Agrupa cables y conectores para transmisión de datos a una velocidad menor de 16Mbps.

- **Categoría 4**: Agrupa los componentes para la transmisión de datos que soportan hasta 16Mbps.
- **Categoría 5**: Es el nivel de máximas prestaciones, soporta velocidades de hasta 100Mbps.
- **Categoría 6**: Se consigue una velocidad de 600Mbps.

STP: Shielded Twisted Pair (**Par trenzado apantallado**).Cada par individual va envuelto por una malla metálica, y a su vez el conjunto del cable se recubre por otra malla, haciendo de jaula de Faraday, lo que provoca que haya mucha menos diafonía, interferencias y atenuación. Se trata de cables más rígidos y caros que el UTP. El STP que estandariza EIA/TIA 568 es un cable de impedancia característica de 50ohms y que actúa a una frecuencia de 300MHz. Los conectores que se usan suelen ser RJ45 metálico y hermafrodita. El apantallamiento permite mejores anchos de banda, Vt mayor, pero son más gruesos y rígidos.

1.5.1.3 CABLE COAXIAL

Otro medio de transmisión común es el cable coaxial. Este cable tiene mejor blindaje que el par trenzado. Las señales eléctricas de alta frecuencia circulan por la superficie exterior de los conductores, por lo que los pares trenzados y los cables de pares resultan ineficientes. El efecto de las corrientes de superficie se traduce en que la atenuación se incrementa con la raíz cuadrada de la frecuencia, así que puede abarcar tramos más largos a velocidades mayores. Son dos las clases de cable coaxial más utilizadas. Una clase, el cable de 50ohms, se usa comúnmente para transmisión digital. La otra clase, el cable de 75ohms, se usa comúnmente para la transmisión analógica; un cable coaxial consiste en un alambre de cobre rígido como núcleo, rodeado por un material aislante. El aislante está forrado con un conductor cilíndrico, que con frecuencia es una malla de tejido fuertemente trenzado. El conductor externo se cubre con una envoltura protectora de plástico. En la figura 6 se muestra una vista en corte por capas de un cable coaxial. La construcción y el blindaje del cable coaxial le confieren una buena combinación de elevado ancho de banda y excelente inmunidad al ruido. El ancho de banda posible depende de la longitud del cable. En cables de 1Km es factible una velocidad de datos de 1 a 2Gbps. Los cables coaxiales se utilizan para transmisión de datos a alta velocidad a distancias de varios kilómetros, es decir, se cubren grandes distancias, con mayores velocidades de transmisión y ancho de banda, así como la conexión de un mayor número de terminales. La respuesta en frecuencia es superior a la del par trenzado. Hasta 400MHz.
Tiene como limitaciones:
- Ruido térmico.
- Intermodulación.

-Necesita amplificadores más frecuentemente que el par trenzado.
-Puede ser rígido o flexible.

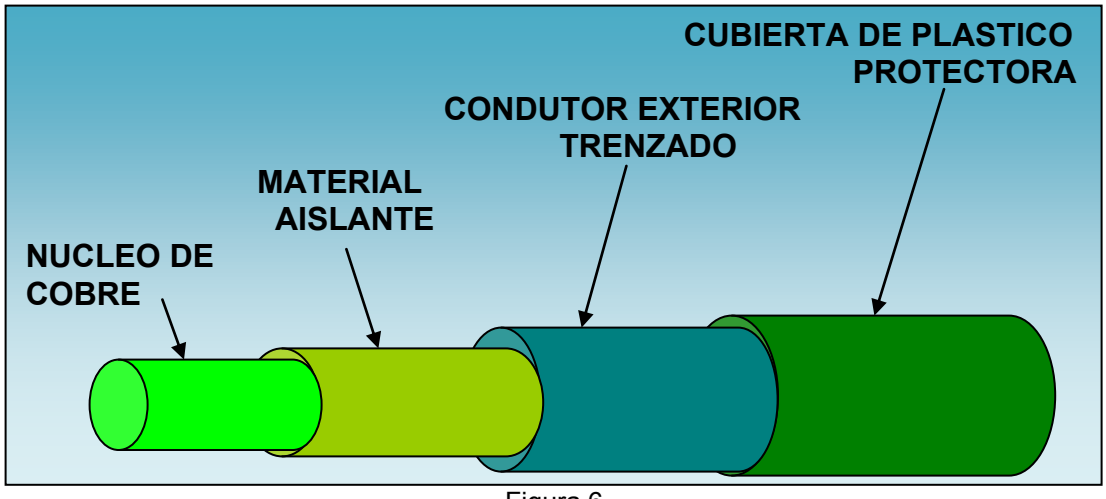


Figura 6

Las interferencias eléctricas no tienen importancia en estos cables si la pantalla exterior carece de discontinuidades. El uso de portadoras de elevada frecuencia inmuniza el sistema frente a las interferencias de baja frecuencia originadas por los dispositivos eléctricos y los tubos fluorescentes. Hay tres tipos principales de cable coaxial:

- **Cables coaxiales estándar de *tipo RG*** utilizados para transmitir señales de televisión doméstica. La mayoría de los cables de tipo RG usan polietileno como aislante interior, aunque el RG-62 emplea aire. Los cables coaxiales de un centímetro de diámetro son más adecuados que los de medio centímetro para velocidades por encima de 30Mbps.
- **Los cables con *núcleos aislados por aire***, que tienen un diámetro pequeño, actúan como retardadores en caso de incendio y tienen una constante dieléctrica pequeña, lo que les proporciona propiedades eléctricas mucho mejores que las de los tipos RG. Presentan una atenuación muy baja, de unos 40dB/100m a 400MHz para los tipos que empleen malla trenzada, y que llega a los 50dB para los de malla continua. Finalmente, son menos costosos que los cables de polietileno o teflón.
- **Cables coaxiales de *polietileno celular irradiado***, que son más caros que los de núcleo aislado por aire, pero cuyas características no presentan las pequeñas variaciones que experimentan estos al ser doblados.

Tipo	Impedancia Nominal(W)	Diámetro máximo de la cubierta(pulgadas)	Capacidad(F/m)	Atenuación nominal(dB/100pies)	Retraso(ns/pie)
RG-174	50.0	0.105	101.0	17.5	1.53
RG-58C	50.0	0.199	101.0	11.0	1.53
RG-58A	52.0	0.200	93.5	11.0	1.53
RG-58	53.5	0.200	93.5	10.0	1.53
RG-58B	53.5	0.200	93.5	10.0	1.53
RG-59B	75.0	0.246	67.6	6.7	1.53
RG-62A	93.0	0.249	44.3	5.2	1.20

Tabla 2

1.5.1.4 FIBRA OPTICA

Es una fibra flexible, extremadamente fina, capaz de conducir energía óptica (luz). Para su construcción se pueden usar diversos tipos de cristal; las de mayor calidad son de silicio, con una disposición de capas concéntricas, donde se pueden distinguir tres partes básicas: *núcleo, cubierta y revestimiento.* El diámetro de la cubierta suele ser de centenas de µm (valor típico: 125µm), el núcleo suele medir entre 2 y 10µm, mientras que el revestimiento es algo mayor: decenas de mm, para darle mayor protección a la fibra se emplean *fibras de kevlar*. La transmisión por fibra óptica se basa en la diferencia de índice de refracción entre el núcleo y la cubierta que tiene un índice de refracción menor. El núcleo transmite la luz y el cambio que experimenta el índice de refracción en la superficie de separación provoca la reflexión total de la luz, de forma que sólo abandona la fibra una mínima parte de la luz transmitida.

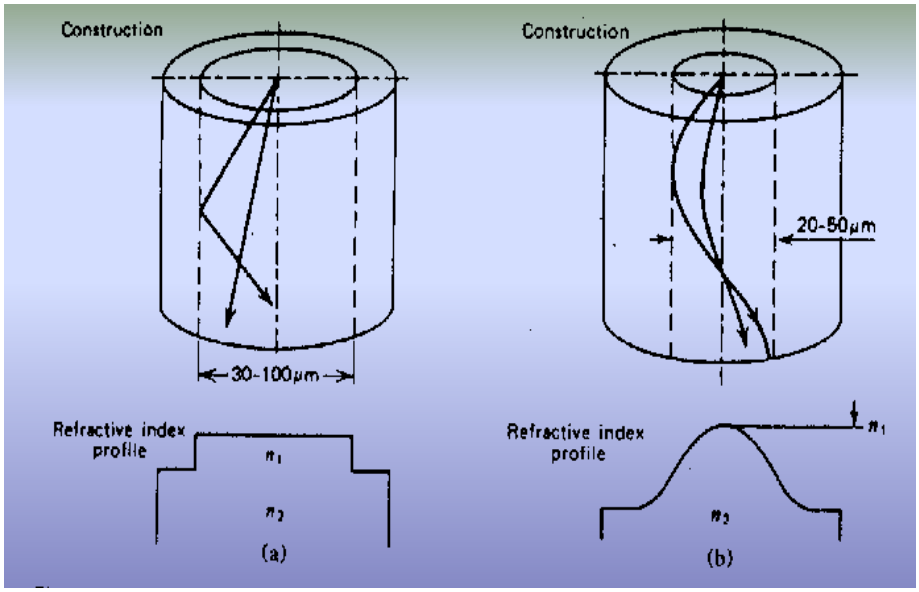


Figura 7

En función de como sea el cambio del valor del índice de refracción las fibras se dividen en:
Fibras ópticas de índice a escala (***stepped-index***): donde el cambio es muy abrupto.
Fibras ópticas de modo gradual (***graded-index*** o ***gradex***): que experimentan un cambio gradual parabólico.

Se emplea en el rango de 10^{14} - 10^{15}μm de longitud de onda (luz visible y parte del infrarrojo), los núcleos de los cables de fibra óptica pueden ser de vidrio o de plástico (polímero). La fibra óptica con núcleo de plástico es más flexible, se puede doblar mejor y los conectores pueden adaptarse mejor sin necesidad de pulir los extremos o de utilizar resinas epóxicas. La fibra óptica de plástico tiene mayor diámetro en el núcleo, lo que hace que los conectores sean menos sensibles a los errores de alineamiento (pérdidas de acoplamiento menores). El cable resulta también menos sensible a las impurezas de fabricación. Un cable con núcleo de plástico no precisa elementos adicionales para alcanzar la rigidez que necesita, como tiras de Kevlar, por lo que es más barato que los de vidrio. La desventaja de los cables con núcleo de plástico es que presentan una atenuación mucho mayor, lo que limita la longitud del enlace. Se distinguen tres tipos de fibras: monomodo, multimodo de índice gradual y multimodo de salto de índice.

- **Fibras multimodo de índice de escala**: el diámetro del núcleo está entre los 50 y 60mm, pero puede llegar a los 200mm. Mientras que el diámetro del recubrimiento suele acercarse al tamaño estándar de los 125mm la dispersión es elevada. Sus aplicaciones se limitan a la transmisión de datos a baja velocidad o cables industriales de control.

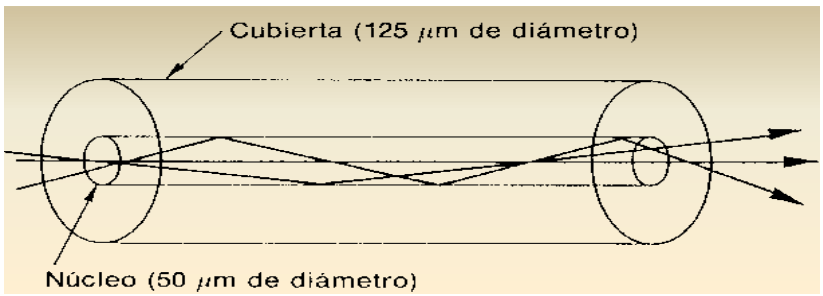


Figura 8

- **Fibras monomodo de índice de escala**: diámetro de entre 1 y 10mm, recubrimiento de 125mm de diámetro. La dispersión es baja y se consiguen anchos de banda de varios GHz/Km.

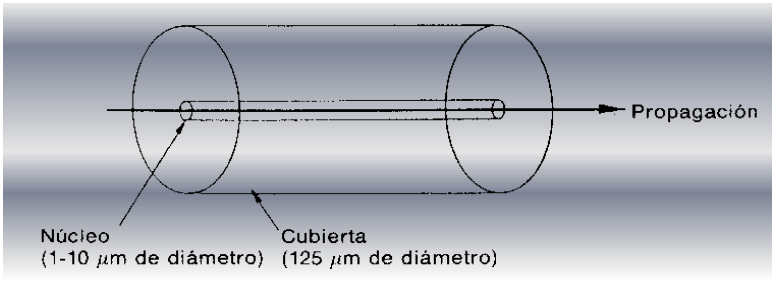


Figura 9

- **Fibras multimodo de índice gradual**: el diámetro del núcleo está entre los 50 y lo 60mm, y el del recubrimiento en 125mm. Aunque existen muchos modos de propagación, la velocidad es mayor que en las fibras multimodo de índice en escala, lo que reduce su dispersión.

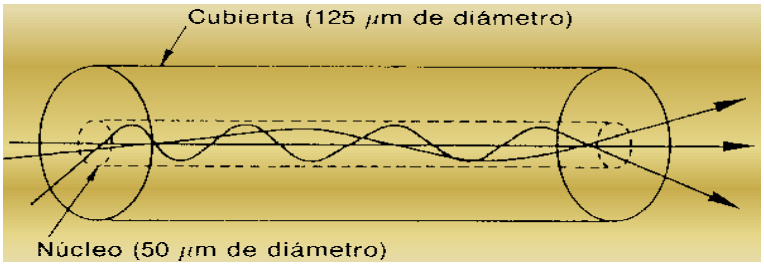


Figura 10

Como transmisores (fuentes de luz) se emplean diodos LED y diodos LASER (éstos últimos para larga distancia y alta velocidad).

1.5.1.4.1 TRANSMISION DE LA LUZ A TRAVES DE LAS FIBRAS

Las fibras ópticas se hacen de vidrio, que a su vez se fabrica con arena, una materia prima de bajo costo disponible en cantidades ilimitadas. El vidrio que se utiliza en las fibras ópticas modernas es muy transparente. La atenuación de la luz dentro del vidrio depende de la longitud de onda de la luz. En la figura 11 se muestra la atenuación para la clase de vidrio que se usa en las fibras, en decibeles por kilómetro lineal de fibra. La atenuaci6n en decibeles está dada por la formula:

$$Atenuación\ en\ decibeles = 10\log_{10}\frac{Potencia\,transmitida}{Potenciarecibida}$$

Por ejemplo, un factor de pérdida de dos da una atenuación de $10 \log_{10} 2 = 3$ dB. La figura 11 muestra la parte cercana al infrarrojo del espectro, que es la que se usa en la práctica. La luz visible tiene longitudes de onda ligeramente más cortas, de 0.4 a 0.7 micras (1 micra = 10^{-6} metros). Para las comunicaciones se utilizan tres bandas de longitud de onda, las cuales se centran respectivamente en 0.85, 1.30 y 1.55 micras. Las últimas dos tienen buenas propiedades de atenuación (una % por kilómetro). La banda de 0.85 micras tiene una atenuación más alta pero la propiedad conveniente de que a esa longitud de onda los láser y los componentes electrónicos se pueden fabricar con el mismo material (arseniuro de galio). Las tres bandas tienen una ancho de entre 25,000 y 30,000GHz. La longitud de los pulsos de luz transmitidos por una fibra aumenta conforme se propagan. Este fenómeno se llama dispersión, y su magnitud depende de la longitud de onda.

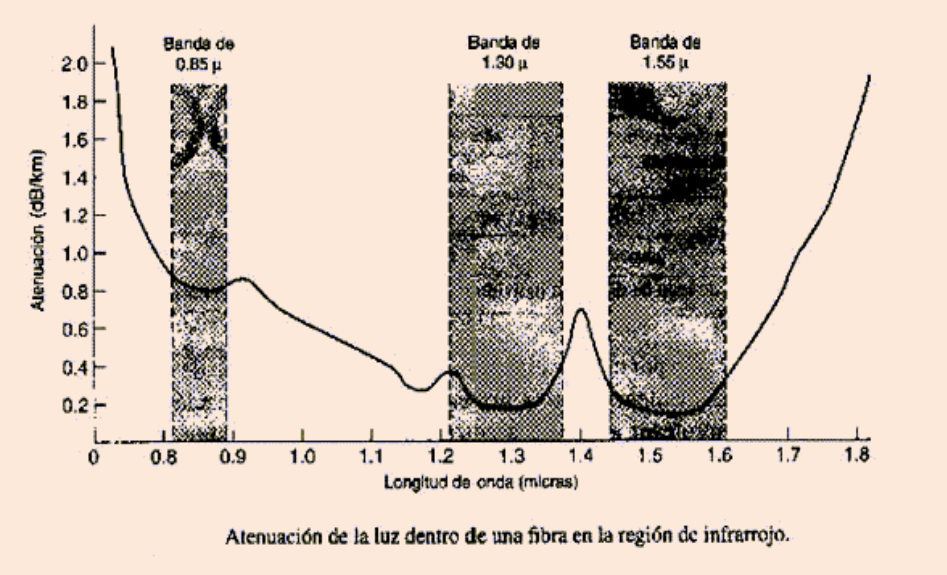


Figura 11

Una forma de evitar que se encimen los pulsos dispersos es incrementar la distancia entre ellos, pero esto solamente se puede hacer reduciendo la velocidad de emisión de las señales. Por fortuna, se ha descubierto que al dar a los pulsos cierta forma especial relacionada con el recíproco del coseno hiperbólico, todos los efectos de la dispersión se cancelan y puede ser posible enviar pulsos a miles de kilómetros sin una distorsión apreciable de la forma. Estos pulsos se llaman solitones.

1.5.1.4.2 CABLES DE FIBRAS

Los cables de fibra óptica son similares a los coaxiales, excepto por el trenzado. La figura12(a) muestra una fibra individual vista de lado. El núcleo de vidrio está al centro, y a través de él se propaga la luz. En las fibras multimodo el diámetro es de 50 micras, aproximadamente el grosor de un cabello humano. En las fibras de modo único el núcleo es de 8 a 10 micras. El núcleo está rodeado por un revestimiento de vidrio con un índice de refracción menor que el del núcleo, a fin de mantener toda la luz en el núcleo. A continuación viene una cubierta plástica delgada para proteger al revestimiento. Las fibras normalmente se agrupan en haces, protegidas por una funda exterior. La figura 12(b) muestra una funda con tres fibras.

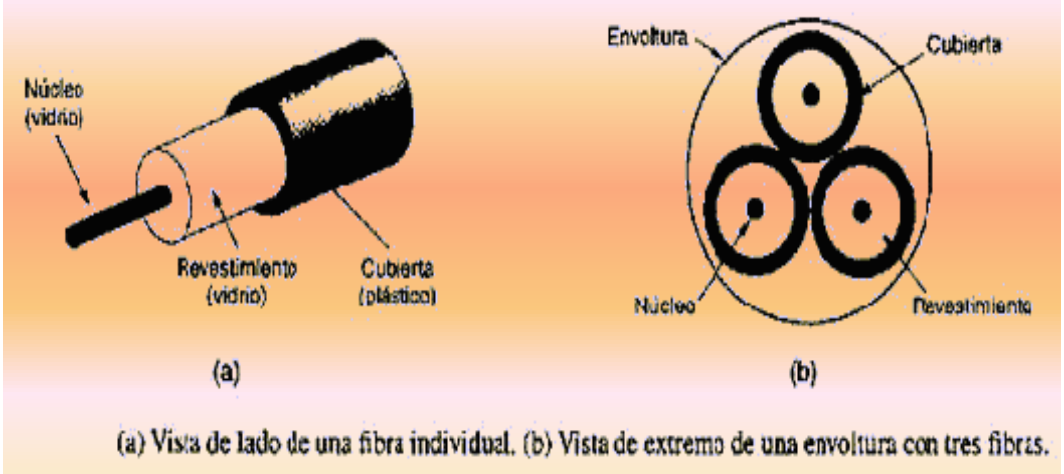


Figura 12

Las fibras se pueden conectar de tres formas diferentes. Primera, pueden terminar en conectores e insertarse en enchufes de fibra. Los conectores pierden casi el 10 o 20% de la luz, pero facilitan la reconfiguración de los sistemas. Segunda, se pueden empalmar de manera mecánica. Los empalmes mecánicos acomodan dos extremos cortados con cuidado uno junto a otro en una manga especial y los sujetan en su lugar, esto resulta en una pérdida de luz del 10 por ciento. Tercera, se pueden fusionar (fundir) dos tramos de fibra para formar una conexión sólida. Un empalme por fusión es casi tan bueno como una fibra de hilado único, pero aún aquí hay un poco de atenuación. Con los tres tipos de empalme pueden ocurrir reflejos en el punto del empalme, y la energía reflejada puede interferir la señal. Se pueden utilizar dos clases de fuente de luz para producir las señales, LED (diodos emisores de luz) y láser semiconductores.

Características	Led	Semiconductor láser
Velocidad de los datos	Baja	Alta
Modo	Multimodo	Multimodo o modo único
Distancia	Corta	Larga
Tiempo de vida	Vida larga	Vida corta
Sensibilidad de la temperatura	Baja	Considerada
Costo	Bajo	Elevado

Tabla 3

El extremo receptor de una fibra óptica consiste en un fotodiodo que emite un pulso eléctrico cuando lo golpea la luz. El tiempo de respuesta normal de los fotodiodos es de 1ns, lo que limita la velocidad de datos a cerca de 1Gbps. El ruido térmico es otro inconveniente, por lo que un pulso de luz debe llevar energía suficiente para ser detectable.

Ventajas frente al cable eléctrico.
Presenta numerosas ventajas muy importantes frente a los tradicionales cables eléctricos:

- ***Mayor velocidad de transmisión***: las señales recorren los cables de fibra óptica a la velocidad de la luz ($c=3x10^9 m/s$), mientras que las señales eléctricas recorren los cables al 50% u 80% de esta velocidad, según el tipo de cable.
- ***Mayor capacidad de transmisión***: pueden lograrse velocidades de varios Gbps a decenas de Km sin necesidad de repetidor. Cuanto mayor sea la longitud de onda, mayor será la distancia y la velocidad de transmisión que podremos tener, y menor la atenuación.
- ***Inmunidad total*** frente a las interferencias electromagnéticas.
- Se consiguen ***tasas de error mucho menores*** que en coaxiales, lo que permite aumentar la velocidad eficaz de transmisión de datos al reducir el número de retransmisiones o cantidad de información redundante necesaria para detectar y corregir los errores de transmisión.
- Tiene un ***menor tamaño y peso***, consideraciones muy importantes.
- Tiene una ***menor atenuación*** que otros medios de transmisión.
- Permite ***mayor distancia*** *entre repetidores*.
- Es un medio muy ***difícil de manipular***.
- Presenta una ***seguridad alta***.
- Apropiados para una ***alta gama de temperaturas***.
- ***Mayor resistencia*** a ambientes y líquidos corrosivos que los cables eléctricos.

Aplicaciones
Destacan las siguientes aplicaciones:

- **Transmisión a larga distancia** En telefonía, una fibra puede contener 60,000 canales.
- **Transmisión metropolitana para enlaces cortos** de entornos de 10km sin necesidad de repetidores, y con capacidad de unas 100,000 conversaciones por cada fibra.
- **Acceso a áreas rurales** Se usan para una longitud de 50 a 150km, con un transporte del orden de 5,000 conversaciones por fibra.
- **Bucles de abonado**

- **Redes de área local (LAN) de alta velocidad.**

Prestaciones

En la figura 13 se pueden ver las prestaciones comparadas de los tres medios de transmisión guiados, siendo el de mejores prestaciones la fibra óptica, y el peor el par trenzado. El par trenzado está representado en verde, el coaxial en azul y la fibra óptica en rojo.

Comparación entre cables.

•***Costo****:* El más caro es la fibra óptica, le sigue el coaxial y luego el par trenzado.
•***Longitud****:* La fibra puede alcanzar los 2km, el par trenzado los 90m y dentro del coaxial el thin alcanza los 185m y el thick los 500m.
•***Velocidad****:* La fibra óptica soporta velocidades que superan los 100Mbps, el coaxial soporta 10Mbps y el par trenzado puede soportar de 10 a 155Mbps, siendo este último el más estándar.
•***Flexibilidad****:* El UTP (par trenzado) es el más flexible, le sigue el coaxial y luego la fibra óptica.
•***Instalación****:* El UTP es el más fácil, el coaxial es relativamente sencillo y la fibra es muy complicada.
•***Resistencia a Interferencias****:* El UTP es el más sensible, el coaxial presenta una buena resistencia y la fibra es inmune a ellas.

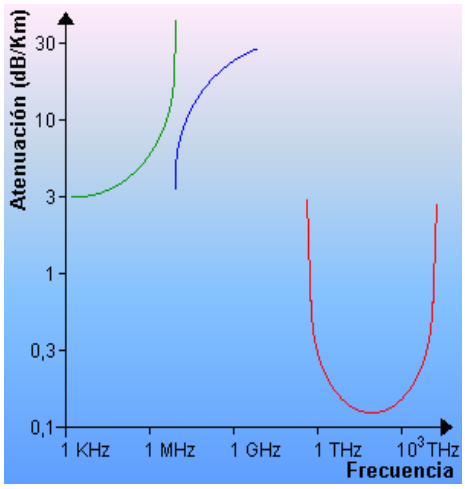


Figura 13

1.5.2 MEDIOS NO GUIADOS

La radiocomunicación puede definirse como Telecomunicación realizada por medio de las ondas eléctricas. La Unión Internacional de Telecomunicaciones (UIT), define las ondas radioeléctricas como las ondas electromagnéticas que se propagan por el espacio sin guía artificial y cuyo límite superior de frecuencia se fija, convencionalmente, en 3,000GHz. La radiocomunicación que hace uso de elementos situados en el espacio, se denomina radiocomunicación espacial. Toda radiocomunicación distinta de la espacial y de la radioastronomía, se llama radiocomunicación terrenal. La técnica de la radiocomunicación consiste en la superposición de la información que se desea transmitir en una onda electromagnética soporte, llamada **portadora**. La inserción de esa información constituye el proceso denominado **modulación**. La onda modulada se envía al medio de propagación a través de un dispositivo de acoplamiento con el medio denominado **antena**. El conjunto de equipos para el tratamiento de la información: moduladores, filtros, antenas, constituye la estación transmisora (o abreviadamente, el transmisor). Cuando la onda transmitida alcanza el punto o puntos de destino, accede al sistema receptor por medio de una antena de recepción, que capta una fracción de la energía. El alcance útil o cobertura de una emisión radioeléctrica depende del tipo e intensidad de las perturbaciones.

1.5.2.1. TRANSMISIÓN INALÁMBRICA

En nuestra era se ha dado origen a la información: gente que necesita estar todo el tiempo en línea. Este tipo de usuario necesita obtener datos para sus laptop, notebook de bolsillo, de mano o de reloj pulsera sin estar conectados a la infraestructura terrestre. Algunas personas creen que en el futuro sólo habrá dos clases de comunicación: de fibra e inalámbrica. Todos los aparatos fijos (esto es, no móviles): computadoras, teléfonos, faxes y demás, se conectarán con fibra; todos los móviles usarán comunicación inalámbrica. Sin embargo, la comunicación inalámbrica también tiene ventajas para los dispositivos fijos en ciertas circunstancias. Por ejemplo, si es difícil tender fibras

hasta un edificio debido al terreno (montañas, selvas, pantanos, etc.), podría ser preferible un sistema inalámbrico. Existen dos tipos fundamentales de transmisión inalámbrica:

Omnidireccionales*:* La antena transmisora emite en todas las direcciones espaciales y la receptora recibe igualmente en toda dirección.

Figura 14

Direccionales*:* La energía emitida se concentra en un haz, para lo cual se requiere que la antena receptora y transmisora estén alineadas. Cuanto mayor sea la frecuencia de transmisión, es más factible confinar la energía en una dirección.

Figura 15

1.5.2.2 EL ESPECTRO ELECTROMAGNÉTICO

Cuando los electrones se mueven crean ondas electromagnéticas que se pueden propagar por el espacio libre (aún en el vacío). El físico británico James Clerk Maxwell predijo estas ondas en 1865 y el físico alemán Heinrich Hertz las produjo y observó por primera vez en 1887. La cantidad de oscilaciones por segundo de una onda electromagnética es su frecuencia, ***f,*** y se mide en Hz (en honor de Heinrich Hertz). La distancia entre dos máximos (o mínimos) consecutivos se llama **longitud de onda** y se designa de forma universal con la letra griega λ (lambda). Al conectarse una antena del tamaño apropiado a un circuito eléctrico, las ondas electromagnéticas se pueden difundir de manera eficiente y captarse por un receptor a cierta distancia. Toda la comunicación inalámbrica se basa en este principio. En la figura 16 se muestra el espectro electromagnético. Las porciones de radio, microondas, infrarrojo y luz visible del espectro pueden servir para transmitir información modulando la amplitud, la frecuencia o la fase de las ondas. La luz ultravioleta, los rayos X y los rayos gamma serían todavía mejores, debido a sus frecuencias más altas, pero son difíciles de producir y de modular, no se propagan bien entre edificios y son peligrosos para los seres vivos. Las bandas que se listan en la parte inferior de la figura 16 son los nombres oficiales de la ITU y se basan en las longitudes de onda, de modo que la banda LF va de 1 a 10Km (aproximadamente 30 a 300KHz).

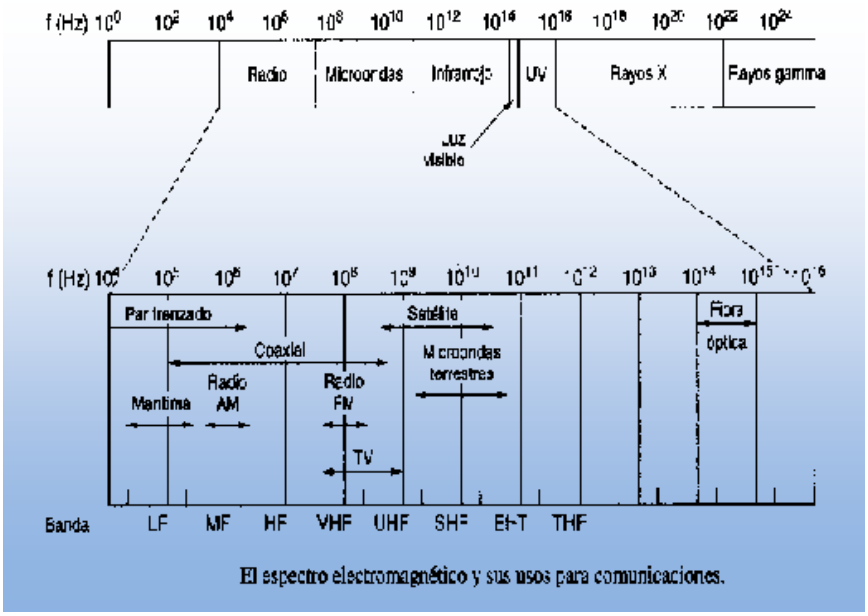


Figura 16

La cantidad de información que puede llevar una onda electromagnética se relaciona con su anchó de banda. Con la tecnología actual, es posible codificar unos cuantos bits por hertz a frecuencias bajas, pero a frecuencias altas el número puede llegar a 40 en ciertas condiciones, de modo que un cable con un ancho de banda de 500MHz puede transportar varios Gbps. La figura 16 debe dejar en claro ahora por que a la gente de redes le gusta tanto la fibra óptica. El espectro electromagnético esta dividido de la siguiente manera:

Símbolo	Nombre	Frecuencia
VLF	Very Low Frecuency	3-30KHz
LF	Low Frecuency	30-300KHz
MF	Mid Frecuency	300-3,000KHz
HF	High Frecuency	3-30MHz
VHF	Very High Frecuency	30-300MHz
UHF	Ultra High Frecuency	300-3,000MHz
SHF	Super High Frecuency	3-30GHz
EHF	Extra High Frecuency	30-300GHz
		300-3,000GHz

Tabla 4

Básicamente se emplean tres tipos de ondas del espectro electromagnético para comunicaciones:
***Microondas**:* 2GHz - 40GHz. Muy direccionales. Pueden ser terrestres o por satélite.
***Ondas de radio**:* 30MHz - 1GHz. Omnidireccionales.
***Infrarrojos**:* $3 \cdot 10^{11}$ - 200THz.

1.5.2.3 ONDAS DE RADIO

Las ondas de radio son fáciles de generar, pueden viajar distancias largas y penetrar edificios sin problemas, de modo que se utilizan mucho en la comunicación, tanto en interiores como en exteriores. Las ondas de radio también son omnidireccionales, lo que significa que viajan en todas direcciones desde la fuente, por lo que el transmisor y el receptor no tienen que alinearse con cuidado físicamente. Las propiedades de las ondas de radio dependen de la frecuencia. A bajas frecuencias, las ondas de radio cruzan bien los obstáculos, pero la potencia se reduce drásticamente con la distancia a la fuente, aproximadamente en proporción $1/r^3$ en el aire. A frecuencias altas, las ondas de radio tienden a viajar en línea recta y a rebotar en los obstáculos. También son absorbidas por la lluvia. En todas las frecuencias, las ondas de radio están sujetas a interferencia por los motores y otros equipos eléctricos. Por la capacidad del radio de viajar distancias largas, la interferencia entre usuarios es un problema. Por esta razón, los gobiernos legislan estrictamente el uso de radiotransmisores. En las bandas VLF, LF y MF, las ondas de radio siguen el terreno, como se ilustra en la figura 17(a). Estas ondas se pueden detectar quizás a 1,000Km en las frecuencias más bajas, y a menos en frecuencias más altas. La difusión de radio AM usa la banda MF. Las ondas de radio en estas bandas cruzan con facilidad los edificios, por ello que los radios portátiles funcionan en interiores. El problema principal al usar estas bandas para comunicación de datos es el ancho de banda relativamente bajo que ofrecen. En las bandas HF y VHF, las ondas a nivel del suelo tienden a ser absorbidas por la Tierra. Sin embargo, las ondas que alcanzan la ionosfera, una capa de partículas cargadas que rodea a la Tierra a una altura de 100 a 500Km, se refractan y se envían de regreso a nuestro planeta, como se muestra en la figura 17(b). En ciertas condiciones atmosféricas, las señales pueden rebotar varias veces. Los operadores de radio aficionados usan estas bandas para conversar a larga distancia. El ejército se comunica también en las bandas HF y VHF. Las perturbaciones que sufren este tipo de

comunicaciones son provocadas por las reflexiones que se producen tanto en la tierra como en el mar, debidas a interferencias multitrayecto. La distancia cubierta por el enlace vendrá dada por:
d = 7.14 · (k·h)½.
h = altura de la antena (m)
k = 1 si no consideramos los efectos de la gravedad. Generalmente se toma k = 3/4.
Para cubrir distancias mayores se usan más radioenlaces concatenados. De igual forma la atenuación:

$$L = 10 \log\left(\frac{4\pi d}{\lambda}\right)^2 \; dB$$

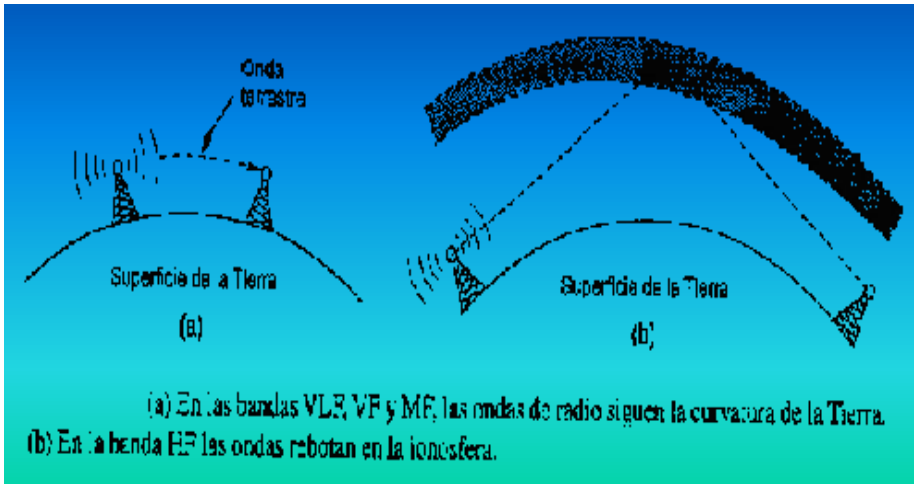


Figura 17

1.5.2.4 TRANSMISION POR MICROONDAS

Por encima de los 100MHz las ondas viajan en línea recta y, por tanto, se pueden enfocar en un haz estrecho. Concentrar toda la energía en un haz pequeño con una antena parabólica (como el tan familiar plato de televisión por satélite) produce una señal mucho más alta en relación con el ruido, pero las antenas transmisora y receptora deben estar muy bien alineadas entre sí. Además, esta direccionalidad permite a transmisores múltiples alineados en una fila comunicarse con receptores múltiples en fila, sin interferencia. Antes de la fibra óptica, estas microondas formaron durante décadas el corazón del sistema de transmisión telefónica de larga distancia. Ya que las microondas viajan en línea recta, si las torres de microondas están muy separadas, partes de la Tierra estorbarán. En consecuencia, se necesitan repetidoras periódicas. Cuanto más altas sean las torres de transmisión, más separadas pueden estar. La distancia entre las repetidoras se eleva en forma muy aproximada con la raíz cuadrada de la altura de las torres. Con torres de 100m de altura, las repetidoras pueden estar espaciadas a 80Km de distancia. A diferencia de las ondas de radio a frecuencias más bajas, las microondas no atraviesan bien los edificios. Además, aún cuando el haz puede estar bien enfocado en el transmisor, hay cierta divergencia en el espacio. La comunicación por microondas se utiliza tanto para la comunicación telefónica de larga distancia, los teléfonos celulares, la distribución de la televisión y otros usos, que el espectro se ha vuelto muy escaso. Esta tecnología tiene varias ventajas significativas respecto a la fibra. La principal es que no necesita derecho de paso; basta comprar un terreno pequeño cada 50Km y construir en él una torre de microondas para saltarse el sistema telefónico y comunicarse en forma directa. Las microondas también son relativamente baratas. Eregir dos torres sencillas y poner antenas en cada uno puede costar menos que enterrar 50Km de fibra a través de un área urbana congestionada o sobre una montaña, y también puede ser más económico que rentar la fibra de la compañía de teléfonos. La zona del espectro de las microondas está dividido de la siguiente manera:

Banda	Frecuencias
L	1 - 2 GHz
S	2 - 4 GHz
C	4 - 8 GHz
X	8 - 12 GHz
Ku	12 - 18 GHz
K	18 - 27 GHz
Ka	27 - 40 GHz

Tabla 5

La distancia que cubre un único radioenlace de microondas viene dada por la expresión:

d = 7.14 · (k·h)½.

h = altura de la antena (m)

k = 1 si no consideramos los efectos de la gravedad. Generalmente se toma k = 3/4.

Figura 18

Para cubrir distancias mayores se usan radioenlaces concatenados.

Las microondas cubren una parte importante del espectro, de los 2 a los 40GHz; el ancho de banda potencial y la velocidad de transmisión aumentan con la frecuencia, por lo que sus prestaciones son muy buenas y tienen múltiples aplicaciones como la transmisión de video y de voz.

Banda (GHz)	Ancho de Banda (MHz)	Régimen de transmisión (Mbps)
2	7	12
6	30	90
11	40	90
18	220	274

Tabla 6

El problema fundamental de este tipo de comunicación es la atenuación, que dependerá de la longitud de onda que estemos utilizando, así como de las condiciones meteorológicas: por ejemplo a partir de los 10MHz aumenta mucho la atenuación a causa de la lluvia. La expresión general de la atenuación con la distancia es:

$$L = 10 \log\left(\frac{4\pi d}{\lambda}\right)^2 \ dB$$

Además se dan problemas de interferencia entre unas y otras emisiones, por lo que es necesario regular las bandas.

4-6 (GHz)	Transmisión a larga distancia
12 GHz	Directos
22 GHz	Televisión por cable

Tabla 7

1.5.2.5 ONDAS INFRARROJAS Y MILIMÉTRICAS

Las ondas infrarrojas y milimétricas no guiadas se usan mucho para la comunicación de corto alcance. Todos los controles remotos de los televisores, grabadoras de video y estéreos utilizan comunicación infrarroja. Estos controles tienen un inconveniente importante: no atraviesan los objetos sólidos. Por otro lado, el hecho de que las ondas infrarrojas no atraviesen bien las paredes sólidas también es una ventaja. Esto significa que un sistema infrarrojo en un cuarto de un edificio no interferirá un sistema similar en cuartos adyacentes. Además, la seguridad de los sistemas infrarrojos contra el espionaje es mejor que la de los sistemas de radio, precisamente por esta razón. Por lo mismo, no es necesario obtener licencia del gobierno para operar un sistema infrarrojo, en contraste con los sistemas de radio, que deben tener licencia. Estas propiedades han hecho del infrarrojo un candidato interesante para las LAN inalámbricas en interiores. De esta manera, las computadoras portátiles capaces de utilizar infrarrojo pueden estar en la LAN local sin tener que conectarse a ella físicamente. Cuando varias personas se presentan a una reunión con sus máquinas portátiles, sólo tienen que sentarse en la sala de conferencias para estar conectados por completo, sin tener que enchufar. La comunicación con infrarrojo no se puede usar en exteriores porque el sol brilla con igual intensidad en el infrarrojo.

1.5.2.6 TRANSMISION POR ONDAS DE LUZ

Una aplicación más moderna es conectar las LAN de dos edificios por medio de láseres montados en sus azoteas. La señalización óptica coherente con láseres es inherentemente unidireccional, de modo que cada edificio necesita su propio láser y su propio fotodetector. Este esquema ofrece un ancho de banda muy alto y un costo muy bajo. También es relativamente fácil de instalar y, a diferencia de las microondas, no requiere una licencia de la CFT. La ventaja del láser, un haz muy estrecho, es aquí también una debilidad. Apuntar un rayo láser de 1mm de anchura a un blanco de 1mm a 500metros de distancia requiere la puntería de una Annie Oakley moderna. Por lo general, se añaden lentes al sistema para desenfocar ligeramente el rayo. Una desventaja es que los rayos láser no pueden penetrar la lluvia ni la niebla densa, pero normalmente funcionan bien en días soleados.

1.5.2.7. SATÉLITES DE COMUNICACIONES

En la década de 1950 y al inicio de la de 1960, se hicieron intentos por establecer sistemas de comunicación rebotando señales en globos meteorológicos metalizados. Desdichadamente, las señales recibidas eran muy débiles para tener un uso práctico. El progreso en el campo de la comunicación celestial tuvo que esperar hasta el lanzamiento del primer satélite de comunicaciones en 1962. La diferencia clave entre un satélite artificial y uno real es que el artificial puede ampliar las señales antes de devolverlas, convirtiendo una curiosidad en un potente sistema de comunicación. El satélite se comporta como una estación repetidora que recoge la señal de algún transmisor en tierra y la retransmite difundiéndola entre una o varias estaciones terrestres receptoras, pudiendo regenerar dicha señal o limitarse a repetirla. Las frecuencias ascendente y descendente son distintas: fasc < fdesc. Para evitar interferencias entre satélites está normalizada una separación entre ellos de un mínimo de 3º (en la banda de la 12-14Ghz) o 4º (4-6GHz).

Ascendente (GHz)	Descendente (GHz)	Ancho de banda (MHz)
4	6	500
12	14	500
19	29	2,500

Tabla 8

El rango de frecuencias óptimo para la transmisión comprende 1-10GHz. Por debajo de 1GHz aparecen problemas debidos al ruido solar, galáctico y atmosférico. Por encima de 10GHz, predominan la absorción atmosférica así como la atenuación debida a la lluvia. Cada satélite opera en una banda de frecuencia determinada conocida como *Transpondedor.* Entre las aplicaciones figuran tanto enlaces punto-punto entre estaciones terrestres distantes como la difusión:

Difusión de TV: el carácter multidestino de los satélites los hace especialmente adecuados para la difusión, en particular de TV, aplicación para la que están siendo ampliamente utilizados.

Telefonía: los satélites proporcionan enlaces punto-a-punto entre centrales telefónicas en las redes públicas de telefonía. Es el medio óptimo para enlaces internacionales con un alto grado de utilización, tecnológica y económicamente es competitivo con otros tipos de enlaces internacionales.

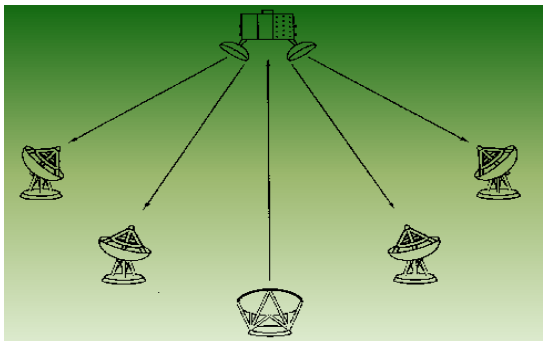


Figura 19

Redes privadas: la capacidad del canal de comunicaciones es dividido en diferentes canales de menor capacidad que se alquilan a empresas privadas que establecen su propia red sin necesidad de poner un satélite en órbita.

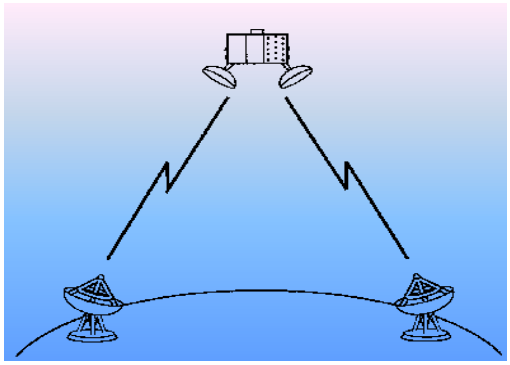


Figura 20

Ejemplo de transmisión por satélite: Sistemas VSAT. Estos sistemas hacen uso de algunos de los canales en que se divide los transpondedores, conectando redes terrestres.

Un problema importante que surge en la transmisión de microondas vía satélite es el retardo debido a las largas distancias que recorren las ondas (aprox. 0.25 segundos) lo que dificulta el control de errores y flujo.

1.5.2.7.1 SATELITES GOESINCRONOS

De acuerdo con la ley de Kepler, el periodo de la órbita de un satélite varía con el radio de la órbita a la potencia 3/2. Cerca de la superficie de la Tierra, el periodo es cercano a los 90 minutos. Los satélites de comunicaciones a altitudes tan bajas son problemáticos porque están a la vista de una estación terrestre determinada sólo durante un intervalo de tiempo corto. Sin embargo, a una altitud aproximada de 36,000km sobre el ecuador, el periodo del satélite es de 24 horas. Con la tecnología actual, no es prudente tener a los satélites espaciados menos de dos grados en el plano ecuatorial de 360 grados, para evitar la interferencia. Con el espaciado de dos grados sólo puede haber 360/2 = 180 satélites geosíncronos de comunicaciones en el cielo al mismo tiempo. Por fortuna, los satélites que utilizan partes diferentes del espectro no compiten, de modo que cada uno de los 180 satélites posibles podría manejar varias corrientes de datos en ambos sentidos simultáneamente. Para evitar el caos total en el cielo, ha habido acuerdos internacionales respecto a quién puede usar cuáles apartados orbitales y frecuencias. En la tabla 9 se listan las principales bandas comerciales. La banda C fue la primera en destinarse al tráfico comercial por satélite; en ella se asignan dos intervalos de frecuencia, el más bajo para tráfico de enlaces descendentes (desde el satélite) y el superior para tráfico de enlaces ascendente (hacia el satélite).

Banda	Frecuencia	Enlaces descendente (GHz)	Enlace ascendente (GHz)	Problemas
C	4/8	3.7-4.2		Interferencia
Ku	11/14	11.7-12.2	14.0-14.5	Lluvia
Ka	20/80	17.7-21.7	27.5-30.5	Lluvia; costo del equipo

Tabla 9 Principales bandas de satélite

La siguiente banda más alta disponible para las portadoras de telecomunicaciones comerciales es la banda Ku. Esta banda no está congestionada, y a estas frecuencias los satélites pueden estar espaciados tan cerca como 1 grado. Sin embargo, existe un problema, la lluvia. El agua es un excelente absorbente de estas microondas cortas. Ya se asignó también ancho de banda en la banda Ka para tráfico comercial por satélite, pero el equipo necesario para aprovecharlo todavía es caro. Además de estas bandas comerciales, existen muchas bandas gubernamentales y militares. Un satélite normal tiene entre 12 y 20 transpondedores, cada uno con un ancho de banda de 36 a 50MHz. Se puede usar un transpondedor de 50Mbps para codificar una sola corriente de datos de 50Mbps, 800 canales digitales de voz a 64kbps, o varias combinaciones distintas. Los primeros satélites tenían un sólo haz espacial que iluminaba la Tierra entera. Con la enorme reducción en precio, tamaño y requerimientos de energía de la microelectrónica se ha hecho posible una estrategia de difusión mucho más compleja. Cada satélite está equipado con múltiples antenas y transpondedores. Cada haz descendente se puede enfocar en un área geográfica pequeña, de modo que pueden tener lugar de manera simultánea múltiples transmisiones ascendentes y descendentes. Un avance nuevo en el mundo de la comunicación por satélite es la invención de microestaciones de bajo costo, llamadas a veces VSAT (very small aperture terminals, terminales de abertura muy pequeña). Estas diminutas terminales tienen antenas de 1 metro y salidas de cerca de 1 watt de potencia. El enlace ascendente por lo general llega a 19.2kbps, pero el descendente es más rápido, con frecuencia de 512kbps. En muchos sistemas VSAT, las microestaciones no tienen suficiente energía para comunicarse en forma directa unas con otras (desde luego, por la vía del satélite).

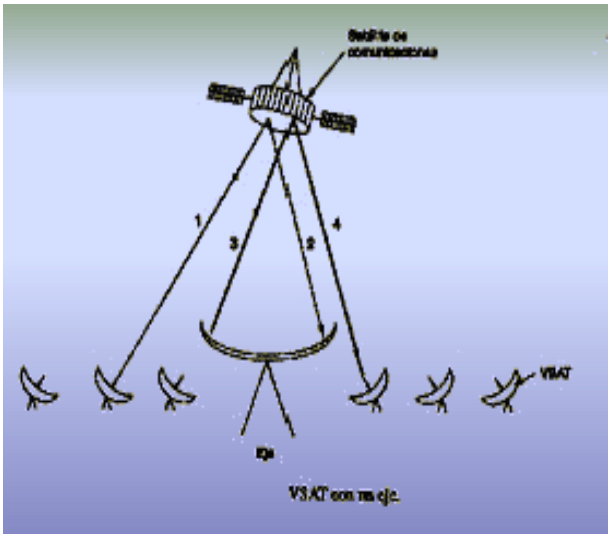


Figura 21

Para ello se necesita una estación terrena especial, el eje, con una antena grande de ganancia alta para retransmitir el tráfico entre VSAT, como se muestra en la figura 21. En este modo de operación, ya sea el emisor o el receptor tiene una antena grande y un amplificador potente. El costo de tener estaciones de usuario final más baratas es un mayor retardo. Los satélites de comunicaciones tienen varias propiedades que son radicalmente diferentes de los enlaces terrestres punto a punto. Dependiendo de la distancia entre el usuario y la estación terrena y de la elevación del satélite sobre el horizonte, el tiempo de tránsito de extremo a extremo es de 250 a 300mseg. Una propiedad importante de los satélites es que por su naturaleza son medios de difusión. No cuesta más mandar un mensaje a miles de estaciones dentro del alcance de un transpondedor que mandarlo a una sola. En algunas aplicaciones, esta propiedad es muy útil. Aún cuando la difusión se puede simular mediante líneas punto a punto, la difusión por satélite puede ser mucho más económica. Por otro lado, desde el punto de vista de la seguridad y confidencialidad, los satélites son un desastre completo: todos pueden oír todo. El cifrado es

esencial cuando se requiere seguridad. Los satélites también tienen la propiedad de que el costo de transmitir un mensaje es independiente de la distancia recorrida. Una llamada al otro lado del océano no cuesta más en cuanto a servicio que una llamada al otro lado de la calle.

1.5.2.7.2 SATELITES DE ORBITA BAJA

En 1990, Motorola abrió nuevo camino al solicitar a la FCC permiso para lanzar 77 satélites de órbita baja para el proyecto Iridio (el iridio es el elemento 77). Más tarde se modificó el plan para usar solamente 66 satélites, de manera que el proyecto debió renombrarse Disprosio (elemento 66), aunque es probable que eso pareciera a muchos el nombre de una enfermedad. La idea era que tan pronto como un satélite se perdiera de vista, otro lo reemplazaría. La meta básica de Iridio es proporcionar servicio mundial de telecomunicaciones usando aparatos manuales que se comunican con los satélites Iridio directamente. El sistema proporciona servicio de voz, datos, avisos, fax y navegación en todos los rincones del planeta. Este servicio compite de frente con PCS/PCN y hace obsoleto al segundo. El sistema utiliza ideas del radio celular, pero con un giro. Normalmente las celdas están fijas mientras que los usuarios son móviles. Aquí, cada satélite tiene una cantidad considerable de haces puntuales que barren la Tierra mientras el satélite se mueve. Así, en este sistema tanto las celdas como los usuarios son móviles, pero las técnicas de relevo que se usan para el radio celular son igualmente aplicables al caso de una celda que abandona a un usuario como lo son al caso de un usuario que sale de una celda. Los satélites se posicionan a una altura de 750km en órbitas polares circulares. Los satélites se dispondrían en collares norte-sur, con un satélite cada 32 grados de latitud. La Tierra entera se cubriría con seis collares de satélites, como lo sugiere la figura 22. La gente que no sepa mucho de química puede visualizar este arreglo como un átomo muy, muy grande de disprosio, con la Tierra como núcleo y los satélites como electrones.

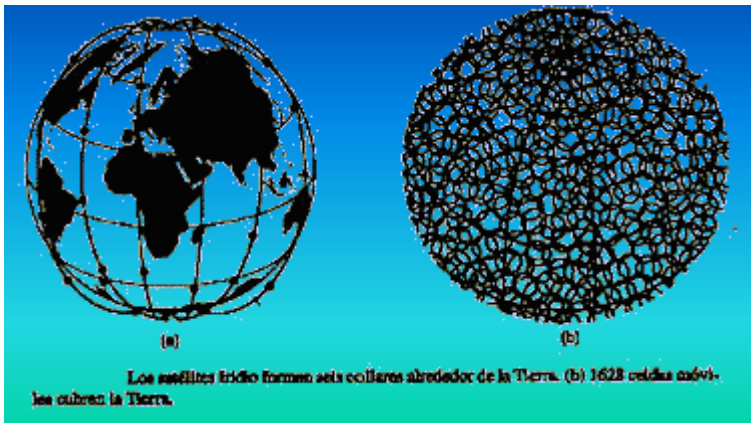


Figura 22

Cada satélite tendrá un máximo de 48 haces de puntuales, con un total de 1,628 celdas sobre la superficie de la Tierra, como se muestra en la figura 23. Las frecuencias se podrían reutilizar cada tres células, como en el radio celular convencional. Cada celda tendría 174 canales dúplex, para un total de 283,272 canales en todo el mundo. Algunos de éstos serían para avisos y navegación, cosa que no requiere mucho ancho de banda. (Los aparatos de avisos que se contemplan exhibirían dos líneas de texto alfanumérico).

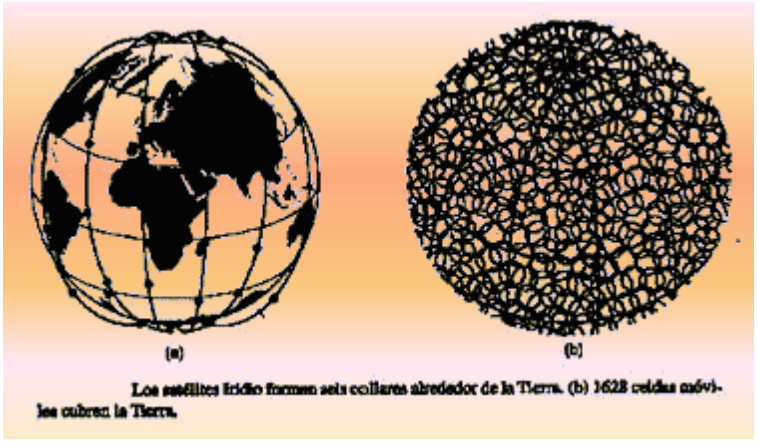


Figura 23

Los enlaces ascendentes y descendentes funcionarían en la banda L, a 1.6 GHz, con lo que harían posible comunicarse con el satélite empleando un pequeño aparato alimentado por pilas. Los mensajes recibidos por un satélite pero destinados a uno remoto serían retransmitidos por satélites en la banda Ka. En el espacio exterior hay suficiente ancho de banda disponible para los enlaces entre satélites. El factor limitante serían los segmentos de los enlaces ascendentes y descendentes. Motorola estima que 200MHz serían suficientes para todo el sistema. El costo proyectado para el usuario final es de casi 3 dólares por minuto. Si esta tecnología puede proporcionar servicio universal en cualquier lugar de la Tierra por ese precio, es improbable que el proyecto muera por falta de clientes. Los viajeros de negocios y otros que quieran mantenerse en contacto todo el tiempo, aún en áreas no desarrolladas, se conectarán en manada. Sin embargo, en las áreas desarrolladas Iridio enfrentará una dura competencia de PCS/PCN con sus telepuntos de "tostador en un poste".

1.6 El MODELO OSI

La Organización Internacional de Estándares (ISO) diseñó el modelo de Interconexión de Sistemas Abiertos (OSI- Open System Interconection) como guía para la elaboración de estándares de dispositivos de computación en redes. Dada la complejidad de los dispositivos de conexión en red y a su integración para que operen adecuadamente, el modelo OSI incluye siete capas diferentes. Estas capas poseen estructura jerárquica. Cada capa se apoya en la anterior, realiza su función, y ofrece un servicio a la capa superior. Este modelo posee la ventaja de poder cambiar una capa sin necesidad de modificar el resto. Las siete capas del modelo OSI son la física, la de enlace de datos, la de red, la de transporte, la de sesión, la de presentación y la de aplicación. Las primeras dos capas (física y enlace de datos) son el hardware que la LAN comprende, como los cables y los adaptadores de red. Las capas 3, 4 y 5 (de red, de transporte, y de sesión) son protocolos de comunicación, como el sistema básico de entrada/salida de red (NetBIOS), TCP/IP y el protocolo medular NetWare (NCP) de Novell. Las capas 6 y 7 (de presentación y aplicación) son el que NOS proporciona servicios y funciones de red al software de aplicación.

Capa 1. Física.- Transmite los datos sobre la red.
Capa 2. Enlace de datos.-Transfiere paquetes al otro extremo de la línea o enlace físico.
Capa 3. Red.- Organiza el trayecto de los mensajes a través de la red.
Capa 4. Transporte.- Vigila la integridad de las informaciones transmitidas de un extremo al otro.
Capa 5. Sesión.- Supervisa y coordina los cambios entre procesos.
Capa 6. Presentación.- Conversión de datos y códigos al formato del destinatario.
Capa 7. Aplicación.- Selección de servicios apropiados a cada aplicación.

Figura 24

1.6.1 CAPA 1 FÍSICA

Se encarga de la transmisión de bits sobre un medio físico. Especifica:

- Voltajes.
- Anchos de impulsos.
- Tipos de conexiones.
- Simples.
- Half duplex.
- Full duplex.
- Forma de conectores.
- Detecta los errores de transmisión

Define las características funcionales para pasar bits de datos hacia el medio de conexión y para recibirlos de él. Incluye las señales:

- RTS (Request To Send-Pedido de Envío).
- CTS (Clear To Send- Listo Para Enviar) en un ambiente RS-232.
- TDM (Time División Multiplexing- Múltiplexion por División de Tiempos) en un entorno ISDN.
- Las características eléctricas y mecánicas definen la interfaz entre el modelo OSI y el medio de conexión para la transmisión.

ANCHO DE BANDA:

- Los canales de comunicación tienen una cierta frecuencia de corte inferior y otra superior.
- Frecuencias por encima de la frecuencia de corte superior o por debajo de la frecuencia de corte inferior, no serán propagadas.
- El ancho de banda de un canal es la diferencia entre ambas frecuencias de corte

1.6.2 CAPA 2 DE ENLACE DE DATOS

Define el protocolo que detecta y corrige errores cometidos al transmitir datos por el cable de la red. La capa de enlace de datos es la causante del flujo de datos de la red, el que se divide en paquetes o tramas (Frames). Cuando un paquete de información es recibido incorrectamente, la capa de enlace de datos hace que se reenvíe. La capa de enlace de datos esta dividida en dos subcapas: El **Control de Acceso al Medio (MAC)** y el **Control de Enlace Lógico (LLC)**. Sus funciones más importantes son la detección de errores y el control de flujo. Ofrece al siguiente nivel una transmisión fiable de bits. En redes de conmutación, además del control de flujo, controla el establecimiento, mantenimiento y liberación de la conexión en cada uno de los enlaces. Por toro lado garantiza un salto sin errores, es decir, asegura que el bit transmitido pasa entre dos nodos, o entre un nodo y una terminal sin problemas. En redes de difusión, también se encarga del control de acceso al medio compartido. Ejemplos de protocolos son: HDLC, LAP-B, LLC, LAP-D, ALOHA, CSMA, CSMA/CD y Paso testigo.

1.6.3 CAPA 3 DE RED

Se encarga de suministrar una conexión de extremo a extremo, es decir, la transmisión de información entre sistemas finales a través de algún tipo de red de comunicación. Libera a las capas superiores de preocuparse por las tecnologías de conmutación utilizadas para conectar los sistemas. Esta capa sólo es necesaria en las redes de conmutación o en redes interconectadas, pues en redes punto a punto o de difusión existe un canal directo entre los dos equipos. En la máquina origen se suministra la dirección del destino. El nivel de red es entonces el que se encarga de encaminar la conexión en cada nodo. Cada nodo requiere un nivel físico y otro de enlace por cada medio de transmisión que le conecta a otro equipo. Sin embargo solamente requiere un nivel de red. En redes de conmutación de circuitos, el nivel de enlace se encarga de mantener y liberar la conexión. Si la red es de conmutación de paquetes por datagramas, entonces el nivel de red toma cada datagrama y decide por que enlace enviar dicho datagrama. Y si la red es de conmutación de paquetes por circuitos virtuales, es el nivel de red el encargado de establecer dicho circuito. En caso de ser necesario el encaminamiento, la función corresponde al nivel de red. Controla la operación de la subred, hace enrutamiento de mensajes y determina el tipo de servicio percibido por los anfitriones de cada red. También realiza la labor de control de congestión, establece la ruta entre las estaciones emisora y receptora, esta capa es la función de conmutación en el sistema telefónico conmutado. Para ir de un punto a otro en la subred, se debe tomar la decisión de que secuencia de nodos intermedios usar, esto lleva a la toma de un algoritmo de enrutamiento.

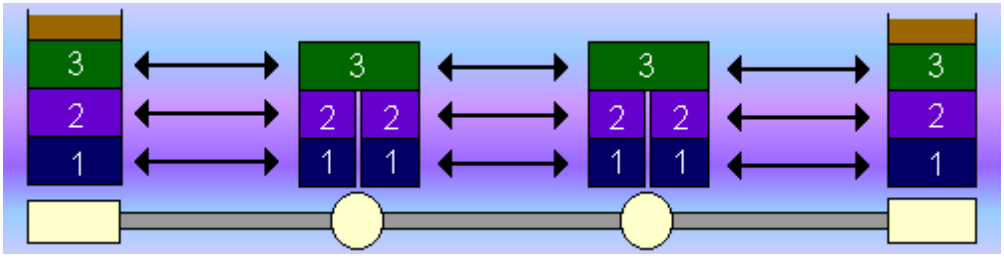


Figura 25

1.6.4 CAPA 4 DE TRANSPORTE

Su función es parecida a la del nivel 2, salvo que garantiza la transmisión sin errores de extremo a extremo, independientemente del tipo de red. Se encarga de que los datos lleguen sin errores, ordenados, sin pérdidas ni duplicados. En una red de conmutación de paquetes por datagramas, es el nivel de transporte el que se encarga de ordenar los distintos paquetes que llegan. En las redes dedicadas y de difusión, no es necesario el nivel de transporte. Este nivel es necesario exclusivamente en redes conmutadas o interconectadas. Requiere más trabajo en una red de conmutación de paquetes por datagramas que en una por circuitos virtuales, debido a la necesidad de ordenar los paquetes. En las redes de conmutación de paquetes, este nivel se encarga de fragmentar el mensaje en el origen, y de recomponerlo en el destino. Es la ultima capa de responsabilidad para el transporte de datos; utilizando técnicas de multiplexado para mejorar el costo o la eficiencia de los servicios de la subred. Es la responsable de la validez e integridad de la transmisión y es la encargada de responder adecuadamente si el enlace falla o se dificulta su establecimiento.

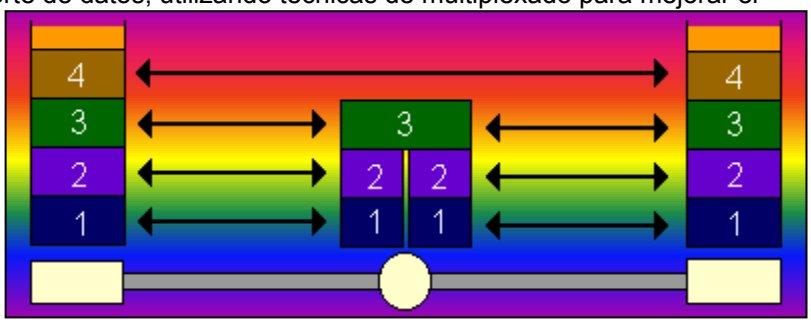


Figura 26

1.6.5 CAPA 5 DE SESION

Se encarga de organizar y sincronizar el diálogo entre los dos extremos. Ofrece mecanismos para gestionar el diálogo entre dos extremos por medio de:

- ***disciplinas de diálogo***, es decir, quien debe emitir en cada instante.
- ***agrupamiento*** de datos en unidades lógicas.
- ***recuperación***, es decir, si se produce algún problema en la comunicación, disponer de algún punto de comprobación a partir del cual poder retransmitir los datos. Maneja las sesiones entre procesos en los anfitriones. Esta capa proporciona la coordinación de las comunicaciones en una forma ordenada. Controla las conexiones de red entre nodos. La capa de sesión es responsable de la creación, mantenimiento y terminación de las sesiones de red.

1.6.6 CAPA 6 DE PRESENTACIÓN

Este nivel elimina los problemas que puedan surgir al comunicar distintas arquitecturas, pues cada arquitectura estructura los datos de una forma específica, que no tienen por que ser compatibles. En el nivel de transporte se traducen los datos a un formato común, que se define en este mismo nivel. En esta capa se definen el formato de los datos que se van a intercambiar entre las aplicaciones y ofrece a los programas de aplicación un conjunto de servicios de transformación de datos. En caso de ser necesario, también se encarga de la compresión y del cifrado, además

negocia y administra la forma en que se representan y codifican los datos. Provee un común denominador para la transferencia de datos de diferentes sistemas (File Transfer)

1.6.7 CAPA 7 DE APLICACIÓN

Este último nivel se encarga de las aplicaciones más frecuentes, como http, transferencia de ficheros (ftp), acceso terminal a estaciones remotas (telnet), etcétera. También define ciertas funciones que pueden ser usadas por varias aplicaciones. En general, la aplicación en sí (el programa, por ejemplo), hace uso de este nivel. Esta capa define la interfaz con los verdaderos programas de aplicación de los usuarios de la red. Define las reglas para entrar en el sistema de comunicaciones. Los programas se comunican unos con otros a través de esta capa, permitiendo la realización de transacciones.

1.6.8 LA TORRE OSI Y LOS SERVICIOS

En el modelo OSI, la comunicación es de par a par, entre iguales. Esto quiere decir que las aplicaciones se comunican entre sí, a través del nivel 7. El nivel 7 a su vez se comunica con su homólogo del otro extremo a través del nivel 6, etcétera. Se diferencia entonces entre el flujo ficticio de datos; reflejado con líneas discontinuas en la figura 27 del nivel real de datos trazo grueso). En la figura está representado el flujo de datos en una red de conmutación.

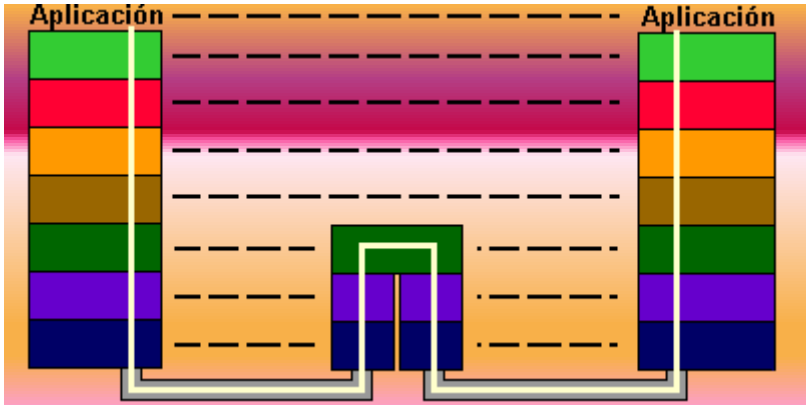


Figura 27

Por otro lado, cada nivel de OSI añade una cabecera a los datos a transmitir, a excepción del nivel 1 que no añade nada, y del nivel 2 que además añade una cola. Dicha cabecera son datos de control para el nivel correspondiente del extremo de la comunicación. Esto se puede apreciar mejor en la figura 28.

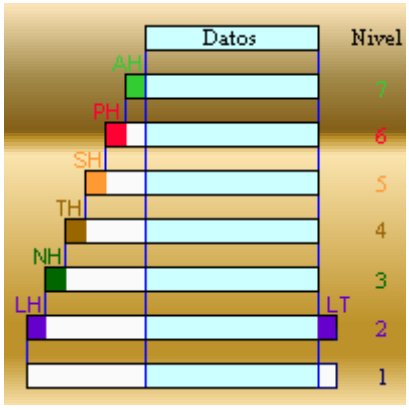


Figura 28

II.-EVOLUCION DE LAS REDES

2.1.1. INTRODUCCION

La frecuencia más elevada de la voz humana no suele exceder los 6,000 hertz, y aunque la inteligibilidad depende fundamentalmente de las frecuencias altas, se ha comprobado experimentalmente que eliminando las frecuencias superiores a 3,400Hz la inteligibilidad de la voz es del 90%, lo cual no supone gran pérdida frente al ahorro que representa en los sistemas de transmisión para el transporte de la señal en la red telefónica. Por otra parte, las frecuencias bajas facilitan la calidad a las palabras y permiten un mejor reconocimiento de la voz de la persona; no obstante, el prescindir de frecuencias inferiores a los 300Hz no implica problema alguno para la identificación de la voz. La gama de frecuencias comprendida entre los 300-3,400Hz, **frecuencia vocal,** es suficiente para entender-comprender con notable calidad de la voz del interlocutor a través de un enlace telefónico. Una vez conocida la gama de frecuencias de la voz humana considerada convenientemente para ser transmitida por la red telefónica, estudiaremos los principales procesos que sufre la señal entre los puntos de emisión y recepción. En un enlace telefónico, la señal sonora se transforma en movimientos mecánicos y estos en corrientes eléctricas, con el fin de favorecer la transmisión a través del medio portador; en recepción, el proceso se contempla de un modo inverso con vistas a recuperar fielmente la señal inicial. Para analizar el proceso de conversión de señales sonoras en eléctricas y viceversa. La telefonía suele restringirse a consideraciones sobre la forma en que los abonados son interconectados, y a un análisis del tráfico que generan. El rápido crecimiento del tráfico de datos generado por oficinas, bancos, computadoras, líneas aéreas, etc., y la introducción de los sistemas telefónicos digitales, ha suscitado la cuestión de que dichos datos puedan enviarse por la red telefónica, y por lo tanto, de proporcionar un servicio integrado.

2.1.2. ESTUDIO DEL TELEFONO

El teléfono es un aparato constituido fundamentalmente por un micrófono, un receptor y otros dispositivos complementarios para emisión y recepción de llamadas, con el fin de establecer comunicaciones habladas entre dos interlocutores situados en lugares distantes. Desde el primitivo teléfono ideado por Bell hasta los existentes en la actualidad, tanto la estética como las prestaciones han avanzado de forma considerable: teléfonos murales, de sobremesa, portátiles, fabricados en madera, plástico de diversos colores, formas clásicas modernas y sumamente caprichosas, con disco, teclado o incluso con marcación utilizando la voz propia de usuario, posibilidad de memorizar números para una posterior llamada telefónica, rellamada, conferencia múltiple, y un largo etcétera que culmina con una posibilidad de incorporar un pantalla que permite a los interlocutores observarse con imágenes vivas en tiempo real. La localización del teléfono desde donde puede establecerse una comunicación, ofrece en la actualidad una amplia gama de posibilidades. Aparte de su ubicación convencional en puntos fijos, bien en el hogar y en las oficinas para uso privado, o como teléfono público en la calle o en cualquier otro tipo de establecimiento, destaca su utilización como equipo móvil tanto en trenes, aviones o automóviles. Actualmente, el servicio telefónico posibilita la transmisión de otros tipos de información distinta a una conversación telefónica, al facilitar el acceso a redes de transmisión de datos u otro tipo de redes de telecomunicación especializada. Sobre los elementos que integran un teléfono, es preciso recordar le existencia de micrófonos de cristal, carbón, condensador, electrodinámicos y electret. En un micrófono electrodinámico, la cápsula se encuentra acoplada a una bobina situada en un campo magnético, de modo que al hablar, las variaciones de la cápsula o diafragma provocan una variación del campo, y se genera una tensión eléctrica de la misma frecuencia con la que se mueve el diafragma por efecto de la voz. Un micrófono electret utiliza una sustancia plástica similar al teflón denominada electret, que esta cargada eléctricamente de una manera permanente. Se basa en la técnica del micrófono de condensador, pero con la particularidad de que el campo eléctrico que se precisa es producido por el electret, y no como el de condensador, en el que lo proporciona una corriente externa. Un micrófono de este tipo tiene un diámetro de un centímetro y ofrece un rendimiento altamente satisfactorio. Un elemento así mismo fundamental en el teléfono

es el dispositivo de marcación automática, disco o teclado. El **disco** produce una interrupción de la corriente eléctrica que envía la central a la que esta conectado el teléfono, tantas veces como indica cada cifra correspondiente al número discado. En cuanto al teclado se utilizan dos clases técnicamente diferentes. El teclado decimal trabaja eléctricamente igual que el disco, ya que al accionar cualquiera de los diez pulsadores numerados del 0 al 9, se interrumpe la corriente de línea tantas veces como indica el número del pulsador seleccionado, a excepción del 0 que corresponde con diez interrupciones.

El teclado multifrecuencia consta de doce teclas correspondientes a los diez números del disco o del teclado decimal y de los signos * y #, estos dos últimos necesarios para servicios telemáticos o de aplicaciones avanzadas de voz. Este tipo de teclado dispone para su envío a línea de siete diferentes frecuencias, prefijadas por el CCITT, de modo que se transmiten a la central por un par distinto de frecuencias en función del digito pulsado. Los teléfonos que incorporan estos teclados deben conectarse a centrales capaces de interpretar una señalización de estas características. Desde la perspectiva del funcionamiento del teléfono en cuanto al modo de efectuar la llamada y consecuentemente de su evolución histórica, es preciso reseñar las tres siguientes clases de equipos telefónicos:

- **Teléfono de Batería Local**.-Caracterizado por precisar pilas para la alimentación del micrófono, incorpora un magneto para hacer sonar el timbre del teléfono distante. Actualmente el magneto se sustituye por un circuito transistorizado.
- **Teléfono de Batería Central**.-Equipo previo a la telefonía automática; la alimentación local se sustituye por otra enviada desde la central procedente de baterías de acumuladores.
- **Teléfono Automático**.-Donde un disco o teclado sustituye a los dispositivos de llamada del teléfono de baterías central.

Hoy en día se siguen instalando estos tres tipos de teléfono, dándose la circunstancia de poder contar con teléfonos de batería local más modernos que algunos modelos automáticos. Todo teléfono individual conectado a una central a través de una línea telefónica se le conoce como **teléfono principal**, siendo posible conectar hasta cuatro teléfonos **supletorios** en derivación de dicha línea. Otra modalidad del teléfono es el asociado a una **centralita**, es decir, a un equipo de conmutación que facilite a modo de red privada la conexión entre los teléfonos a ella conectados, o entre estos y los de la red pública telefónica. Una gran mayoría de los equipos telefónicos existentes en la actualidad puede conectarse a este tipo de equipos centralizados. El concepto de centralita no supone exclusivamente en la interconexión de un reducido número de teléfonos, ya que el mercado ofrece amplias posibilidades de elección, no sólo en cuanto a su capacidad sino a sus prestaciones; en este sentido cabe citar las de tecnologías digitales que precisan teléfonos así mismo digitales.

2.1.2.1 FUNCIONAMIENTO DEL TELEFONO

El funcionamiento de un teléfono analógico, tomando como ejemplo uno de disco por ser uno de los más comunes y para su más fácil comprensión, y su modo de conexión con la central local, se muestra en las figuras 29 y 30. En la figura 29 aparece el teléfono conectado a la central local en posición de reposo (**on hook**), por medio de los hilos **a** y **b**, razón por las que se les suele denominar **a/b**.

Figura 29

El circuito de voz (auricular y micrófono) se encuentra desconectado de la línea y el timbre dispuesto para recibir la señal de llamada de la central; en el momento en el que el usuario oye sonar el timbre y descuelga el microteléfono, el conmutador de gravedad desconecta el timbre y pone el circuito de voz en la línea, quedando dispuesto para establecer la comunicación.

Si lo que el abonado desea es establecer una comunicación procede a levantar (**off hook**) el microteléfono, con lo que el timbre se desconecta por la acción del conmutador de gravedad, y el circuito de voz se pone en línea circulando la corriente directa generada por la batería de la central, pero con la particularidad de que en este caso el disco actuará produciendo una señal al ser manipulado por el usuario como en la figura 30.

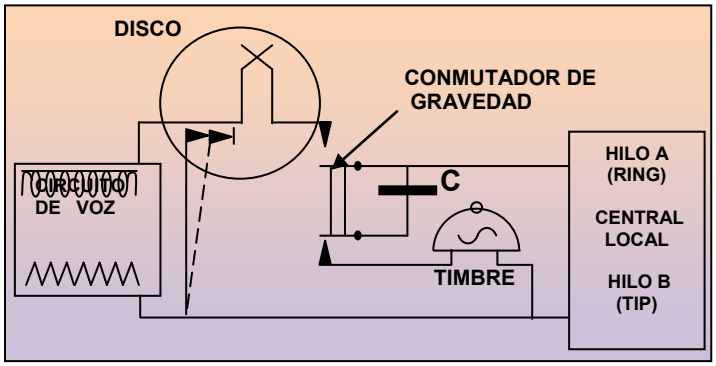


Figura 30

En el momento en el que se produce el giro del disco, el circuito de voz se puentea quedando desactivado, y el retorno de este, a una cadencia regulada produce aperturas del circuito a un ritmo de 10 por segundo, que son detectadas por la central en forma de pulsos (el número de pulsos indica el dígito marcado). Cuando se deja de manipular el disco, el abonado queda en disposición de establecer la comunicación, siempre y cuando se logre establecer el enlace con el teléfono de su interlocutor, lo que apreciará por el tono de llamada. Al finalizar, cuelga y el teléfono queda en disposición de recibir o realizar una nueva llamada.

2.1.2.2 CONVERSION DE LA VOZ EN CORRIENTE

Los primeros aparatos estaban equipados con una batería que se conectaba a través del micrófono a la línea (sistema de batería local) y la corriente se modulaba en función del cambio de la resistencia que este experimentaba con el sonido; estos necesitaban de un magneto para generar la corriente de llamada. Hoy se aplica el mismo principio, pero la batería esta en la central (sistema de batería central) y los micrófonos de gránulos de carbón se reemplazan por otros electromagnéticos; la corriente directa que circula por la línea se utiliza para señalización.

2.1.2.3 CONVERSION DE LA CORRIENTE EN VOZ

La señal eléctrica, modulada por la voz, recibida en el teléfono, es transformada en sonido por medio del auricular, que suele ser electromagnético, y transforma estas variaciones en sonido, ya que al variar la corriente varía el campo magnético y la membrana del auricular oscila reproduciendo fielmente el sonido original.

2.1.2.4 ESTUDIO DEL MICROTELÉFONO

El microteléfono se compone del micrófono y del audífono en una empuñadura para su fácil manejo, con una distancia de 17cm aproximadamente entre el oído y la boca figura 31.

2.1.2.4.1 CARACTERISTICAS DEL MICROTELÉFONO

1) La resistencia del microteléfono es de 200Ω, para una alimentación de $-48V_{CD}$ a través de 2*400Ω. En donde 1,200 Ω equivale a 4.3Km.
2) El microteléfono debe ser capaz de operar con una corriente mínima de 20mA, a un voltaje mínimo de $-40V_{CD}$.
3) La equivalente de recepción es de: -5.5dB+1.5dB dB+ Ganancia
   -5.5dB-2.0dB dB- Atenuación
4) La equivalencia de transmisión.
5) La precisión acústica precisada al microteléfono a una potencia menor de 100dB, sin que exista distorsión es de 20μpa (pascales).

6) La velocidad de los impulsos es de $10 \pm impulsos/seg$.
7) La etapa de recepción debe resistir 5,000 horas de trabajo continuo.
8) El microteléfono debe operar efectivamente a alturas entre los 3,000 metros sobre el nivel del mar.
9) El microteléfono debe soportar temperaturas entre los –40°C-66°C a una humedad relativa de 5%-95%.
10) En la etapa de conversación del microteléfono, debe tener una resistencia con ruido máxima de 15dB.
11) La impedancia del microteléfono esta entre los 600Ω a 900Ω, con una alimentación de 2*400Ω.

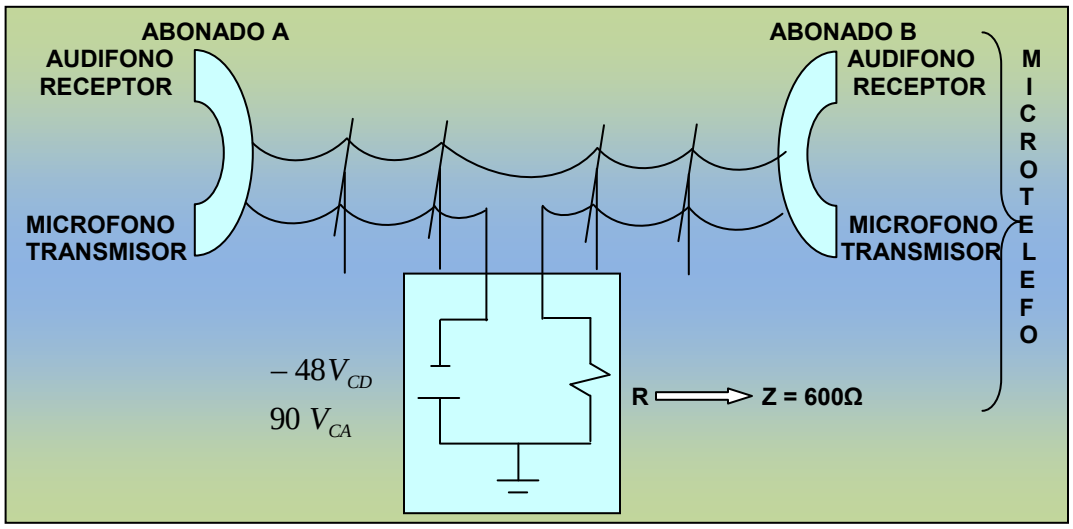


Figura 31

Para los impulsos, debe cumplir con las siguientes características:

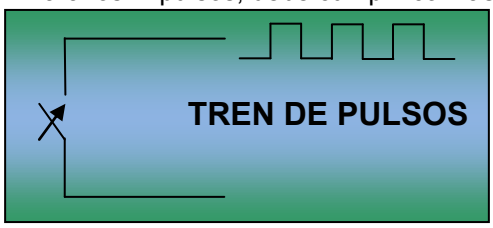


Figura 32

En la etapa de generación del tren de pulsos, por ejemplo si se marca el número 1 se genera un tren de pulsos, para el dígito 2 se genera un tren de 2 impulsos; así hasta que se marca el dígito 0 que generará un tren de 10 impulsos. En la etapa de abrir/cerrar debe cumplir con el $67 \pm 3\%$ de abrir y el $33 \pm 3\%$ de cerrar, con un tiempo total de respuesta menor a 6mseg. Lo que implica:

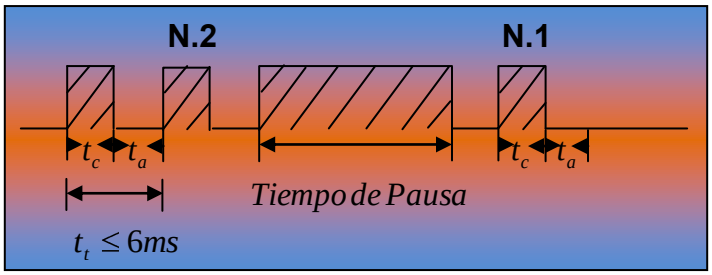


Figura 33

Entre cada tren de impulsos y otro debe de haber un tiempo de pausa de aproximadamente 300mseg para que el conmutador de la central telefónica, reconozca el dígito marcado, debe al

menos generarse el 90% de la amplitud de la señal en un tiempo no mayor a 5mseg. Para la etapa de multifrecuencias, se realiza mediante dos grupos de frecuencias: uno denominado grupo de frecuencias inferiores y otro denominado grupo de frecuencias superiores. Entre cada grupo de frecuencias, que se transmite simultáneamente no debe ser mayor de 40mseg.

2.1.2.4.2 DIAGRAMA DEL MICROTELÉFONO

2.1.2.4.3 ESTUDIO DEL MICRÓFONO

El micrófono es un trasconductor que convierte las ondas sonoras en señales de impulsos eléctricos (corriente). El micrófono, se diseñará de acuerdo a la frecuencia a transmitir. Para un canal telefónico la resistencia del micrófono es de 40Ω, las reactancias de las bobinas de alimentación es de 2*400Ω, el voltaje de alimentación es de 4.5 volts. Su funcionamiento se basa en las variaciones de resistencia que experimentan ciertas sustancias cuando sufren modificaciones de presión. Dicho micrófono esta constituido por una cápsula de carbón seco de gran pureza y cubierta por una membrana. El sonido hace vibrar la membrana, esta comprime al mismo ritmo los gránulos de carbón y en consecuencia la resistencia varía provocando variaciones proporcionales en la corriente de alimentación del micrófono, viajando la señal a través del medio portador hasta el extremo distante, figura 34.

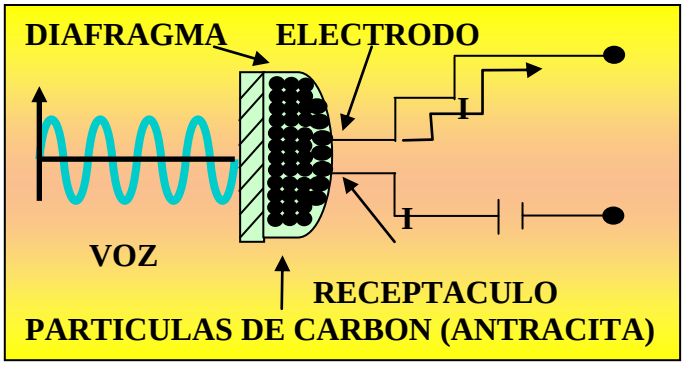


Figura 34

La corriente llega al receptor telefónico, formado por un imán con dos bobinas arrolladas en sus extremos; las variaciones de la señal recibida promueven así mismo una variación del campo magnético, creando una membrana adosada al dispositivo idénticas vibraciones a las emitidas desde el micrófono. Si tenemos dos partículas de carbón a las cuales se les aplica presión con la voz figura 35

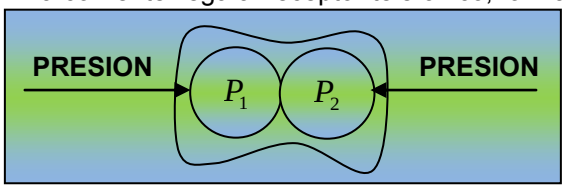


Figura 35

Sabemos que la resistencia:

$$R = \delta \frac{l}{A}$$

$donde:$

$R \rightarrow \text{Re}\, sistencia\ normal\ de\ las\ particulas.$

$\delta \rightarrow \text{Re}\, sistividad\ del\ material.$

$l \rightarrow Longitud.$

$A \rightarrow Area.$

A mayor presión de la voz, aumentará el área de las partículas, dando lugar a una disminución de la resistencia y viceversa. Si el área menor por dejar de ejercer presión por la voz, la resistencia del micrófono aumentará. En otras palabras, un micrófono tiene un comportamiento como el de una resistencia variable como en la figura 36 de una señal:

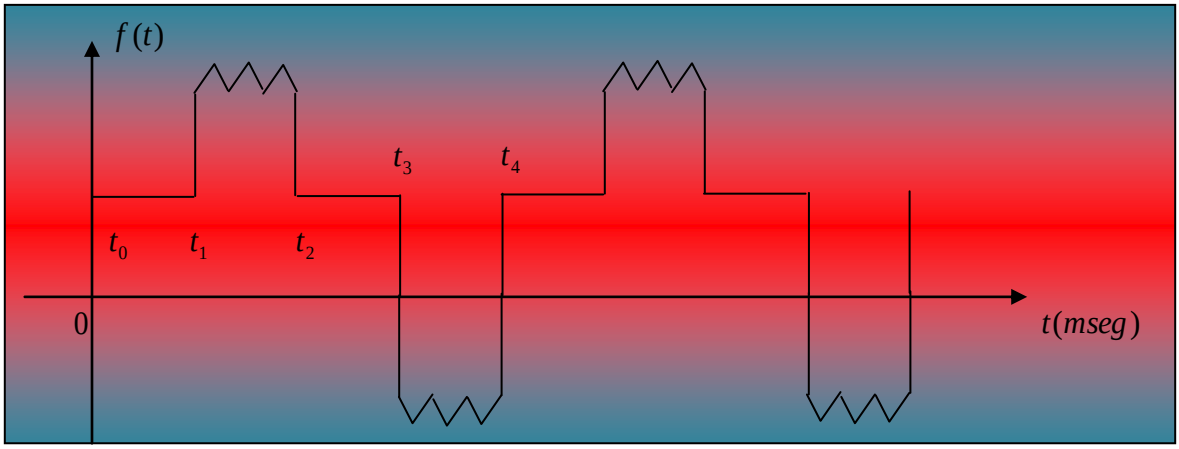


Figura 36

En $t_0 - t_1$: El diafragma esta en reposo, por que no se aplica la presión a través de la voz.

En $t_1 - t_2$: Al diafragma se le aplica la señal de voz disminuyendo la resistencia (aumento del carbón) y ha aumentado la corriente.

En $t_3 - t_3$: El diafragma pasa a su estado de reposo.

En $t_3 - t_4$: El diafragma sufre una descomposición (descompresión), o sea, pasa a su máximo de resistencia, por lo tanto la corriente disminuye a cero posteriormente pasa a su nivel máximo negativo. Con todo lo anterior, mediante la voz aplicada al micrófono se genera una señal analógica pulsante de corriente figura 37

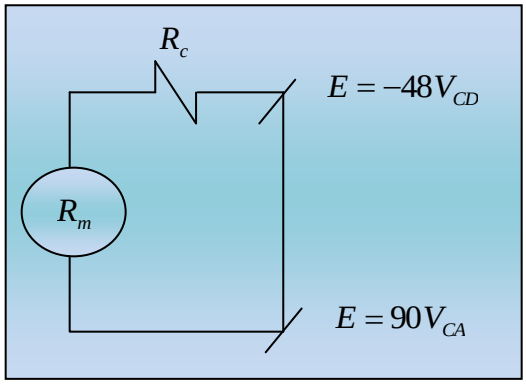


Figura 37

Al micrófono se le puede estudiar analíticamente como muestra la figura 38

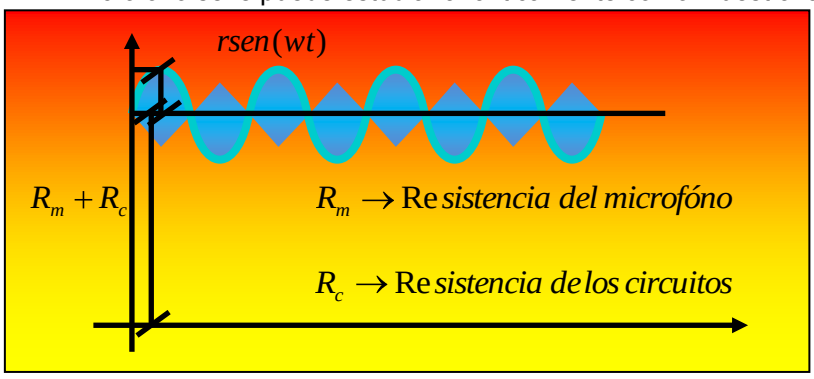


Figura 38

Por ley de ohm:

$$I = \frac{E}{R} = \frac{\frac{E - RI}{E}}{R_m + R_c - rsen(wt)}$$

$$I = \frac{E}{\left(R_m + R_c - rsen(wt)\right)\left(\frac{R_m + R_c}{R_m + R_c}\right)}$$

$$I = \frac{E}{\left(\frac{R_m + R_c}{R_m + R_c} - \frac{rsen(wt)}{R_m + R_c}\right)\left(R_m + R_c\right)}$$

$$I = \frac{E}{\left(1 - \frac{rsen(wt)}{R_M + R_c}\right)\left(R_m + R_c\right)}$$

$$I = \left(\frac{E}{R_m + R_c}\right)\left(\frac{1}{1 - \frac{rsen(wt)}{R_m + R_c}}\right)$$

$$I = \frac{E}{R_m + R_c}\left[1 + \frac{rsen(wt)}{R_m + R_c} + \left(\frac{rsenw(wt)}{R_m + R_c}\right)^2 + \cdots + \left(\frac{rsen(wt)}{R_m + R_c}\right)^{n-1}\right]$$

$$I = \frac{E}{R_m + R_c} + \frac{Ersen(wt)}{\left(R_m + R_c\right)^2} + \frac{Er^2 sen(wt)}{\left(R_m + R_c\right)^3} + \cdots$$

De la anterior ecuación sólo se toman los términos de primer orden, puesto que los términos de segundo orden, causan distorsión, porque:

$$sen^2(wt) = \frac{1}{2} - \frac{1}{2}\cos(2wt)$$

y si $w = 2\pi f$ y $f = 3100\,Hz$, entonces se sale del ancho de banda permitida la señal y no se permite ni tolera la distorsión:

$$\Rightarrow I = \frac{E}{R_m + R_c} + \frac{Ersen(wt)}{\left(R_m + R_c\right)^2}\,Amperes$$

La corriente $\left(\quad\right)$ que se modula mediante la voz, tiene componente constante (en reposo):

$$I = \frac{E}{R_m + R_C}(A)$$

y la componente variable operando el micrófono es:

$$I = \frac{Ersen(wt)}{\left(R_m + R_c\right)^2}$$

y si el sen 90°=1

$$\Rightarrow I = \frac{E}{\left(R_m + R_c\right)^2}(A)$$

2.1.2.4.4 ESTUDIO DEL AUDIFONO

El audífono es un trasconductor que convierte, las ondas de impulsos eléctricos en señales de ondas sonoras, su configuración se muestra en la figura 39.

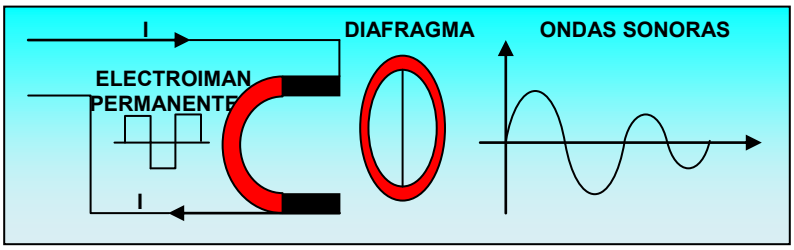


Figura 39

Resistencia del audífono: 100Ω.
Los capacitores de alimentación: 2μfd/100 V.

2.1.2.4.4.1 ANALISIS DE LA INDUCTANCIA

Recordamos que:

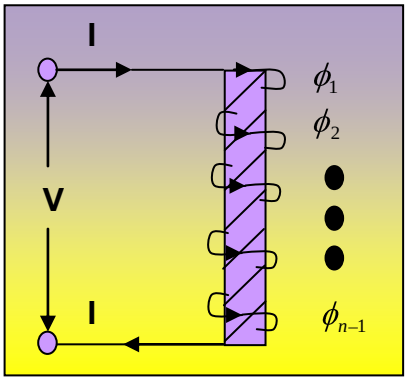


Figura 40

$\phi_T = N\varphi_{n-1}(weber) \rightarrow (1)$

$\varphi_t = flujo\,magnético\,total.$

$N = número\,de\,espiras.$

$\varphi_{n-1} = Flujo\,magnético\,en\,cada\,espira\,(weber).$

De la ley de Faraday:

$$V(t) = \frac{d\phi}{dt} \rightarrow (2)$$

Sustituyendo la ecuación (1) en la ecuación (2):

$$V(t) = \frac{dN\phi_{n-1}}{dt}$$

$$V(t) = N\frac{d\phi_{n-1}}{dt}$$

$$V(t) = N\frac{d\phi}{dt}$$

Se necesita de la corriente para generar flujo magnético:

$\phi : f(i)$

$$V(t) = N\frac{d\phi}{dt}\left(\frac{di}{di}\right)$$

Acomodando términos:

$$V(t) = N\frac{d\phi}{di}\left(\frac{di}{dt}\right)$$

donde $N\frac{d\phi}{di}$ es la inductancia (L)

$$V(t) = L\frac{di}{dt} \rightarrow (3)$$

Obtención del voltaje en la bobina (V).
De la ecuación (3) tenemos:

$$Ldi = V(t)dt$$

$$di = \frac{1}{L}V(t)dt$$

Integramos:

$$\int di = \int \frac{1}{L}V(t)dt$$

$$i(t) = \frac{1}{L}\int V(t)dt(A) \rightarrow (4)$$

2.1.2.4.4.2 FUERZA DE ATRACCIÓN

Se dice que un imán permanente, al cual se le arrolla un alambre, para que el paso de la corriente (I) genera flujo magnético (ϕ), para atraer y repelar al diafragma esta en función de la siguiente ecuación:

$$F_A = f(If_0) \rightarrow (5)$$

donde: $F_A =$ Fuerza de atracción.
$f =$ Función.
$I =$ Corriente (mA).
$f_{0=}$ Frecuencia (Hz).

Para obtener la fuerza de atracción en el audífono:

$$F_A = K\phi_T{}^2 \rightarrow (6)$$

donde: $\phi_T =$ flujo magnético total.
$\phi_0 =$ flujo permanente del electroimán.
$\phi_i = Isen(wt) =$ flujo magnético variante debido a la corriente modulada por la voz.

La ecuación (6) será:

$$F_A = K(\phi_0 + \phi_i)^2$$

$$F_A = K\phi_0{}^2 + 2K\phi_0\phi_i + K\phi_i{}^2$$

$$F_A = K\phi_0{}^2 + 2K\phi_0(sen(wt)) + k(Isen(wt))^2$$

$$F_A = K\phi_0{}^2 + 2K\phi_0 Isen(wt) + kI^2 sen^2(wt)$$

pero: $sen^2(wt) = \frac{1}{2} - \frac{1}{2}\cos(wt)$

$$F_A = K\phi_0{}^2 + 2K\phi_0 Isen(wt) + kI^2\left[\frac{1}{2} - \frac{1}{2}\cos(wt)\right]$$

$$F_A = \underbrace{K\phi_0{}^2}_{F_1} + \underbrace{2K\phi_0 Isen(wt)}_{F_2} + \underbrace{\frac{1}{2}KI^2}_{F_3} - \underbrace{\frac{1}{2}KI^2\cos(wt)}_{F_4}$$

En general tenemos:

$F_A = F_1 + F_2 + F_3 - F_4$

donde: F_1 : Nos dice que el diafragma será atraído o repulsado directamente por el flujo magnético en el electroimán.

F_2 : Es la parte más importante de la fuerza de atracción, pues ahí esta contenida la señal de la información (Isen (wt)).

F_3 : Indica que la amplitud de señal al cuadrado, es directamente proporcional a la constante de acoplamiento (0.6 y 0.7).

F_4 : Es la componente que se desecho por introducir **distorsión** en la señal original, pues se observa que cambia la señal original de un seno a un coseno, además de variar al doble la frecuencia angular (Zw).

2.1.3 PLAN DE NUMERACIÓN

En un sistema telefónico, el plan de numeración es un conjunto de normas a cumplir por las empresas y los abonados, con el fin de regular la práctica de acceso a comunicaciones telefónicas nacionales e internacionales. Es la parte fundamental de una central telefónica. Con el plan de numeración, se pretende que el usuario, se conecte a la red, para solicitar una llamada, que puede ser local, larga distancia nacional y/o internacional. Disponiendo cada nación del suyo propio, producto de este ordenamiento, se le asigna un número a cada abonado al servicio telefónico, diferenciado del resto de las terminales conectadas a la red. El número que identifica cada terminal telefónica ofrece información sobre el país donde esta situado, la zona geográfica y la ciudad; abonados de dos ciudades distintas pueden tener el mismo número telefónico, pero el hecho de incluir prefijos cuando llama uno al otro, los identifica perfectamente. A cada teléfono se le asigna un número que posibilita la tarificación y proporciona a los equipos de conmutación el adecuado encaminamiento para efectuar la conexión. La identificación de las primeras cifras de una llamada advierte si es internacional, nacional, provincial o local, y permite así a la central elegir el enlace correspondiente. Aunque los planes de numeración tienden a ofrecer números con la menor cantidad de cifras, no siempre resulta posible por la elevada densidad telefónica y la diversidad de nuevos servicios que lógicamente precisan un número particularizado (fax, ISDN, telefonía móvil, etc.). Se conoce como **número internacional** al conjunto de cifras asignadas a un equipo; esta formado por el indicativo del país al que pertenece, el indicativo interurbano de su zona de numeración y el número local del abonado. El CCITT recomendaba una longitud máxima de 12 cifras para el número internacional. La primera cifra del indicativo nacional es el código de zona; el mundo esta divido en nueve zonas, y cada país pertenece a una zona en la tabla 10 se muestra la relación existente entre el número de zona y el área geográfica. En todas las zonas, salvo en dos de ellas, deben añadirse una o dos cifras al número de zona para conseguir el indicativo nacional.

1 NORTEAMERICA	6 AUSTRALIA
2 AFRICA	7 EX-URSS
3 EUROPA	8 ASIA ORIENTAL
4 EUROPA	9 EXTREMO ORIENTE Y ORIENTE MEDIO
5 SUDAMERICA	0 DESOCUPADO

Tabla 10

Las dos excepciones son las zonas 1 (Norteamérica y Caribe) y la 7 (exURSS). Para cada una de estas zonas existe un plan de numeración asociado, lo que significa, por ejemplo, que ningún abonado del Canadá tiene un mismo número nacional que ningún abonado de estados Unidos. En consecuencia, para conectar con cualquier abonado de la zona 1, la cifra 1 va seguida únicamente del número nacional. La situación para la exURSS es similar. La situación de Europa es totalmente distinta: existen muchos países con grandes redes nacionales, cuyos números nacionales tiene nueve cifras. Para estos países se necesita un indicativo nacional de dos cifras, y eso sólo puede conseguirse asignando a Europa dos números de sobra. La división del mundo en las zonas mostradas en la tabla 10 se ha diseñado con el fin de que satisfaga las necesidades mundiales pues, evidentemente, conforme algunos grandes países vayan desarrollando sus redes telefónicas, será necesario hacer algunos ajustes. De acuerdo al CCITT, para dar servicio al menos se requiere que la central contenga el código de numeración para 1,000 abonados. Esos 1,000 abonados, su plan de numeración es de tres dígitos o sea 000-999.

Si la demanda telefónica, va en ascenso de acuerdo con el CCITT, se debe satisfacer al aumentar unidades de 1,000 abonados c/u. Hasta un máximo de 10 unidades o sea con capacidad para 10,000 abonados. Para 10,000 abonados se agrega un dígito más:

$$\begin{matrix} xxxx \\ 0000 \\ \underbrace{9999}_{10{,}000\,abonados} \end{matrix}$$

$$\begin{matrix} x\,xxxx \\ 0\,0000 \\ 9\,9999 \\ \underbrace{100000}_{100{,}000\,abonados} \end{matrix}$$

Si la demanda del servicio telefónico se encuentra entre una central telefónica y un máximo de 10 centrales telefónicas, se usará como plan de numeración 5 dígitos o sea servicio para 100,000 abonados.

Si el servicio telefónico, esta comprendido entre 10 y 100 centrales $\underbrace{\underbrace{xx}_{100}\,\underbrace{xxx}_{10{,}00}}_{1{,}000{,}000}$ telefónicas, se requerirá de un plan de numeración de 6 dígitos, para dar servicio a 1, 000,000 de abonados.

$\underbrace{\underbrace{xxx}_{1{,}000}\,\underbrace{xxxx}_{10{,}000}}_{10{,}000{,}000}$ La demanda del servicio telefónico no debe exceder de 1,000 centrales telefónicas para un área específica. En caso de tener la necesidad de incrementar el servicio, las áreas se deben conjuntar en regiones telefónicas de acuerdo al área geográfica. Pues el CCITT indica que para llamadas nacionales, el plan de numeración no debe exceder de 9 a 10 dígitos. Usando 8 dígitos, se tiene capacidad de servicio para 10,000 000 de abonados. Para el octavo dígito nos indica el área de las 1,000 centrales telefónicas

$$\underbrace{x}_{area}\ \underbrace{xxx}_{centrales}\ \underbrace{xxxx}_{número\,del\,abonado}$$

por ejemplo:

$$\underbrace{\underbrace{5}_{area}\ \underbrace{733}_{número\,de\,la\,central}\ \underbrace{4552}_{número\,del\,abonado}}_{Llamada\,Local}$$

2.1.4 LA RED TELEFÓNICA

En los últimos años la red telefónica se ha desarrollado vertiginosamente, por lo que en la actualidad es posible establecer comunicaciones entre abonados separados por miles de kilómetros. Las llamadas de larga distancia pasan por diversas etapas de conmutación a través de varios enlaces de transmisión posible, antes de alcanzar su destino; para que estas comunicaciones sean posibles, los diseñadores de sistemas deben integrar diferentes facetas de las telecomunicaciones y deben llegar a compromisos razonables. Aunque la estructura de las redes telefónicas se ha desarrollado de forma poca sistemática, siguiendo el ritmo del incremento de la demanda. El paso de una llamada a través de una red nacional puede representarse mediante un diagrama multinivel como el mostrado en la figura 41.

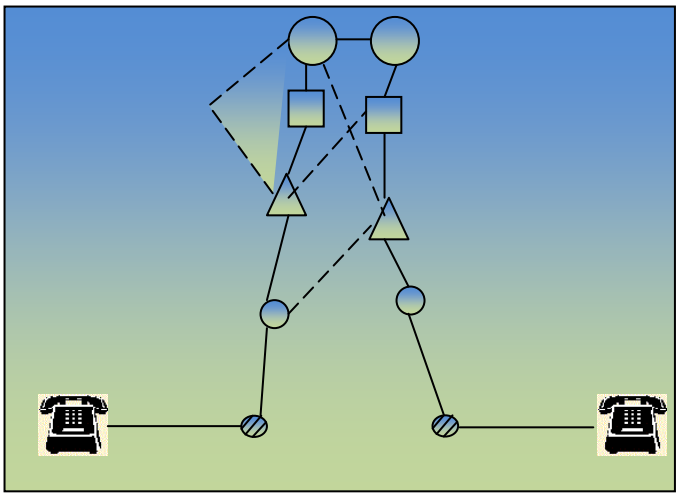


Figura 41

En la figura 41 podemos ver que existen diversos niveles de conmutación que se combinan para formar la red total. Lo normal es imaginar el sistema dividido en dos partes. La primera es la red de enlace local, que da servicio al abonado local, y que consta de la línea que va del abonado a la central local, de la central local al centro de conmutación primario, y de ahí al abonado llamado a través de otra central local. La segunda parte del sistema es la red de enlace interurbano, que se relacione únicamente con las llamadas que pasan al nivel del centro primario y por encima de él. De esta forma, el centro primario esta asociado a las dos partes de la red. El número de centrales existentes en cada uno de los diferentes niveles depende de varios factores: la extensión física de la red, el número de abonados, la cantidad de tráfico, el crecimiento previsto y los métodos de transmisión utilizados. Por encima del nivel superior del sistema nacional existe un nivel que da acceso a la red internacional, y que consta de una o más centrales internacionales.

2.1.4.1 RED EXTERNA

La red externa consta de los cables que conecta las líneas del abonado con la central telefónica, también son los cables que conecta a las distintas centrales telefónica. Cuando se desea prestar servicio a un número limitado de abonados, no es necesario que se instale una central telefónica para dar el servicio, sino que la empresa u oficina instala su propio conmutador privado (PABX) que se conecta al conmutador de la empresa telefónica, la topología usada es una malla como la figura 42.

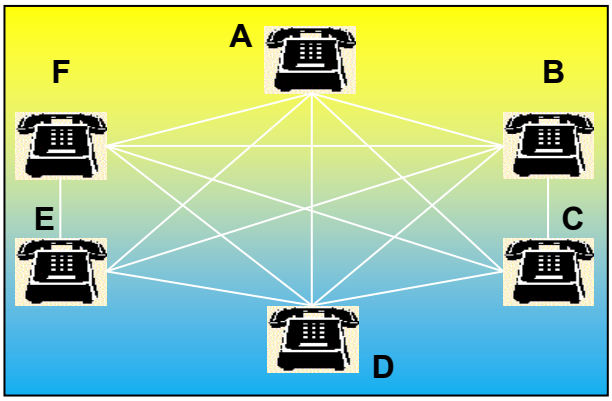


Figura 42

Y el número de enlaces será:

$$N_e = \frac{n(n-1)}{2}$$

De acuerdo con la anterior relación, a medida que el número de abonados, se incrementa, es necesario utilizar un conmutador que sea el núcleo de la topología en estrella, figura 43.

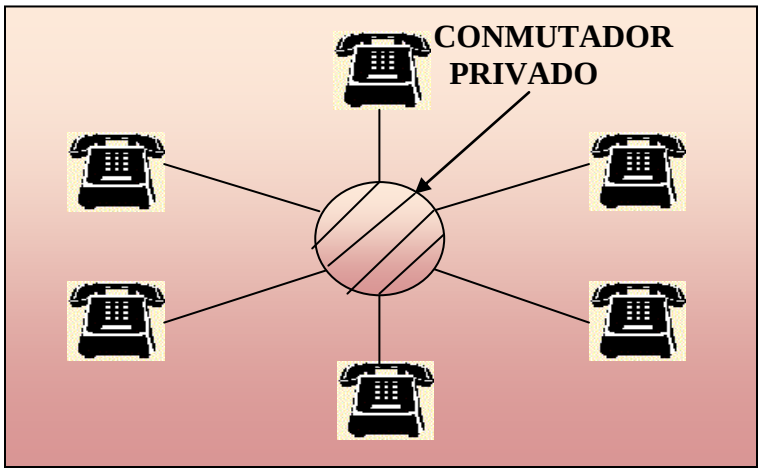


Figura 43

2.1.4.2 RED TRONCAL

Son los cables de fibra óptica de 12, 24 hasta 100 pares por cable o en su caso cable de 600 pares, los cuales se separan en **strip** de 50 pares cada uno, los cuales se identifican con números de 1,000 en adelante, tiene un calibre de ϕ de 0.5mm (AWG 24). La red troncal une únicamente:

- A las centrales de servicio local.
- A las centrales de servicio local y lada.
- A las centrales de lada-lada.
- Al conmutador de la central con las centrales locales y/o lada.

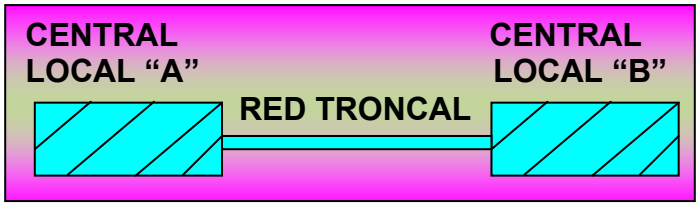


Figura 44

2.1.4.3 RED PRINCIPAL

Son los cables que parten del distribuidor de la central, hacia la caja de **distribución**, puede usar cables de 12 ó 24 pares de fibra óptica, en caso de usar cable de cobre, este tiene las siguientes características: Su calibre es 0.64mm o sea AWG 22. Normalmente la instalación de los cables es a través de canalizaciones.

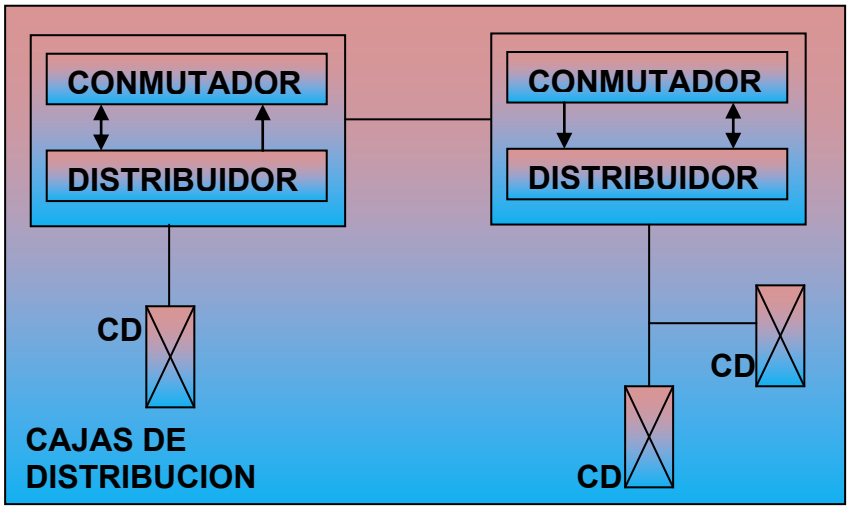


Figura 45

2.1.4.4 RED DIRECTA

Son los cables que parten del distribuidor de la central hacia los abonados, sin pasar por una caja de distribución, debido a que los abonados se encuentran a una distancia promedio de 300 metros a la redonda de la central telefónica. El cable de cobre usado es conocido como **paralelo 18**.

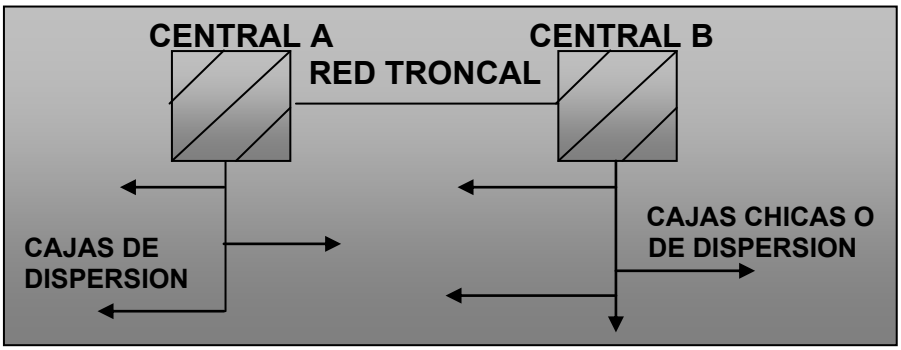


Figura 46

2.1.4.5 RED SECUNDARIA

Son los cables que parten de la caja de distribución hacia las cajas de dispersión, que contienen los cables para 10 abonados, las **cajas de dispersión o cajas chicas**, son las que se encuentran en los postes, fachadas de empresas u oficinas, las cajas de dispersión, se identifican porque contienen el distrito, número de la central, número del abonado y la marcación. A la red secundaria, se le conoce como **red aérea**, pues los cables de 100 pares, se encuentran colocados entre los postes de madera y la central telefónica, el cable más usado es conocido como **ASP**, pues tiene una guía de acero que sirve para tensar el mismo cable. De estos cables se forman grupos de 50 pares, que se identifican en la caja de distribución con la letra A, B, C D, E, etc.. Los grupos de 50 pares a su vez, se subdividen en grupos de 10 pares numerados de 1 a 5; anteponiéndoles la letra que les corresponde A1, B2, C3, etc..

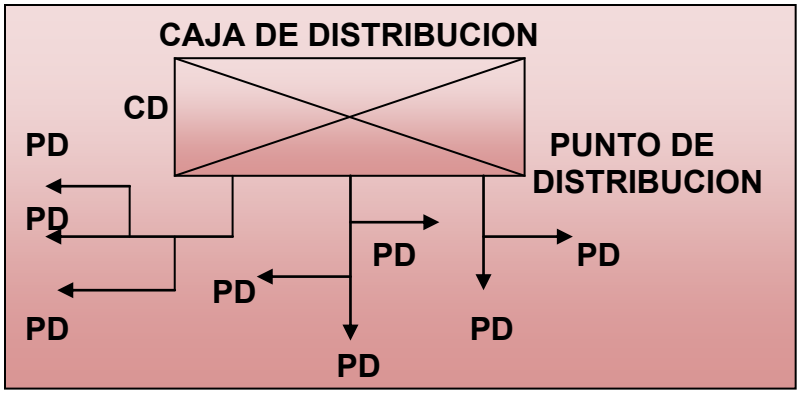


Figura 47

2.1.4.5.1 RED SUBSECUNDARIA

Es aquella que satisface las necesidades de abonados situados fuera de la zona urbana, pero de acuerdo a estudios económicos, no es costeable proporcionar servicio a través de una central local; el servicio se proporciona desde la zona urbana hacia cajas reguladoras (para que no se atenúe la señal). La figura 48 muestra una caja de distribución para 700 pares:

RED SECUNDARIA	RED PRINCIPAL
A-B	11-12
C-D	13-14
E-F	15-16
G-H →	

Son para servicios especiales: bomberos, hospitales escuelas, etc..

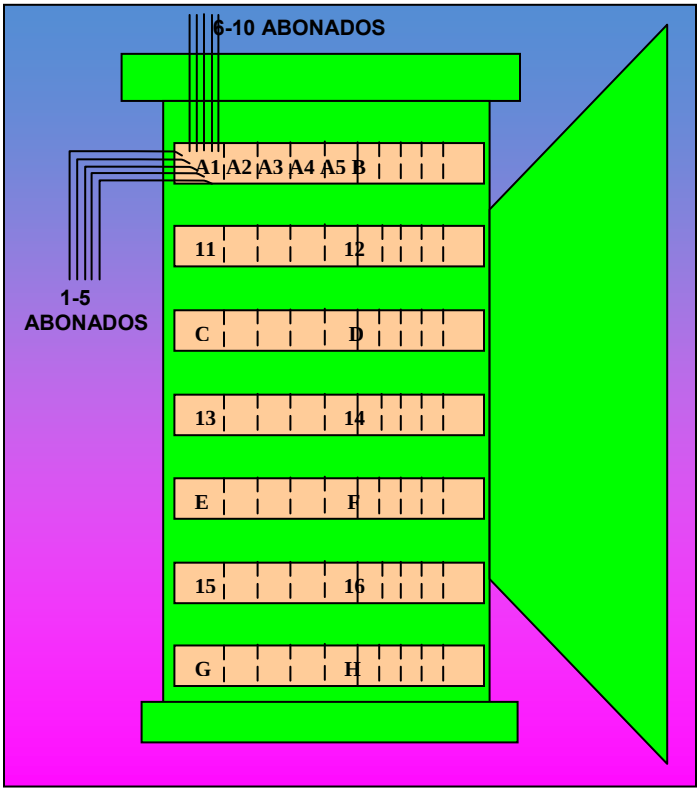
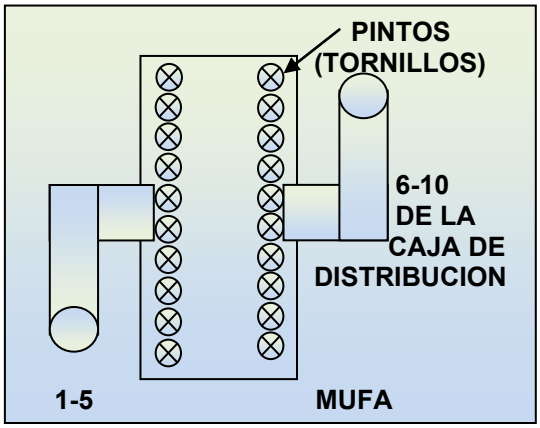


Figura 48



Para el A1 su mufa se compone como lo muestra la figura 49.

Figura 49

2.1.4.6 PUPINIZACION

Recordamos, que en un sistema, puramente capacitivo, el capacitor se convierte en un circuito abierto para el paso de la corriente directa, una vez que se ha cargado. En un sistema telefónico, la línea que conforma, principalmente la **red secundaria**, tiene un comportamiento capacitivo. Esto quiere decir, que en el instante en el que se descuelga el microteléfono la línea del **tip** y el **ring**, se comporta como una capacitancia, donde al tomarse su máximo valor de corriente y una vez cargado el capacitor, la corriente se hace **cero**, en unos milisegundos.

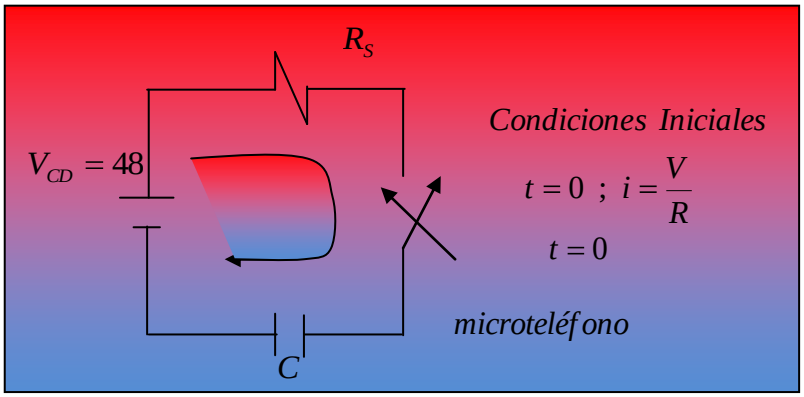


Figura 50

Analíticamente:
Aplicando LVK:

$$V = V_R + V_C$$

$$V = iR + \frac{1}{C}\int \frac{di}{dt}dt \rightarrow (1)$$

Derivando para eliminar la integral:

$$dV = R\frac{di}{dt} + \frac{1}{C}\int \frac{di}{dt}dt$$

$$0 = R\frac{di}{dt} + \frac{i}{C} \rightarrow (2)$$

Aplicamos que $D = {}^{d}\!/_{dt}$:

$$0 = RDi + {}^{i}\!/_{C}$$

Factorizando i:

$$0 = \left(RD + {}^{1}\!/_{C}\right)i$$

Dividiendo entre R:

$$0 = \left(\frac{RD}{R} + \frac{1}{RC}\right)i$$

$$0 = \left(D + \frac{1}{RC}\right)i \rightarrow (3)$$

En una ecuación diferencial lineal, homogénea y de primer orden:

$$i = Ke^{{}^{-t}\!/_{RC}} \rightarrow (4)$$

Para calcular a K aplicamos condiciones iniciales:

$$i = Ke^{{}^{-t}\!/_{RC}} \quad \forall t = 0; \ i = {}^{V}\!/_{R}$$

$$i = Ke^{0} = K$$

$$K = {}^{V}\!/_{R} \rightarrow (5)$$

Sustituyendo la ecuación (5) en la ecuación (4):

$$i = \frac{V}{R}e^{{}^{-t}\!/_{RC}} \rightarrow (6)$$

Obtención de la corriente en un sistema puramente capacitivo:

Para $t = 0;\ C = 2\mu f / 48V;\ R = 600\Omega$

$$i(0) = \frac{-48}{600} e^{0} = 80\,mA$$

Para $t = 0.5\,seg$

$$i(0.5) = \frac{-48}{600} e^{\frac{0.5}{600(*10^{-6})}} = 0$$

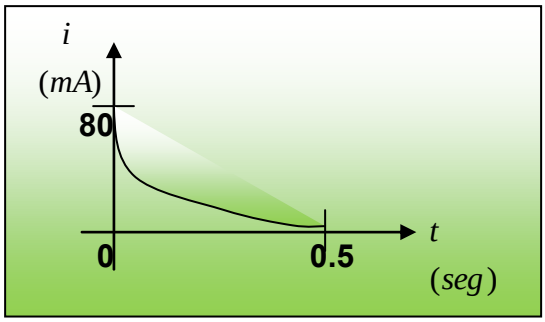


Figura 51

De acuerdo a todo lo anterior la red secundaria, se conectan bobinas de pupinización, **para quitar el efecto capacitivo de la red**, las bobinas de pupinización tiene una inductancia de 88mHy a una reactancia inductiva de 7Ω, las bobinas de pupinización, se encuentras en cajas, herméticamente selladas, con protección de plomo; de 30, 50, 70 y 100 bobinas, que serán colocadas en la línea de cada abonado. El fenómeno de pupinización causa los siguientes efectos en la red telefónica:

- Limita la banda de transmisión, como un filtro paso bajas obstaculizando el paso de frecuencias superiores a las de frecuencia de corte.
- Disminuye la atenuación dentro de la banda de paso.
- La atenuación es prácticamente igual para todas las frecuencias dentro de la banda de paso.
- Aumenta la impedancia característica.
- Reduce la velocidad de propagación.
- En troncales de conmutación de larga distancia, además de disminuir la atenuación, mejora las pérdidas de retorno en el extremo de la larga distancia.

2.1.4.6.1 BOBINAS DE PUPINIZACION

Tiene forma de anillo (toroide), en el cual se colocan los devanados de alambre (**tip** y **ring**). El núcleo es de cobre con aleación de hierro pulverizado, con el fin de mejorar la **permeabilidad**.

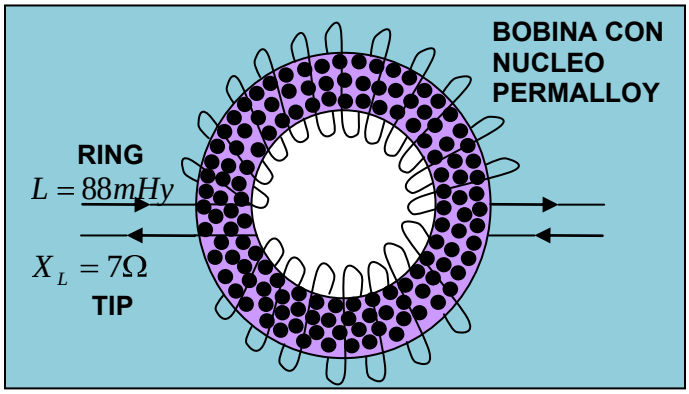


Figura 52

Los orificios que contiene el anillo, es con el fin de evitar la **saturación** de la señal y da como resultado la **distorsión** de la señal. Normalmente estas bobinas, se conectan en la red secundaria, correspondiendo una para cada abonado, para una distancia aproximadamente de 1,830 metros. Por ejemplo Telmex utiliza el siguiente código de bobinas:
19H88-50

$$\underbrace{19}_{\substack{Indica\,el\,Calibre\\ del\,Alambre\\ (AWG\,19)}}\quad \underbrace{H}_{\substack{Distancia\\ Máxima\\ (1{,}830m)}}\quad \underbrace{88}_{\substack{Inductancia\\ (88mHy)}}\quad \underbrace{-50}_{\substack{Número\,de\,Bobinas\\ Contenidas\,en\,la\\ caja}}$$

2.1.4.6.2 NORMAS DE APLICACIÓN

Telmex ha escogido el sistema designado 19H88 (bobinas de 88 mHy espaciadas cada 1,830 metros) con las siguientes características:

- Troncales entre centrales:
  1.-Mínimo de puntos de pupinización: 2.
  2.-Distancia entre las bobinas de los extremos a la central: ½ sección (915 metros).
  3.-Desviación máxima de distancia individual entre bobinas es de $\pm 5\%$.
- Líneas de abonado:
  1.-Mínimo de puntos de pupinización: 2.
  2.-Distancia de la primera bobina a la central: ½ sección (915 metros).
  3.-Distancia mínima de la última bobina a la caja de distribución: 915 metros.
  4.-Desviación máxima de distancia entre bobinas $\pm 5\%$.
  5.-En casos donde se tenga que prolongar la pupinización hacia cable secundario, para dar servicio a un grupo de abonados lejanos, se continuará la cuenta a partir de la central, procurando que la última bobina quede como máximo a ¾ de sección o más del suscriptor más cercano.

2.1.4.7 ESTRUCTURA DE LA RED TELEFÓNICA

Todo equipo telefónico tiene que estar posibilitado para comunicarse con cualquier otro en cualquier parte del país o del resto del mundo. Para conseguir este objetivo es preciso disponer de una **estructura de red**, entendiendo por tal el conjunto de equipos de abonados y centrales automáticas de conmutación telefónica interconectadas entre sí según unas pautas de encaminamiento de las comunicaciones previamente fijadas. La red esta diseñada en una **red jerárquica**, es decir una disposición de centrales conectadas entre sí, de modo que cada una de ellas dependiese de otra de un rango superior, permaneciendo unidas entre sí las de máxima categoría. La red jerárquica corresponde de un sistema básico de interconexión de centrales que en la mayoría de los casos se modifican en función de las peculiaridades del área geográfica y del volumen de tráfico a transmitir; estas circunstancias obligan a crear rutas directas entre centrales que no se contemplan en la jerarquización inicial de centrales. El punto donde se reúnen las líneas de abonados de todos los aparatos telefónicos de una determinada área queda definido como **central local**. De la posibilidad de interconectar entre sí la totalidad de las centrales locales surge la necesidad de estructurar la red, y de este modo se hace necesario de contar con un nivel superior de conmutación, **central primaria**, que al estar conectada a un cierto número de aquellas, permite la interconexión de equipos telefónicos pertenecientes a cualquiera de ellas. La misión de la central primaria es realizar transito para la interconexión de éstas. Existen centrales denominadas centrales tándem que son centrales de transito que cursan llamadas entre centrales primarias, actuando como concentradores y no pertenece a la red jerárquica, sino es un conjunto de enlaces directos no contemplados en la red jerárquica. La comunicación de abonados dependientes de dos centrales primarias se lleva a cabo mediante la conexión de otra central de mayor grado, la **central secundaria**, de la cual dependían todas las centrales del nivel inferior. La misión de las centrales secundarias es interconectar centrales primarias cursando llamas de transito, sin disponer en ningún caso de abonados propios. Las centrales que sirven para cursar llamadas entre centrales secundarias pertenecientes a distinta área que se conectan entre sí, son la **central terciaria**. La **central internacional** son las que cursan el tráfico entre distintos países.

2.1.5 CONMUTACION

La función de la conmutación es la encargada de establecer las conexiones apropiadas para enrutar o dirigir la comunicación a través de la red telefónica hacia su destino correcto por la vía más adecuada. Los equipos telefónicos se conectan a las centros de conmutación a través de las líneas de abonado, mientras que las centrales se conectan entre sí disponiendo de circuitos apropiados, enlaces, que posibilitan la conexión telefónica de abonados pertenecientes a dos

centrales distintas. Estos enlaces entre centrales están constituidos por medios de transmisión, como soporte de la señal telefónica, y por elementos pertenecientes a los equipos de conmutación de las centrales que interconectan. Tales enlaces permiten la conversación telefónica en ambos sentidos, pero a efectos de llamada se clasifican en unidireccionales y bidireccionales, entendiendo que en el primer caso sólo pueden establecerse llamadas en un sentido y en el segundo en ambos, aunque no simultáneamente. En función de las características y los cometidos de cada central, los equipos de conmutación están equipados para realizar llamadas locales (entre dos abonados de la misma central), llamadas salientes (de un abonado a otro perteneciente a otra central distinta), llamadas entrantes (conexión entre un enlace de llegada y la línea de abonado del teléfono destino), y llamadas de transito (la conexión precisa atravesar centrales intermedias entre enlaces de llegada y de salida). La finalización de una comunicación telefónica implica que la totalidad de los enlaces quedan libres con vistas a ser utilizadas en la siguiente comunicación. Tomando como referencia las cifras marcadas por el abonado que inicia la llamada, el equipo de conmutación aporta la inteligencia precisa para seleccionar el tipo de enlace requerido, y debe disponer en todo momento de la información interna necesaria para analizar la ocupación de los enlaces. Los sistemas modernos de conmutación incorporan computadoras para llevar a cabo estas misiones de control y decisión. Resulta imprescindible realizar estas funciones de supervisión y organización ya que, entre otras razones, el número de abonados que atiende una central es mayor que el número de enlaces de salida. En el caso, altamente improbable, de que todos los abonados dependientes de una misma central intentarán simultáneamente iniciar una comunicación telefónica, con abonados de otra central, los órganos de la central se verían imposibilitados para establecer estas conexiones. Desde otro punto de vista, debe indicarse que todo par de hilos conectados a los equipos telefónicos de una central disponen en esta de su correspondiente equipo de línea el cual detecta el descolgado del teléfono, iniciando el proceso de llamada que encaminará el equipo de señalización; en términos generales se dispondrá de un circuito de salida por cada veinte teléfonos conectados a la central. Dentro de la red general telefónica se pueden distinguir estructuras de **red analógica** y de **red digital**.

2.1.5.1 SISTEMAS DE CONMUTACIÓN

Son muchos los tipos de centrales de conmutación que en la actualidad coexisten en el mundo, aunque la tendencia de todos los países esta encaminada a la incorporación total de sistemas de conmutación digital. Configurar una clasificación de los sistemas de conmutación supone considerar las técnicas empleadas en las redes de conexión y unidades de control de las centrales. La siguiente distribución sitúa en el tiempo los distintos sistemas aparecidos en el mundo de la conmutación telefónica:

- **Conmutación Manual**.-Utilizada entre los años 1880-1910.
- **Conmutación Electromecánica**.-Cubre un período de sesenta años entre 1910-1970 distinguiendo las siguientes generaciones de sistemas:
    1) **Sistemas Paso a Paso**.-Entre los años 1910-1960.
    2) **Sistemas de Control Directo**.-Tipo Rotary, entre 1920-1960.
    3) **Sistemas de Barras Cruzadas**.-En el período que transcurre entre los años 1940-1975.
- **Conmutación Electrónica**.-Aparecida al final de los años sesenta, abarca tres generaciones de sistemas:
    1) **División Espacial y Control de Programa Almacenado**.-En el período de 1965-1975.
    2) **División Temporal con Mando Digital Centralizado**.-Entre los años 1970-1985.
    3) **División Temporal con Mando Digital Distribuido**.-Desde 1985.

Un sistema de conmutación digital esta estructurado en base a un bloque de interfaces, que facilita la conexión con las líneas de abonado y enlace de otros sistemas de conmutación, la red de conexión digital, que establece las interconexiones con los distintos elementos del sistema, y el bloque de control que, mediante procesadores, coordina el tráfico del sistema y supervisa todas sus funciones. El tratamiento de 30,000 llamadas/hora en centrales de conmutación especial en el año de 1976, se convirtió cuatro años más tarde en 550,000, utilizando centrales de conmutación temporal.

FUNCIONES DE LA CONMUTACIÓN DIGITAL

Los equipos de conmutación deben de proporcionar multitud de funciones para conseguir un perfecto interfuncionamiento de la red. Dentro de ellas, destacamos como más significativas las siguientes:

- Interconexión entre líneas de abonado de la red.
- Supervisión de líneas, enlaces y análisis de las situaciones.
- Control, actuación sobre la red en base a la información recibida.
- Señalización con las terminales del abonado y con otros centros de conmutación.
- Almacenamiento de las señales de llamada para completar su encaminamiento.
- Selección y conexión, establecimiento final de la comunicación.
- Explotación y mantenimiento del conjunto de la red.
- Sincronización de todas las centrales que configuran una red digital integrada.
- Temporización o sincronización de los elementos internos de la central.
- Conmutación de paquetes, posibilidad de admitir conexiones de terminales de datos que trabajan en dicha modalidad mediante la incorporación de equipos complementarios.
- Tarificación del tráfico cursado a través de las líneas de abonado que acceden a la central.
- Centralización de las funciones de operación, mantenimiento, administración y gestión de la red.

2.1.5.1.1 CONMUTADORES DE MATRIZ

Conmutadores de matriz. Dentro del sistema telefónico son comunes varias clases de conmutadores. La clase más simple es el conmutador de matriz, el cual se muestra en la figura 53. En un conmutador con “n” líneas de entrada y “n” líneas de salida, el conmutador de matriz tiene “n” intersecciones llamadas puntos de cruce, donde se pueden conectar una línea de entrada y una de salida con un conmutador semiconductor, como se aprecia en la figura 53(a). En la figura 53(b) vemos un ejemplo las líneas entre sí. Todos los bits que llegan al conmutador por la línea 4, por ejemplo, se envían de inmediato por la línea 0. De este modo, el conmutador de matriz instrumenta la conmutación de circuitos al efectuar una conexión eléctrica directa, casi como la de los cables puenteadores de los conmutadores de la primera generación, sólo que en forma automática y en microsegundos.

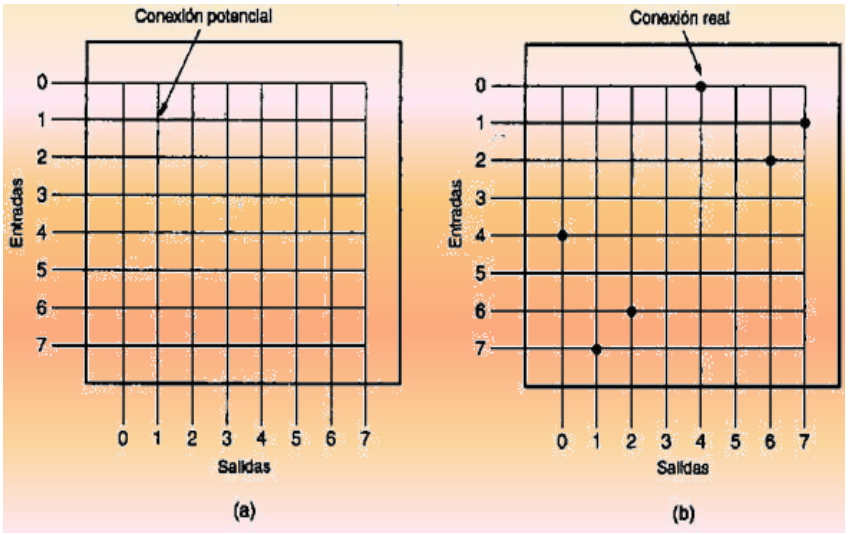


Figura 53

Si suponemos que todas las líneas son dúplex y que no existen autoconexiones, solamente se necesitan los puntos de cruce arriba de la diagonal, que son n(n – 1)/2. Para n = 1000, necesitamos 499,500 puntos de cruce. Aunque es posible construir un circuito integrado VLSI con esta cantidad de conmutadores de transistores, no lo es tener 1000 terminales en el circuito

integrado. Por ello, un sólo conmutador de matriz es útil solamente para oficinas finales relativamente pequeñas.

2.1.5.1.2 CONMUTADORES POR DIVISION EN EL ESPACIO

Si dividimos el conmutador de matriz en marcos pequeños y los interconectamos podemos construir conmutadores de múltiples etapas con muchos menos puntos de cruce. Éstos se llaman conmutadores por división en el espacio. En la figura 54 se ilustran dos configuraciones. En la primera etapa, cada matriz tiene “n” entradas, así que necesitamos N/n de ellas para manejar todas las N líneas que entran. La segunda etapa tiene “k” matrices, cada una con N/n entradas y N/n salidas. La tercera etapa es una repetición de la primera, pero invertida de izquierda a derecha. Cada matriz intermedia se conecta a cada matriz de entrada y cada matriz de salida. En consecuencia, es posible conectar cada entrada a cada salida usando ya sea la primera matriz intermedia de la figura 54 o bien la segunda. De hecho, existen dos trayectorias disjuntas de cada entrada a cada salida, dependiendo de cuál matriz intermedia se escoja. En la figura 54(b) hay tres trayectorias para cada par de entrada/salida. Con “k” etapas intermedias (k es un parámetro de diseño), existen “k” trayectorias disjuntas. En la primera etapa hay N/n matrices, cada una con nk puntos de cruce, para un total de Nk. En la segunda etapa hay “k” matrices, cada una con (N/n)~ puntos de cruce. La tercera etapa es como la primera. Al sumar las tres etapas obtenemos:
Cantidad de puntos de cruce = 2kN + k(N/n)

El conmutador se puede bloquear. Considere de nuevo la figura 54(a). La etapa 2 tiene ocho entradas, de modo que se puede conectar un máximo de ocho llamadas al mismo tiempo. Si llega la llamada nueve, tendrá que recibir una señal de ocupado, aunque el destino esté disponible. El conmutador de la figura 54(b) es mejor porque puede manejar un máximo de 12 llamadas en lugar de 8, pero tiene más puntos de cruce. Debe ser obvio que, cuanto mayor sea “k”, más costoso será el conmutador y menor la probabilidad de bloqueo.

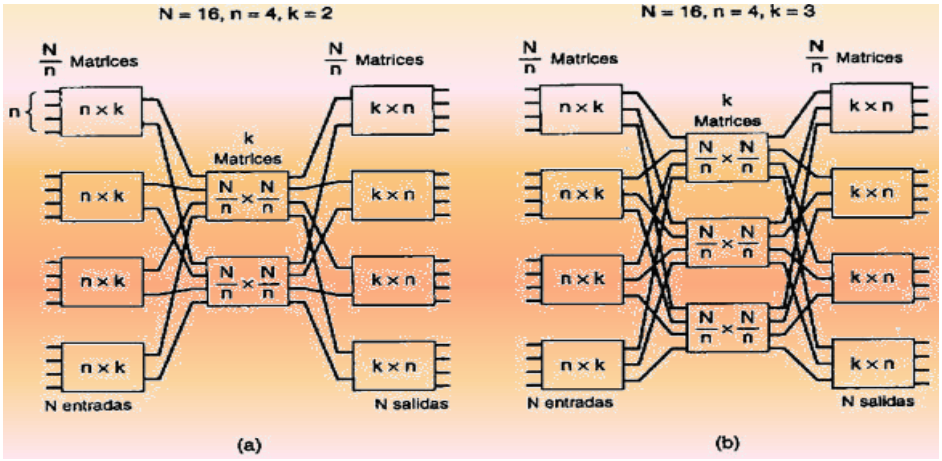


Figura 54

2.1.5.1.3 CONMUTADORES POR DIVISION EN EL TIEMPO

El conmutador por división en el tiempo se ilustra en la figura 55. En la conmutación por división en el tiempo, las “n” líneas de entrada se examinan en secuencia para construir un marco de entrada con “n” ranuras. Cada ranura tiene “k” bits. El corazón del conmutador por división en el tiempo es el intercambiador de ranuras de tiempo, que acepta marcos de entrada y produce marcos de salida en los que se han reordenado las ranuras de tiempo. En la figura 55, la ranura de entrada 4 sale primero, a continuación la 7, y así sucesivamente. Por último, el marco de salida se desmultiplexa y la ranura de salida 0 sale por la línea 0, etc. En esencia, el conmutador ha transferido un byte de la línea de entrada 4 a la línea de salida 0, otro byte de la línea de entrada 7 a la línea de salida 1, y así sucesivamente. El intercambiador de ranuras de tiempo funciona como

sigue: cuando un marco de entrada está listo para procesarse, cada ranura se escribe en un buger de RAM dentro del intercambiador. Las ranuras se escriben en orden, de modo que la palabra “i” del buger contiene la ranura “i”. Una vez almacenadas en el buger todas las ranuras del marco de entrada, se construye el marco de salida leyendo las palabras del buffer. Un contador va de 0 a n – 1. En el paso “j” se lee el contenido de la palabra “j” de una tabla de transformación y se usa para apuntar a una dirección del buffer en RAM. Así, si la palabra 0 de la tabla de transformación contiene un 4, se leerá primero la palabra 4 del buger en RAM y la primera ranura del marco de salida será la ranura 4 del marco de entrada. De este modo, el contenido de la tabla de transformación determina cual permutación del marco de entrada se generará como marco de salida, y por ende cual línea de entrada se conectará con cuál línea de salida. Los conmutadores por división en el tiempo usan tablas que son lineales en lugar de cuadráticas en cuanto a la cantidad de líneas, pero tienen otra limitación. Es necesario almacenar “n” ranuras en la memoria temporal RAM y luego leerlas otra vez en un periodo de marco de 125pseg. Si cada uno de estos accesos a la memoria tarda “T” microsegundos, el tiempo necesario para procesar un marco es 2nT microsegundos, así que tenemos 2nT = 125 o n = 125/2T. Si la memoria tiene un tiempo de ciclo de 100 nseg, podemos manejar cuando mucho 625 líneas. También podemos invertir esta relación y usarla para determinar el ciclo de memoria requerido para manejar una cantidad determinada de líneas.

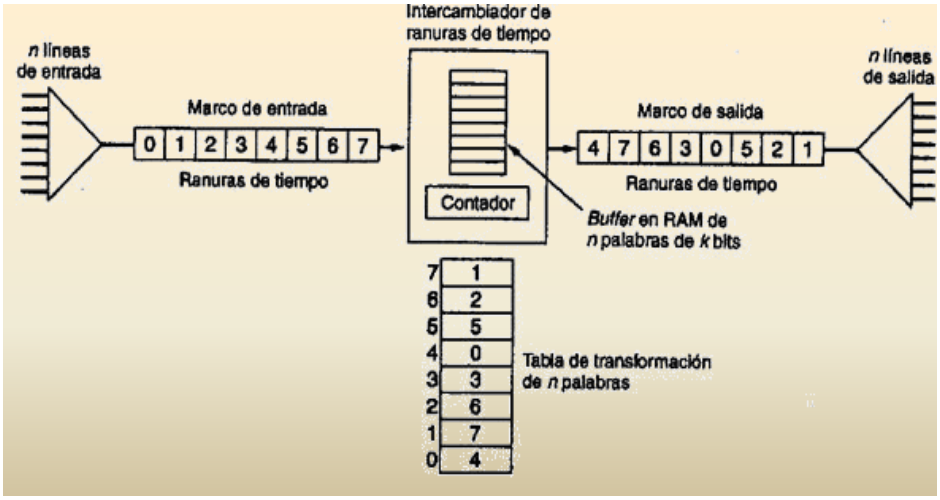


Figura 55

2.1.6 SEÑALIZACION

El establecimiento previo de un determinado lenguaje entre las terminales telefónicas y las centrales que las conectan, con el fin de encaminar la llamada hasta su destino y completar la comunicación se conoce como **señalización**. Se inicia al descolgar el auricular del teléfono que produce la llamada y detectar la central una determinada señal. A partir de ese momento la central debe identificar el número del abonado, facilitarle el tono de marcación, identificar el número del abonado destino, decidir el enlace de salida, concretar el encaminamiento entre las centrales, avisar al abonado llamado, efectuar la conexión, mantenerla hasta su término impidiendo la entrada de otras llamadas y, reestablecer todos los órganos de la comunicación cuando haya finalizado. Además deben de registrar la llamada, para proceder a su facturación de acuerdo con una normativa. El establecimiento de toda conexión telefónica contempla varios tipos de señalización según los tramos de la comunicación, uno entre el **abonado-central** y el inverso en el extremo opuesto, un segundo es la **señalización interna** del centro de conmutación, y el último, la **señalización entre centrales**.

2.1.6.1 SEÑALIZACION DE ABONADO

Es el conjunto de señales que se manejan en la línea de abonado que tienen por objeto ocupar, supervisar y liberar dichas líneas. Se pueden distinguir tres tipos de estas señales:

- **Señales de Información**.-Constituidas por tonos en los rangos de frecuencia vocal. Estas envían información al abonado distante.
- **Señales de Supervisión**.-Son peticiones de servicio. Levantar el microteléfono equivale a enviar la señal de **descolgado** (o de ocupación de línea) que indica el origen de llamada. Reponer el microteléfono equivale a enviar la señal de **colgado** (o de liberación de línea) que indica desconexión. Para este tipo de señalización se abastece corriente directa desde la central sobre la línea del abonado. La señal de confirmación de ocupación, esta constituida por corriente alterna con frecuencia de 425Hz a 450Hz se genera en la central desde donde la recibe el abonado que descuelga con tono de invitación a marcar. Las señales de supervisión indican a la central que el abonado desea originar, contestar desconectar una llamada. Este dispositivo se diseñara para indicar cuatro condiciones posibles:
  1) **Estado Normal de Reposo**.-Existe cuando el microteléfono esta colgado.
  2) **Estado Llamante**.-Se indica mediante la señal de ocupación de línea (descolgado).
  3) **Estado de Conversación**.-Es una condición de descolgado.
  4) **Estado de Desconexión o Liberación**.-Se indica mediante la señal de colgado.

  Las señales de supervisión se generan antes y después de que se ha establecido la conversación. La corriente directa que se establece en la línea del abonado se emplea como señal de supervisión, así como para alimentar el microteléfono del teléfono que transmite. Debido a la necesidad de evitar la interferencia de las señales de supervisión y las de voz, los sistemas de señalización de supervisión se deben diseñar muy cuidadosamente para que las corrientes de voz no causen operaciones falsas.
- **Señales de Control**.-Es información que se requiere para completar la conexión. El disco dactilar genera este tipo de señales mediante la interrupción del flujo de corriente directa y el teclado genera señales monofrecuentes (tonos).

2.1.6.2 SEÑALIZACION ENTRE CENTRALES

La señalización entre centrales puede manejarse en base a C.D. o en base a C.A.. La señalización a C.D. se aplica a distancias cortas. La señalización a C.A. se emplea principalmente entre troncales interurbanas y siempre que la señalización a C.D. no sea posible. Se han desarrollado dos clases generales de métodos de señalización a C.D. que son: **Señalización en Circuito** y **Señalización E y M**.

2.1.6.2.1 SEÑALIZACION EN CIRCUITO

Es el tipo más simple, se emplea más comúnmente en troncales urbanas. Las señales de supervisión y control se generan; ya sea: interrumpiendo el flujo de corriente, cambiando su valor o invirtiendo su dirección en el extremo distante de la línea troncal los cambios de contacto se detectan en el otro extremo de la troncal.

2.1.6.2.2 SEÑALIZACION POR INVERSIÓN DE LA BATERIA

La señalización por inversión de la batería se utiliza muy frecuentemente en los sistemas de conmutación electromecánicos. Mediante esta señalización se realizaba la supervisión y control de las líneas troncales entre centrales urbanas. Cuando una troncal urbana esta libre, existe polaridad en sus conductores; en las centrales de coordenadas y paso a paso el conductor **R** de la troncal tiene batería y el conductor **T** tierra. La polaridad se crea durante procesos de llamada. Este estado de batería y tierra de la línea troncal le indica a la central de origen que el teléfono llamada esta colgado y sonando. Cuando el teléfono es levantado, la señal de **descolgado** que resulta provoca

que el equipo de la central terminal invierta el potencial de batería de la línea troncal hacia la central de origen. Esto representa para la central de origen la indicación que el abonado llamado ha contestado, con lo que el equipo de conmutación completa la trayectoria de voz.

2.1.6.2.3 SEÑALIZACION E Y M

La letra **E** se ha tomado de la **e** intermedia de la palabra recepción y la **M** de la **m** de transmisión. La señalización E y M se puede emplear con los métodos señalización a C.D. y a C.A., pudiéndose utilizar diferentes arreglos de terminal para ambas clases. Entre los sistemas de señalización E y M a C.D. que más se emplean son los sistemas dúplex, full-dúplex y half-dúplex. Estos sistemas permiten la señalización y el pulso de marcación sobre distancias más largas de lo que es posible con la señalización en circuito. La señalización E y M se emplea con los métodos C.A. de frecuencia única de los sistemas dentro y fuera de banda. En todos estos sistemas, las señales se pueden enviar en ambas direcciones al mismo tiempo sin que interfieran entre sí. En el método de señalización E y M, la terminal E es conductor de recepción de señal que refleja la excitación del extremo lejano de la troncal. Tierra en la terminal E indica que se ha recibido una señal desde el otro extremo. Cuando la troncal esta libre existe la condición de cero señal, se dice entonces que la terminal E esta abierta o no ha aterrizado. La terminal M transmite la situación en el extremo cercano de la troncal. Se aterriza cuando la troncal esta libre o siempre que el teléfono del abonado del extremo cercano esta colgado en cuyo caso no se envía señal. Cuando la troncal se tomo o el abonado llamado descuelga, el potencial de batería se sustituye por tierra en la terminal M, transmitiendo señal hacia el otro extremo de la troncal.

2.1.6.3 SEÑALIZACION A CORRIENTE ALTERNA

La señalización a C.A. que emplea frecuencias en el rango de voz (300Hz-3,400Hz) se conoce como señalización dentro de la banda de frecuencia vocal. En estos sistemas se emplean una misma trayectoria para la información de la voz y de señalización por lo que se debe evitar la interferencia mutua. En particular se debe proteger el equipo receptor de señalización para evitar operación falsa con los sonidos de conversación pues el receptor permanece en operación durante la conversación para responder a las indicaciones de señalización. La señalización fuera de banda utiliza frecuencias fuera de la banda de la frecuencia vocal, generalmente en el rango de 3,400Hz-3,700Hz, evitando de esta manera la interferencia de la voz. Además, permite el empleo de niveles más altos de tonos de señalización. El sistema de señalización dentro de banda es más usado es el modo monofrecuente o de frecuencia única que utiliza la frecuencia de 2,000Hz en ambas direcciones para troncales que operan en base a 4 hilos. Para operación a 2 hilos, se proporcionan dos frecuencias, 2,600Hz en una dirección y 2,400Hz en la dirección contraria pues, como se sabe, en este caso la misma trayectoria de transmisión a 2 hilos se emplea entre terminales. Las señales de C.D. que se reciben del equipo troncal se convierten en tonos de 2,600Hz para su transmisión sobre el canal de voz. En el extremo distante los tonos que se reciben se regresan a señales de C.D..

2.1.6.4 SEÑALIZACION DENTRO DE BANDA

Puesto que la frecuencia de señalización esta dentro del ancho de banda de la banda de voz (300Hz-3,400Hz), existirán, problemas asociados a este método de señalización: no podrá funcionar durante la conversación, y los equipos deberán ser capaces de distinguir entre una forma de onda vocal y una señal. A estos efectos se dispone de 2 parámetros que pueden variar: la frecuencia de la señal y el tiempo de identificación de la misma. Otras consideraciones que ayudarían a distinguir entre una voz y una señal son:

- Que la voz a la frecuencia de la señal esta acompañada por otras frecuencias.
- Que se puede utilizar más de una frecuencia de señal.
- Que las señales puede ser ráfagas codificadas de la frecuencia de la señal.

La elección esta relacionada con las características frecuenciales de la voz. Cuando mayor es la frecuencia mayor es la diafonía, por lo que resulta necesario hacer una transmisión a bajo nivel. Si

la amplitud es pequeña, el receptor debe ser muy sensible, con lo que aumenta la probabilidad de que la señal vocal de bajo nivel simula la señalización. Las características del canal pueden variar, de un enlace a otro, en el extremo superior de la banda, de forma que en algunos enlaces de cierta antigüedad la frecuencia de corte puede estar por debajo de los 3,400Hz. Además, la variación de la amplitud con la frecuencia es bastante pronunciada en las frecuencias altas, por lo que cualquier cambio en la frecuencia de la señal dará lugar a un cambio significativo en la amplitud de la misma. A partir de todas estas consideraciones se observa la necesidad de llegar a una solución intermedia, y en la práctica la frecuencia se elige dentro del intervalo que va de 2,040Hz a 3,000Hz.

2.1.6.5 SEÑALIZACION POR IMPULSOS

La identificación de una señal se determina a partir de su duración y de su secuencia. Este tipo de señalización tiene las siguientes características:

- Tiene un mayor repertorio de señales que la señalización en directa.
- Se pueden transmitir mayores niveles de tensión y, por consiguiente, proporciona una mejor relación S/R.
- Es menos vulnerable a las interferencias.
- Complica las conversiones C.D./C.A. y C.A./C.D., ya que los impulsos tienen que estar cuidadosamente sincronizados.
- Necesita equipos de memoria en el receptor para la identificación de los impulsos.

2.1.6.6 SEÑALIZACION EN DIRECTA

Existen dos tipos de señalización por frecuencia vocal en directa:

A) De secuencia dirigida y **B) De secuencia no obligada con dos estados**. El primero en el sistema de señalización CCITT No. 5 y el segundo es el sistema BellSF. En el tipo A) se interrumpe una señal cuando se detecta un acuse de recibo, mientras que en el B) la información de la señal se transmite por el tipo de cambio de estado y no se utilizo acuses de recibo. En términos de fiabilidad A) es preferible a la señalización por impulsos que a su vez es preferible al tipo B); aunque el A) es mucho más lento que el B), pues depende de las señales de acuse de recibo y, por lo tanto, del tiempo de propagación la lentitud del sistema A) hace que sólo se utilice en aplicaciones especiales. En el sistema B), el tono esta activado durante la mayor parte del tiempo de no conversión, lo que puede llevar a una sobre carga del sistema de transmisión sino se limita el nivel de la señal.

2.1.6.7 SEÑALIZACION FUERA DE BANDA

Este término se aplica, generalmente, a un sistema de señalización en el que la frecuencia de la señal esta incluido dentro del intervalo que va de 3,400Hz a 4,000Hz. La frecuencia recomendada por el CCITT es de 3,825Hz, aunque también se utilizan los valores 3,700Hz y 3,850Hz. Este método sólo es aplicable a sistemas con portadora, ya que los equipos utilizados para transmitir en banda base pueden atenuar la frecuencia de la señal. En comparación con la señal dentro de banda existen dos ventajas:

- No es necesario tomar precaución alguna para evitar que la voz imite a la señal.
- Se pueden transmitir la voz y las señales simultáneamente.

La señalización dentro de la etapa de conmutación suele ser en directa, de aquí que la señalización fuera de banda se haga enlace a enlace con convertidores de C.A./C.D. y C.D./C.A. En cada extremidad se utilizan filtros para garantizar que no haya frecuencias parásitas y para aislar la señal antes de que llegue al receptor. Este tipo de señalización tiene la ventaja de su sencillez y, por consiguiente, de ser bastante económico. Puede ser de dos tipos: por impulsos o en directa a dos etapas existen dos inconvenientes inherentes a ambos modos: la señalización en directa no puede realizarse a un nivel demasiado alto debido al riesgo de sobre carga (por lo que el receptor debe ser muy sensible), mientras que la señalización por impulsos, para realizar la función

de memoria, exige circuitos más sofisticados. En la práctica se prefiere el modo en directa debido a su simplicidad (en contra posición con la señalización dentro de banda, en la que el modo por impulsos será más ventajosa). La señalización fuera de banda es más atractiva que la señalización dentro de banda, aunque no siempre se puede aplicar a "s" plantas de transmisión existentes sin un gasto considerable, en consecuencia se utiliza comúnmente en los sistemas FDM, siendo la señalización por frecuencia vocal la más común en los sistemas existentes. Existen dos modos de señalización en directa: de tono durante trabajo y de tono durante reposo, habiendo pocas diferencias entre las que poder elegir para la mayor parte de las aplicaciones; no obstante, suele preferirse el modo durante reposo o si el sistema es de utilización general, ya que el tono durante el trabajo tiende a sobre cargar el sistema de transmisión.

2.1.6.8 SEÑALIZACION DE LINEA

La función principal de la señalización de línea es supervisar la conexión entre centrales. El circuito troncal de la central genera información en base a C.D. convirtiéndose después a señales de C.A. para manejar, sobre la línea troncal, señales de una sola frecuencia de duración variable que se transmiten hacia el circuito troncal distante. En este extremo, la señal regresa a su forma de pulsos de C.D. de duración variable con la que el circuito troncal efectúa las funciones de señalización subsecuentes hacia el equipo de conmutación. Las señales de C.D. que se generan en el circuito troncal, para la señalización de línea, son de tres tipos, que se diferencia por su duración:

$Pulso\,corto$	$150ms \pm 20\%$
$Pulso\,largo$	$600ms \pm 20\%$
$Señal\,continua$ $(para\,bloqueo)$	$1{,}000ms$

Además una señal se considera como permanente cuando esta es mayor a los $2{,}000ms$. El intervalo de tiempo entre dos señales que se envían en la misma dirección por la misma troncal es igual o mayor a $330ms$. A base de estos elementos, se establece un **código de señalización de línea**, el cual proporciona las siguientes señales de línea:

- **Señal de Toma**.-Consiste de un elemento de señal corta.
- **Señal de Liberación Forzada**.-Consiste de un elemento de señal larga.
- **Señal de Respuesta y de Nueva Respuesta**.-Consiste de un elemento de señal corta; se envía hacia la central (de origen para indicarle que el abonado llamado ha levantado su microteléfono). La función de esta señal es de supervisión, pudiéndose emplear para iniciar el cobro. Las señales de nueva contestación siguen a una señal de liberación, si la parte llamada vuelve a levantar su microteléfono después de haberlo colgado.
- **Señal de Liberación Hacia Atrás**.-Consiste de un elemento de señal larga; su función es de supervisión y se envía para indicar que el abonado llamado ha colgado. Esta señal inicia en la troncal de origen la temporización para la liberación del equipo que quedó retenido.
- **Señal de Liberación Hacia Adelante**.-Consiste de un elemento de señal larga. El envío de esta señal se inicia en la troncal de salida, una temporización de $5ms\ a\ 10\,ms$ durante la cual se debe recibir desde la otra terminal de línea a la señal de liberación de guarda. La señal de liberación hacia delante se puede enviar en cualquier momento de la selección o la conversación iniciando en la troncal de entrada, al otro extremo del circuito, la interrupción inmediata del circuito de conmutación o bien de la conversación. Esta señal normalmente se envía en los siguientes casos:
  1) Cuando el abonado A cuelga al final de la conversación.
  2) Cuando el abonado A cuelga al final de la selección.
- **Señal de Liberación de Guardia**.-Consiste de un elemento de señal larga y se transmite en la dirección hacia atrás como respuesta a la señal de liberación hacia delante, para indicar que se ha realizado la liberación de la conexión en el extremo de entrada del

circuito. Para asegurar la liberación apropiada de la conexión en una central de tránsito, se hace accionar una alarma cuando la troncal de salida recibe una señal de liberación de guardia antes de que la conexión en la central se libere. Como las señales de liberación de guardia, liberación forzada y liberación hacia atrás son de la misma longitud, la condición de alarma ocurre también después de la señal de liberación hacia atrás. La señal de liberación de guardia se envía únicamente si la señal de liberación hacia delante ha sido procedida por una señal de tono con longitud correcta. Si no se recibe liberación de guardia, por ejemplo debido a una falla en la línea. La troncal de salida se bloquea.

- **Señal de Bloqueo**.-Consiste de una señal continua que se envía desde la troncal de entrada para bloquear la troncal de salida en el otro extremo del circuito. La troncal de salida se libera tan pronto como la señal de bloqueo cesa.
- **Señales de Operadora**:
    1) **Señal de Ofrecimiento y Señal de Cancelación**.-Consisten, cada una, de un elemento de señal corta. La señal de ofrecimiento se envía cuando la operadora desea entrar en la conversación; la señal de cancelación, cuando quiere dejarla. Los abonados que se encuentran en la comunicación, al entrar la operadora en el mismo circuito del habla escuchan un tono de ocupado con un nivel de audición más bajo.
    2) **Señal de Rellamada**.-Consiste de dos elementos de señal corta. Esta señal se envía cuando la operadora quiere llamar a un abonado que, a solicitud de la misma, ha repuesto su microteléfono al enterarse de que tiene una llamada de larga distancia.
    3) **Señales de Medición**.- Consiste de un elemento de señal corta que se conoce como pulso de medición. Se envían pulsos de medición durante la conversación. Las señales de medición se envían en la dirección hacia atrás desde la central en la que se efectúa el cobro o la recepción o la retransmisión de la señal de respuesta esta central no retransmite ninguna de las siguientes señales hacia atrás. Los impulsos de medición se reciben en la central de salida y al final de cada impulso el medidor del abonado avanza un paso. Las señales de liberación hacia atrás y nueva respuesta del abonado llamado se reciben después en la central de control de cuota. Al recibir una señal de liberación hacia atrás, la central de control de cuota empieza la supervisión del tiempo. Si temporizo antes de recibir una señal de liberación hacia delante o una señal de nueva contestación, envía una señal de liberación forzada hacia atrás a la central de origen. Puesto que la señal de liberación forzada consiste de un elemento de señal larga, no avanzará el medidor del abonado sino que iniciará únicamente señalización de liberación hacia delante.

La tabla 11 resume las señales que se manejan en la señalización de línea.

Señal	Duración	Dirección
Toma	150mseg	→
Liberación forzada	600mseg	←
Respuesta	150mseg	←
Liberación hacia atrás	600mseg	←
Liberación hacia adelante	600mseg	→
Liberación de guardia	600mseg	←
Bloqueo	Continuo	←
Operadora	150mseg	→
Medición	150mseg	←

Tabla 11

2.1.6.9 SEÑALIZACION DE REGISTRO

Las señales de registro se emplean para transmitir información numérica que se necesita para el establecimiento de la conexión. Las frecuencias de señalización están dentro de la banda de voz y para hacer posible la señalización simultanea sobre un mismo canal en ambas direcciones en un circuito de 2 hilos, se utilizan diferentes frecuencias para la señalización hacia atrás. El equipo se utiliza para el envío y recepción de señales de registro esta asociado únicamente con los registros y receptores de código.

2.1.6.10 SEÑALIZACION MULTIFRECUENCIA

Este tipo de señalización se emplea para la transmisión de información numérica o de selección (señalización entre registros). El sistema transmite los dígitos por combinaciones de 2 a 6 frecuencias; las combinaciones para los dígitos 1 al 0 y 5 para las señales adicionales (códigos auxiliares). La velocidad de transmisión promedio de las cifras es por lo menos 5 dígitos por segundo. Los dígitos se envían bajo el control del equipo receptor por medio de las señales de control. Se emplean dos tipos de señales de control. Señales que se emplean para establecer la conexión con la línea llamada y señales que se emplean para indicar el estado de esta línea. El primer tipo se conoce como señales A y el segundo como señales B. Se emplean las mismas frecuencias para las señales A y B. El cambio para la interpretación de señales de control del modo A y B se realiza mediante la señal A3, como se muestra en la tabla 12.

C/S				Número de la señal	Señales A	Señales B
1140	1020	900	780			
X	X			1	Enviar siguiente dígito	Abonado libre (cobro)
X		X		2	Enviar 1er dígito	Abonado ocupado
	X	X		3	Cambio a señales B	Intercepción
X			X	4	Congestión	Congestión
	X		X	5		Abonado libre (sin cobro)
		X	X	6	Identificación de abonado que llama	Número prohibido

Tabla 12

- **Señal de Congestión (A4)**.-En cualquier momento de establecer la conexión, un receptor de código puede enviar señal de congestión hacia el registro de origen. El registro que recibe esta señal indica entonces la señalización de liberación de avance.
- **Solicitud de Identificación**.-Cuando un registro interurbano de origen ha recibido suficiente información de dígitos para comenzar la conexión hacia la central terminal, su receptor de código envía la señal A6 en lugar de A1, lo cual significa la petición del número del abonado que llama (identidad de A). El registro emisor debe estar listo para recibir la señal de A6 en cualquier estado y cambiar para la transmisión del número que corresponde a la identidad de A. Cuando el registro emisor recibe A6, la transmisión del número del abonado B se suspende y se envía la categoría del abonado A en la forma de señal numérica 1 a 0 que corresponde a 10 categorías:
    1) Para llamadas desde operadora.
    2) Para llamadas desde abonado normal.
    3) Para abonado restringido
    4) Para abonado de alcancía.
    5) Para servicio interno.

Si el sistema local no tiene división en categorías, siempre se debe transmitir el dígito 2 para marcar un abonado normal. El receptor responde al dígito de categoría con la señal A1, que significa: transmisión del siguiente dígito (la primera vez=al primer dígito) del número A. El transmisor envía entonces el primer dígito del número A, con lo que el receptor contesta una vez más con A1 y así sucesivamente. Los dígitos se transmiten desde un registro de origen local y se reciben en un receptor de Código que puede pertenecer a otro registro. Las señales de control se transmiten desde el receptor de código hasta el registro de origen. La transmisión de dígitos esta doblemente controlada en un sistema que se conoce como de **secuencia obligada** que se explica a continuación:

1) Desde el registro de origen se transmite la señal numérica continuamente.
2) Cuando el receptor de código se reciben ambas frecuencias, se realiza la identificación del dígito y se regresa en forma continua de señal de control.
3) La señal de control se recibe en el registro de origen e interrumpe la transmisión de la señal numérica.
4) Cuando las dos frecuencias de avance desaparecen en el receptor de código, este interrumpe la transmisión de la señal de control.
5) Cuando la señal de control desaparece en el registro de origen, la nueva señal de numérica requerida por la señal de control se transmite

El principio de señalización a secuencia obligada se ilustra en la figura 56.

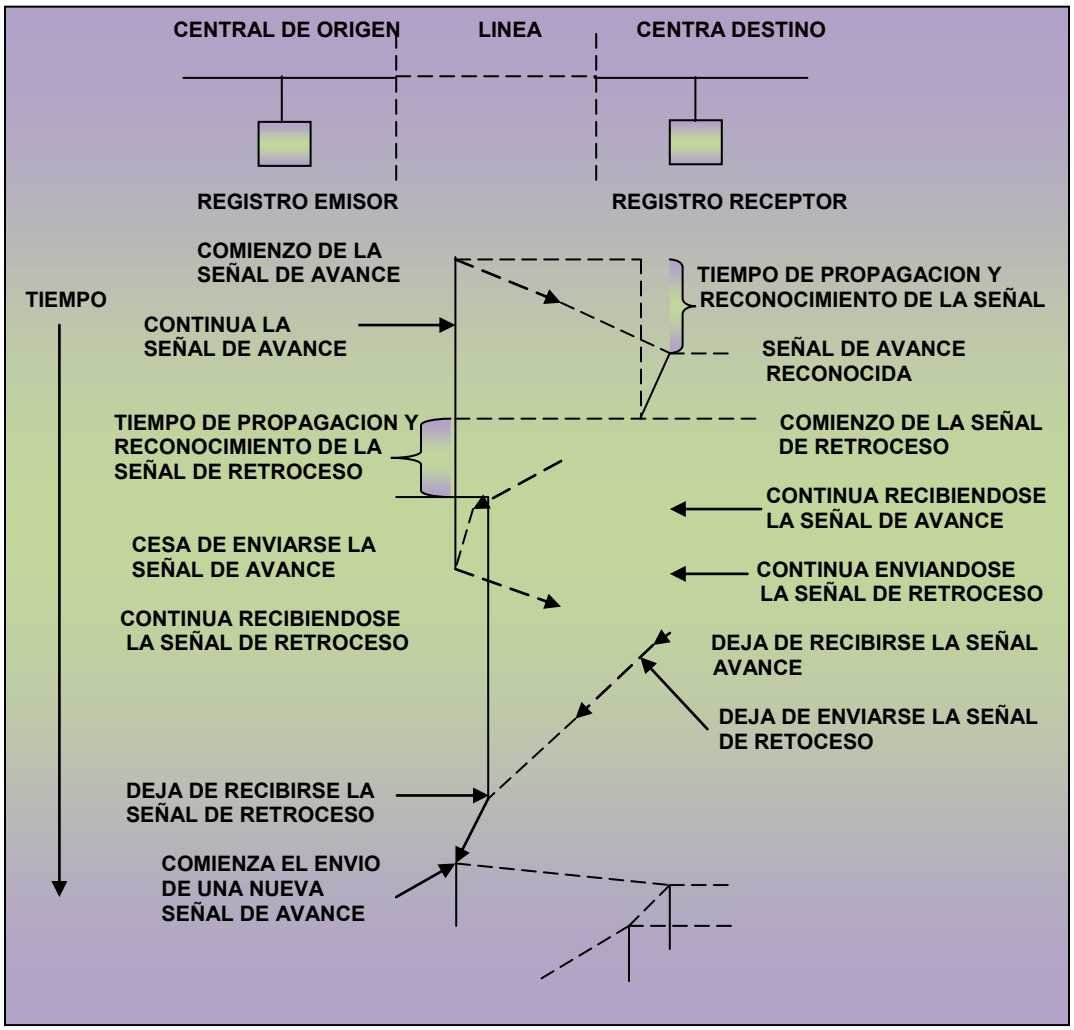


Figura 56

Cuando el último dígito del número A se ha transmitido, el receptor continúa enviando A1, la señal con la cual el transmisor contesta con código A15 indicando el final del número A. Entonces el receptor envía A1, con la cual continua la transmisión del número B en donde se interrumpió.

- **Señales de Fin de Selección**.-Como señales de fin de selección se emplea la señal de control A3 seguida por una las señales de control B1 a B6. La señalización de fin de selección generalmente se realiza en la forma normal controlada como sigue: cuando en la central terminal se recibe suficiente información de dígitos y la conexión se ha extendido a la línea llamada y verificado su estado, el receptor de código terminal envía la señal de A3 de regreso hacia el registro de origen, el cual responde con uno de los siguientes dígitos que indica la clase de servicio:
  1) Llamada de operadora.
  2) Llamada de abonado normal.
  3) 3 a 15 reserva.

  Al recibir el dígito de clase de llamada, el receptor de código terminal transmite las señales B apropiadas, en general una de las dos señales siguientes:

  B1: Abonado Libre.
  B2: Abonado Ocupado.

  A continuación tanto el registro de origen como el terminal se restauran y, si el abonado B se encuentra libre, la conexión entre el abonado que llama y el llamado se establece. Si el abonado B esta ocupado, en caso de una llamada normal, la conexión se libera en el punto más cercano al abonado A; mientras que la conexión se deja establecida con posibilidad de intervención, si la llamada se origina por operadora. Existen excepciones en la transmisión controlada de las señales de fin de selección. Supóngase, por ejemplo, que un registro de origen esta enviando registros hacia un registro interurbano para una llamada de Larga Distancia. El registro interurbano automáticamente continuará solicitando nuevos dígitos enviando señales A1 pues no sabe el número de dígitos necesarios en la central de destino. Cuando el registro de origen ya no tiene dígitos para enviar, debido a que el abonado a completado la marcación, la línea entre el registro de origen y el interurbano estará silencia, hasta el momento en que el registro interurbano envía señal A3, en este caso, la longitud específica es de $100ms - 150ms$, entonces la señalización se continua en la forma normal de secuencia obligada.

2.1.7 INTRODUCCION AL DIMENSIONAMIENTO DE CENTROS DE CONMUTACIÓN

Si se desea diseñar un sistema telefónico que funcione en forma óptima, es decir, con la máxima eficiencia y al mínimo costo, se deben estudiar suficientemente la cantidad del equipo que permitiese atender a una cantidad de llamadas igual al 10% del número total de abonados, sin importar el número de peticiones (intentos de llamada) que se rechazan por falta de equipo, debido a un tráfico mayor que el considerado y el costo del sistema. Lo que un suscriptor espera de un sistema telefónico cuando hace uso de él es que este se conecte inmediatamente, o casi inmediatamente, con la parte solicitada. Desea también que dicha conexión se realice al primer intento, este libre de fallas y permita una comunicación suficientemente inteligible. Por otro lado, a la administración telefónica le interesa manejar sistemas que operen en forma productiva; es decir, los costos de introducción e instalación, así como los de mantenimiento y operación deben ser lo más bajo posible. En la práctica, estos requisitos se satisfacen estructurando el sistema con un número limitado de trayectorias de conexión; El número preciso de ellos se puede fijar mediante la Teoría de Tráfico. La aplicación de los principios de esta teoría lleva al valor apropiado del número de trayectorias de conexión que permite, por un lado, diseñar sistemas de bajo costo y por otro sistema que puedan atender inmediatamente o casi todas las peticiones de servicio. Lo anterior significa que el diseño de un sistema de conmutación no sólo requiere la concepción física que satisfaga la función de conmutación, sino que también requiere su dimensionamiento que le permita funcionar en condiciones óptimas de costo y calidad de servicio, estos son algunos de los objetivo de la Teoría de Tráfico.

2.1.7.1 SISTEMAS DE PÉRDIDA Y SISTEMAS DE ESPERA

De acuerdo a como reaccionan los sistemas telefónicos ante el suscriptor que efectúa la llamada y encuentra el estado de congestión, estos se clasifican en sistemas de pérdida y en sistemas de espera (o de retraso). En los sistemas de pérdida, el abonado que no puede establecer su llamada por falta de trayectorias libres de conexión recibe un tono de ocupado que le obliga a colgar para posteriormente repetir su intento. Por otro lado, en los sistemas de espera sí un abonado trata de establecer una conexión cuando ya no existe trayectoria libre alguna, este no recibe tono de ocupado sino que se le permite esperar hasta que se desocupe una trayectoria; es decir, la solicitud de servicio se almacena. Casi todas las centrales privadas, las centrales de redes locales y los centros de conmutación de Larga Distancia, están constituidos como sistemas de pérdida. El principio de los sistemas de espera se aplica únicamente a ciertas partes del equipo que deben realizar funciones especiales durante el establecimiento de conexiones. La calidad de servicio de un sistema se mide en función de la magnitud de las pérdidas y el tiempo de los retrocesos. Por lo general, la calidad de servicio de un sistema es una cifra que se establece y la tarea que se debe resolver es diseñar un sistema que se apegue tanto como sea posible a los valores especificados, con un costo mínimo. Sin embargo, con frecuencia se necesita comparar dos sistemas de conmutación diseñados para la misma función. Desde el punto de vista técnico, es necesario comparar cual de los dos sistemas maneja más eficientemente el tráfico, es decir, cual de los dos sistemas tendrá las pérdidas más bajas o los retrocesos, para lo cual es necesario contar con métodos adecuados de cálculo, estos métodos de cálculo constituyen la Teoría de Tráfico. El tráfico telefónico se distingue principalmente por su carácter aleatorio, es decir, no se puede predecir cuando un abonado iniciará una llamada y cuando la terminará. Solamente se puede establecer, en base a observaciones prácticas, que tan probable es que un abonado específico inicie una llamada dentro de un intervalo de tiempo determinado y que tan probable es que termine dicha dentro de otro intervalo específico de tiempo. De aquí que sea importante para el estudio de la teoría de tráfico tener las nociones básicas de la teoría de probabilidad.

2.1.7.2 FORMULA DE BERNOULLI

Un dato importante para el dimensionamiento de sistemas es la probabilidad de que x abonados simultáneamente realicen llamadas. Si la probabilidad de que Q llamadas se realicen simultáneamente es pequeña, entonces no es necesario suministrar Q trayectorias de conexión sino menos de Q. Para generalizar sustituimos el número total de abonados por n y para el número de abonados que están simultáneamente ocupados x. La probabilidad de que x de un total de n abonados estén simultáneamente hablando es entonces:

$$p_x = \binom{n}{x} p^x (1-p)^{n-x} \quad (1)$$

Esta expresión para dicha probabilidad se conoce como fórmula de Bernoulli. Desde luego que la suma de todas las probabilidades debe ser igual a 1:

$$\sum_{x=0}^{n} p_x = \sum_{x=0}^{n} \binom{n}{x} p^x (1-p)^{n-x} = [p + (1-p)]^n = 1$$

La fórmula de Bernoulli establece la probabilidad con la cual ocurre un suceso de que x de un total de n abonados simultáneamente realicen llamadas. Como la probabilidad de ocupación p establece el tiempo promedio durante el cual un abonado se encuentra ocupado con respecto al tiempo de observación total, p es una medida de la magnitud del tráfico telefónico de este abonado específico. Con n abonados el producto np nos da la magnitud del tráfico total que

genera n abonados. A este producto se le conoce como **intensidad de tráfico telefónico** y. Su valor numérico indica cuantos abonados, en promedio, están simultáneamente ocupados en llamadas, o cuantas líneas, en promedio están ocupadas.

2.1.7.3 FORMULA DE POISSON

Vamos a introducir ahora la intensidad de tráfico $y = np$ en la fórmula de Bernoulli empleando $p = y/n$ y suponiendo que la intensidad de tráfico $y = np$ es constante. Si ahora n crece y p disminuye continuamente de forma tal que la ecuación $y = np = cons\tan te$; siempre se satisface, de la fórmula de Bernoulli mediante un proceso de límites, para $n \to \infty$ y para $p \to 0$ se obtiene:

$$p_x = e^{-y}\frac{y^x}{x!} \to (2)$$

que es la fórmula de Poisson. En consecuencia, la fórmula de Poisson permite calcular la probabilidad de p_x con la cual x abonados estarán hablando, simultáneamente conocida como intensidad de tráfico y. Esto, desde luego bajo la suposición de que el número de abonados que producen la intensidad de tráfico y es muy grande y que la probabilidad de ocupación p del abonado individual es infinitamente pequeña. Esta suposición es suficientemente correcta en muchos casos de tráfico telefónico.

2.1.7.4 CANTIDADES Y UNIDADES DE LA TEORIA DE TRÁFICO

El danés A. K. Erlang (1878-1929), fue el primero en abordar el estudio del tráfico telefónico en base al cálculo de probabilidad estableciendo con esto lo que conoce como la teoría de tráfico. Como se ha visto, la intensidad de tráfico y es la medida de la magnitud del tráfico; es un valor promedio alrededor del cual varía el tráfico real. Su valor numérico indica el número promedio de llamadas que existen durante el período de observación. En forma estricta, la intensidad de tráfico es una cantidad adimensional, pero se le ha asignado la unidad erlang (erl), en memoria del fundador de la teoría. La media de ocupación de una línea (o de un dispositivo) $\alpha = y/n$ erl es la aportación de una línea en la intensidad total del tráfico. Su valor numérico representa la probabilidad de ocupación de la línea y nunca puede ser mayor de la unidad. Frecuentemente se le expresa en términos de porcentaje. Llamando T al tiempo de observación, C al número total de ocupaciones que ocurren durante el tiempo de observación y t_m al tiempo promedio de duración de estas ocupaciones (media o promedio de ocupación), la intensidad de tráfico se puede calcular a partir de estas cantidades expresándola como función del tiempo de observación con la siguiente expresión:

$$y = Ct_m \to (3)$$

Si t_m no se mide en términos de fracciones del tiempo de observación sino en términos de horas, lo cual es práctica normal, es necesario dividir entre el tiempo T de observación expresado en horas para obtener y en erl, es decir:

$$y = \frac{Ct_m}{T}\, erl \to (4)$$

El tiempo T de observación se puede fijar en forma arbitraria. La intensidad de tráfico y es entonces un valor promedio para todo el tiempo T de observación. La **hora de máximo de tráfico** es el período continuo de una hora en la que se registra el mayor número de comunicaciones en

un sistema. Si se cuentan las ocupaciones que ocurren en una hora y su número denotado por c, la intensidad de tráfico en erl esta dado por:

$$y = ct_m \rightarrow (5)$$

siempre que t_m se exprese en hrs. Como se deduce de la fórmula (5), determinada la intensidad de tráfico se puede lograr con un número grande c de ocupaciones con tiempo promedio de ocupación t_m corto, o con unas cuantas ocupaciones, pero con tiempo promedio muy grande. Se conoce como volumen de tráfico Y el producto del número C de todas las ocupaciones que ocurren durante el período T de observación por tiempo promedio de ocupación t_m; se mide en erlangs hora $\left(erlh\right)$:

$$Y = Ct_m \; earl\, h \rightarrow (6)$$

También es posible calcular el volumen de tráfico Y a partir de los t_m individuales de todas las ocupaciones C. Se obtiene:

$$Y = t_1 + t_2 + t_3 + \cdots + t_c = \sum_{v=1}^{\sigma} t_v \rightarrow (7)$$

es decir, es simplemente la suma de todos los tiempos de ocupación durante el período de observación.

A continuación establecemos la diferencia que existe entre el tiempo promedio de ocupación y el tiempo promedio de conversación. El tiempo de conversación es parte del tiempo que emplean las llamadas que se completan, es decir, comienza a computarse desde el momento en que la conexión se ha establecido; es prácticamente el tiempo por el cual el abonado paga. Por otro lado, el tiempo promedio de ocupación, es el tiempo total durante el cual una línea o una trayectoria de conexión se ocupa, incluyendo el tiempo que se emplea para que la conexión se establezca. Es decir, que el tiempo de ocupación de una línea relacionado con una llamada que se completa es mayor que el tiempo de conversación. Sin embargo, como el tiempo promedio de ocupación también incluye las ocupaciones cortas que ocurren con intentos de llamada que no se completan, este tiempo llega a ser, en la mayoría de los casos, más corto que el tiempo promedio de conversación.

2.1.7.5 GENERACION DE TRÁFICO

La intensidad de tráfico que se alimenta al sistema, se conoce como tráfico ofrecido A (en erlangs). La porción del tráfico ofrecido que el equipo de conmutación acepta es **el tráfico cursado** y (en erlangs) y la porción del tráfico que no pasa a través del sistema sino que se desvía (debido, por ejemplo, a un número insuficiente de troncales de servicio) es el **tráfico de desborde** o **tráfico residual** cuya densidad la denotaremos por D (en erlangs). Por lo tanto, la suma del tráfico cursado y (carga cursada) y el tráfico de desborde D es igual al tráfico ofrecido (carga ofrecida):

$$A = y + D \rightarrow (8)$$

Si denotamos por O el número de llamadas que se ofrecen durante todo el período de observación T, por E las llamadas que se completan y por P las llamadas que se repiten, el tráfico ofrecido es:

$$A = \frac{Ot_m}{T} erl \rightarrow (9)$$

el tráfico cursado.

$$y = \frac{Et_m}{T} erl \rightarrow (10)$$

y la intensidad de tráfico residual o de desborde que también se puede llamar intensidad de tráfico perdido es:

$$\frac{Ot_m}{T} = \frac{Et_m}{T} + \frac{Pt_m}{T} \therefore$$

$$O = E + P \rightarrow (11)$$

Es decir, **llamadas ofrecidas** es igual a llamadas completas más llamadas pérdidas. Ahora, el número de llamadas pérdidas P se puede referir al número de llamadas ofrecidas O o al número de llamadas cursadas E. Esto resulta de dos valores diferentes de pérdida B y V los cuales para el caso de pérdidas pequeñas, casi son iguales:

$$B = \frac{P}{O} \rightarrow (12)$$

$$V = \frac{P}{E} \rightarrow (13)$$

La perdida B que se refiere al tráfico ofrecido, (sólo esta pérdida) es igual a la **probabilidad de pérdida** pues en este caso el número de llamadas que se rechazan (número de casos favorables por lo que se refiere a la pérdida), se divide entre el número total de llamadas ofrecidas (número de casos posibles). El cálculo de V se realiza fácilmente si se conoce B y viceversa:

$$V = \frac{B}{1-B} \rightarrow (14)$$

$$B = \frac{V}{1-V} \rightarrow (15)$$

Generalmente, las pérdidas se expresan en términos de porcentaje. Las fórmulas de conversión toman entonces las siguientes formas:

$$V = \frac{100B}{100-B}$$

$$B = \frac{100V}{100-V}$$

y el tráfico cursado y es:

$$y = A(1-B) \rightarrow (16)$$

2.1.7.6 HORA DE MÁXIMO TRÁFICO

La capacidad de tráfico es igual a la máxima carga que el sistema puede cursar con una pérdida específica. Es decir, cuando ocurre esta carga máxima, la pérdida no debe exceder el valor especificado. Existe una íntima relación entre el tráfico cursado y y la capacidad de tráfico de un equipo de conmutación o de un grupo trocal. Sin embargo, el usuario de un sistema telefónico desea que, aún durante los períodos de máximo tráfico su comunicación pueda establecerse. Es necesario considerar entonces, dentro de un período de 24 horas, el período en el que ocurre el máximo tráfico. Así, se conoce como **hora ocupada u hora de máximo tráfico** el período de 60 minutos durante el día, en el cual se registra el valor más alto del tráfico. El tráfico telefónico es una cantidad que se caracteriza por sus variaciones en función del ritmo de actividad de la sociedad. Sus variaciones pueden ser diarias, presentando máximos de tráfico una, dos o tres veces al día durante días hábiles normales. Esto se ilustra en la figura 57. Las variaciones también pueden ser durante la semana, figura 58, el tráfico disminuye normalmente durante los sábados y domingos. El tráfico telefónico también tiene variaciones de temporada, durante ciertas épocas del año existe tráfico intenso y durante otras épocas el tráfico baja.

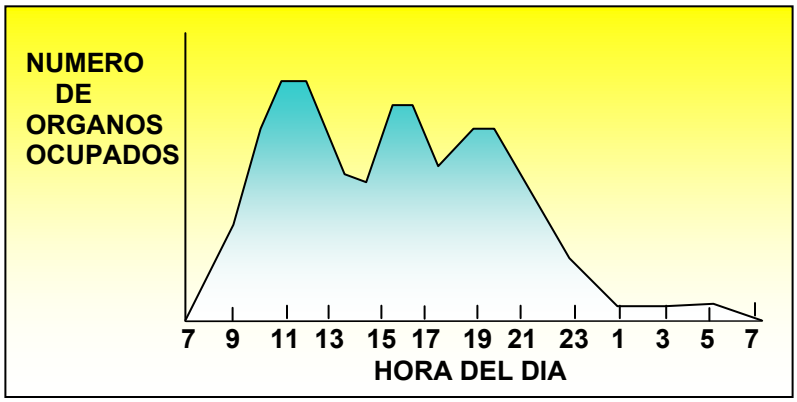


Figura 57

Frecuentemente se registra tráfico intenso antes de los días festivos principales, por ejemplo Navidad, Año Nuevo y Semana Santa; después de estas fechas el tráfico baja.

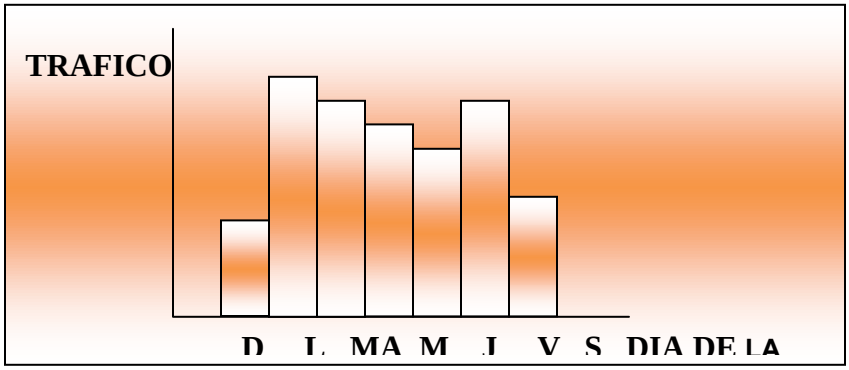


Figura 58

Un concepto muy ligado con el de hora cargada (también hora pico) es el **de factor de concentración** K (relación de hora pico al día). Indica la porción de tráfico diario total que se maneja en la hora pico. Para calcular el valor de concentración K, a partir de las mediciones en diferentes días, se obtiene el valor medio del cociente que resulta de dividir el volumen de tráfico en la hora pico entre el volumen total de tráfico del día respectivo. Este valor es aproximadamente $K = 1/8$.

2.1.7.7 FORMULA DE ERLANG

La fórmula de Erlang se utiliza para calcular la pérdida o probabilidad de bloqueo en sistemas de pérdida. Pueden definirse dos casos de aplicación de la fórmula de Erlang, primero para el cálculo de la pérdida en el caso de grupos troncales de accesibilidad completa y segundo para el cálculo de la pérdida en el caso de grupos troncales de accesibilidad limitada.

2.1.7.7.1 GRUPOS DE TRONCALES DE ACCESIBILIDAD COMPLETA

Un ejemplo sencillo es el siguiente; supóngase que las troncales fuente alcanza las troncales de servicio sobre el equipo de conmutación constituido por un grupo de troncales como grupo troncal de accesibilidad completa. Como se recordará, esto significa que independientemente del estado de ocupación de las troncales, cualquier trocal fuente libre puede conectarse con una troncal de servicio en tanto exista cuando menos una troncal de servicio libre. Supongamos ahora que a este grupo troncal de servicio se le ofrece, sobre el equipo de conmutación, tráfico puramente al azar

ocasionado por un número infinito de fuentes que llega sobre un número infinito de troncales fuente. Sabemos que, para este tipo de tráfico, la fórmula de Poisson permite calcular la probabilidad de que x troncales fuente estén ocupadas simultáneamente. Así, si la intensidad de tráfico ofrecido se denota por A entonces:

$$p_x = e^{-A}\frac{A^x}{x!} \rightarrow (7)$$

Si ahora el número de troncales de servicio se limita a N, aparecerá pérdida siempre que las N troncales de servicio y por lo tanto también N troncales fuente, estén ocupada, pues bajo estas indicaciones se rechazará cualquier intento adicional de llamada. Se ingiere entonces que es posible determinar, mediante la fórmula de Poisson, la probabilidad de pérdida B. Calculando que tan probable es que en el grupo infinitamente grande de troncales fuente este simultáneamente ocupadas N o más de N troncales. Esta probabilidad B esta dada por:

$$B = \sum_{v=n}^{\infty} e^{-A}\frac{A^v}{v!} \rightarrow (8)$$

Esta fórmula que fue propuesta por Molina lleva necesariamente a la interpretación de que llamada que encuentra condición de bloqueo (las N troncales de servicio ocupadas) permanecerá en la troncal fuente hasta que se libere una troncal de servicio, siendo hasta entonces que se acepta con el resto del tiempo de duración contribuyendo, en consecuencia a la carga del sistema (llamadas pérdidas mantenidas). Sin embargo, este hecho no acuerda con la realidad en los sistemas de pérdida en donde una llamada que se rechaza desaparece inmediatamente del sistema llamada **pérdidas eliminadas**. La fórmula de Erlang para sistema de pérdida considera este hecho:

$$E_x = \frac{\frac{A^x}{x!}}{1 + A + \frac{A^2}{2!} + \cdots + \frac{A^N}{N!}} \rightarrow (9)$$

en donde: $(x = 0,1,2\ldots,N)$

Si $N \rightarrow \infty$, la fórmula de Erlang se convierte en la fórmula de Poisson, pues en este caso:

$$1 + A + \frac{A^2}{2!} + \cdots = e^A$$

E_x es la probabilidad de x de N troncales estén simultáneamente ocupadas.

De nuevo las llamadas adicionales se rechazan sólo si las N troncales de servicio están ocupadas. Por lo tanto, haciendo $x = N$ en la ecuación (19), se obtiene la probabilidad de pérdida B:

$$B = E_{x=N} = \frac{\frac{A^N}{N!}}{1 + A + \frac{A^2}{2!} + \cdots + \frac{A^N}{N!}} \rightarrow (20)$$

La ecuación (20) se conoce como la fórmula de pérdida de Erlang. Evidentemente, si lo que se especifica es la pérdida, la fórmula permite calcular el tráfico ofrecido permisible (carga ofrecida) y por lo tanto la capacidad de tráfico del sistema. O bien, si lo que se conoce es el tráfico ofrecido, permite calcular el número de troncales de servicio que se necesita para mantener la pérdida especificada.

2.1.7.7.2 GRUPOS TRONCALES DE ACCESIBILIDAD LIMITADA

La fórmula que permite calcular la pérdida en caso de grupos troncales de accesibilidad limitada se conoce como la **fórmula de interconexión de Erlang**. Es válida sólo si se satisfacen las siguientes condiciones: el grupo trocal de servicio debe formar una graduación ideal; esto significa que el grupo troncal de servicio debe quedar accesible a través de un arreglo de conmutación de una sola etapa a los subgrupos fuente con disponibilidad K uniforme, constante y el tráfico debe llagar cuando menos $\binom{N}{K}$ subgrupos fuente, es decir, a través de tantos como posibilidades existan de seleccionar K troncales diferentes de un total de N. En este caso es posible alambrar las troncales de servicio, de tal manera que cada combinación K de N **troncales de servicio** se conecte cuando menos un subgrupo fuente. Si estas condiciones se satisfacen y si cada subgrupo fuente ofrece al grupo troncal de servicio la misma cantidad de tráfico, entonces es posible desarrollar para este arreglo de conmutación de una sola etapa la fórmula para obtener la probabilidad de pérdida B, promediada sobre todos los subgrupos fuente.

Supongamos que una llamada llega procedente de un subgrupo fuente cuando ya existan q ocupaciones en el arreglo considerado como un todo. Esta llamada se perderá si el subgrupo fuente considerado tiene acceso solamente a troncales ocupadas. La probabilidad Z_q de que esto suceda es:

$$Z_q = \frac{\binom{q}{k}}{\binom{N}{K}} \rightarrow (21)$$

Si la probabilidad de que existan q ocupaciones es P_q una llamada se perderá con la probabilidad:

$$B_q = Z_q P_q \rightarrow (22)$$

Para todos los posibles estados de ocupación $q = 0,\ldots,N$, la probabilidad de pérdida es:

$$B(A,N,K) = \sum_{q=0}^{N} Z_q P_q \rightarrow (23)$$

Las probabilidades P_q se pueden obtener en la forma de las soluciones de un sistema de ecuaciones lineales. Insertándolas en la ecuación (23), se obtiene la fórmula de interconexión de Erlang:

$$B(A,N,K) = \frac{\sum_{q=0}^{N} Z_q M_q \frac{A_q}{q!}}{\sum_{q=0}^{N} M_q \frac{A_q}{q!}} \rightarrow (24)$$

M_q es una abreviación cuyos valores se deben calcular de la ecuación:

$$M_{q+1} = (-Z_q) M_q \rightarrow (25)$$

en donde $M_0 = 1$.

Para $K = N$, la fórmula de interconexión de Erlang se convierte, por supuesto, en la fórmula de Erlang para grupos troncales de servicio de accesibilidad completa. Para otros arreglos que no están graduados en forma ideal, la pérdida también se puede calcular exactamente, pero el cálculo

es tan grande que sólo se puede realizar para arreglos pequeños. Para arreglos más grandes, se necesitaría resolver más de 10^{10} ecuaciones lineales. Por esta razón, la pérdida se obtiene de tablas cuyos valores se han calculado con métodos de aproximación.

2.1.7.8.-REDES DE CONMUTACION DE VARIAS ETAPAS

La fórmula de Erlang para grupos de accesibilidad completa se puede utilizar para calcular la pérdida en una red de conmutación de varias etapas, si esta red forma un grupo de accesibilidad completa. Sin embargo, en general las redes de conmutación de varias etapas forman grupos de accesibilidad limitada. De todas formas, si se llega a las troncales de servicio como grupo troncal de accesibilidad completa cuando la red esta bajo la condición de no carga, debido a la congestión interna del sistema de enlace, el grupo troncal se convierte en grupo de accesibilidad limitada cuando la red esta cargada. Para este tipo de arreglos, el cálculo exacto de la pérdida es sumamente difícil y en la mayoría de los casos, imposible. La accesibilidad (disponibilidad) de un arreglo de varias etapas, es decir, el número de troncales de servicio a las que se tiene acceso sobre los eslabones, cambia de un instante a otro; depende de las condiciones que ya existen, o sea, de cuantos y cuales eslabones se encuentran ocupados en el momento respectivo. Sin embargo, se pueden encontrar arreglos de una sola etapa y accesibilidad fija (aunque desconocida al principio) cuya pérdida se puede determinar equivalente a los arreglos de varias etapas de accesibilidad variable.

La disponibilidad de un arreglo equivalente se elige de modo que la equivalencia se realice desde el punto de vista de la teoría de tráfico, es decir, a determinados tráficos ofrecidos el arreglo equivalente debe producir la misma pérdida. En consecuencia, es posible determinar las pérdidas con ayuda del arreglo equivalente más simple. La accesibilidad fija del arreglo equivalente es aproximadamente igual al valor promedio de la accesibilidad variable del arreglo de varias etapas y se conoce como **accesibilidad equivalente o efectiva** K. Esta cantidad se determina del arreglo de varias etapas mediante un método de aproximación o mediante pruebas de pérdidas que se realizan con una computadora digital. Para esto basta emplear un sólo valor de tráfico ofrecido pues la accesibilidad efectiva es en gran medida independiente de la magnitud del tráfico ofrecido. En esta forma, con el valor K_{ef} y el número N de troncales de servicio, se puede obtener la pérdida del arreglo equivalente de una etapa y consecuentemente también la del arreglo de varias etapas, para cualquier valor de tráfico ofrecido tomado de las tablas concernientes al arreglo de una sola etapa que se escogió. Si el arreglo equivalente se escoge específicamente de modo que este graduado en forma ideal, su pérdida se puede calcular exactamente mediante la fórmula de interconexión. Aunque esta fórmula tiene una forma cerrada comparativamente simple, su evaluación es complicada. Por esta razón, mediante un sistema de procesamiento de datos se han calculado y tabulado un gran número de valores para arreglos graduados en forma ideal. Así, con estas tablas, de tres cantidades que se conocen se puede determinar con facilidad la cuarta. Por ejemplo, para ciertos valores de $B, N\ y\ K = K_{ef}$ se obtiene el valor permisible del tráfico ofrecido A.

En esta forma, con el amplio dominio de la teoría de tráfico se han podido resolver sólo unas cuantas tareas que, aunque importantes son comparativamente simples. Incluso se establecieron algunas restricciones de simplificación. Se supuso, por ejemplo, tráfico puramente al azar, es decir, que el tráfico es independiente del número de troncales ya ocupadas. Sin embargo, esta suposición no es completamente cierta en la práctica, pues no toma en cuenta a los abonados impacientes que al recibir el tono de ocupado cuelgan y realizan con frecuencia repetidos intentos de llamada. Por otro lado, el tráfico puramente al azar se puede originar bajo condiciones prácticas solamente si el número de troncales fuente es considerablemente mayor al número de troncales de servicio. Si este es el caso, el número de troncales fuente aún libres siempre es considerablemente mayor que el número de troncales fuente ocupadas, pues solamente puede haber tantas troncales fuente ocupadas como troncales de servicio ocupadas. El hecho de que las comparativamente pocas troncales fuente ocupadas ya no puedan ofrecer más llamadas, prácticamente no tienen

efecto en el carácter puramente aleatorio, del tráfico ofrecido. Sin embargo, en la práctica real también se tienen interés en los arreglos, en los que el grupo troncal fuente es ligeramente mayor que el grupo troncal de servicio. En muchos casos, el tráfico que ya no se puede manejar se hace fluir hacia otra unidad del equipo de conmutación, permitiéndose las pérdidas sólo cuando este equipo también queda incapacitado para manejar el tráfico.

2.1.7.9.-CARTACTERISTICAS DE LOS SISTEMAS DE RETARDO

En los sistemas de espera no es suficiente establecer un sólo parámetro como lo es la pérdida en el caso en los sistemas de pérdida. Generalmente se establecen tres parámetros:

- **La probabilidad de retardo** $p(¨> 0)$.-Indica que tan probable es que la llamada que se ofrece tenga que esperar debido a que todas las trayectorias de conexión disponibles ya están ocupadas. Su magnitud es igual al cociente (promedio sobre el período de observación) del número de llamadas que esperan entre el número total de llamadas que ofrecen.
- **El retardo promedio** t_w **de llamadas retardadas**.-Indica en promedio, el tiempo que debe esperar una llamada que espera. Otro parámetro que se establece frecuentemente es el tiempo medio de espera h (retardo promedio) referido a todas las llamadas que se ofrecen. Esto significa que al observar el valor promedio, el retardo 0 de todas las llamadas no retardadas también esta incluido. El valor de h se obtiene de:

$$h = t_w P(> 0)$$

- **La probabilidad** $P(> t)$ **de que se exceda un cierto retardo** t .-Indica que tan probable es que una llamada que se ofrece tenga que esperar más tiempo que el especificado t hasta que se atiende. Su magnitud es el cociente (promediado en el período de observación) del número de llamadas que esperan más de un tiempo específico dividido entre el número total de llamadas que se ofrecen.

2.1.8.-SERVICIOS OFRECIDOS POR LA RED TELEFÓNICA BASICA

El servicio ofrecido por RTB (Red Telefónica Básica), que facilita la comunicación vocal por medio un aparato telefónico con otro distante. Pero el servicio telefónico como otros, ha experimentado una considerable evolución. Del aparato básico al avanzado; de las facilidades básicas, a la inteligencia de la red. De igual manera, en torno a la RTB y al servicio telefónico han ido surgiendo otra serie de servicios que enriquecen y amplían las facilidades ofrecidas por este. Así, podemos citar las siguientes categorías:

- Telefonía Básica.
- Telefonía Pública.
- Servicios OXY.
- Servicios Suplementarios.
- Servicios CLASS.
- Servicios de Teleconferencia.

2.1.8.1.-TELEFONIA BASICA

Se entiende por **servicio telefónico básico** aquel que permite al usuario, por medio de un aparato telefónico adecuado, establecer y recibir todo tipo de llamadas telefónicas por conmutación: metropolitanas, provinciales, nacionales, internacionales, hacia servicios especiales diversos y otros de operadoras de atención locales y distantes, así como acceder a servicios de inteligencia de red, utilizar los servicios suplementarios y otros. Por **línea telefónica principal** se entiende aquella a la que corresponde un determinado número telefónico dependiente de la central telefónica a la que este se encuentre adscrito. En cuanto a la modalidad de instalación o del servicio a prestar, las líneas telefónicas tienen la consideración de:

- Líneas individuales (particulares, no particulares y de teléfonos públicos de servicio).

- Líneas de enlace.
- Líneas diversas (de alimentación y de corriente de llamada).
- Líneas de zonas de extrarradio.

La red telefónica ha experimentado una notable modernización durante los últimos años. Se procede a la sustitución de equipo analógico por digital en todos los elementos que intervienen en el proceso de la comunicación. Pero no sólo eso, sino que incluso la tradicional configuración jerárquica de la red telefónica tomará una estructura de red flexible, en la que las centrales de conmutación gozarán de una elevada autonomía e inteligencia. Esta nueva capacidad permitirá optimizar el tratamiento de cada llamada, depurando los recursos de la red y facilitando a las centrales para una respuesta inmediata en los estados iniciales de aquella, cuando sea precisa dicha actuación. Este nuevo modelo de red hace necesario el concepto tradicional de jerarquía y niveles de la anterior estructura analógica de red. Las centrales de conmutación se constituyen en unidades remotas, centrales autónomas y centrales nodales. Con dos áreas de red definidas: local y de tránsito. Las centrales nodales se interconectan entre sí, y las autónomas lo hacen con las nodales por las vías o los caminos que sean precisos. Naturalmente, no es posible concebir el servicio telefónico sin el aparato telefónico. Existen infinidad de ellos, de todas las marcas y modelos, al cual más ingenioso y con mayores prestaciones.

2.1.8.1.1 NUMEROS DE SERVICIO

- 020.-Larga Distancia Nacional Vía Operadora.
- 030.-Hora Exacta.
- 031.-Despertador.
- 040.-Asistencia de Directorio Nacional:
    - Números Locales.
    - Cambios de Números.
    - Números Telefónicos de Poblaciones del Interior de la Republica Mexicana.
    - Horario de Atención las 24 horas.

  Por medio del servicio Asistencia a Directorio, se puede solicitar información de un número de la misma localidad u otro distinto de la Republica Mexicana y la operadora buscará la información, para que un sistema de voz le proporcione el número. Además de obtener el número buscado, se da la opción de comunicarse sin que tenga que marcar.
- 050.-Atención a Clientes sobre Reparación de Líneas Telefónicas y Cambios de Aparatos.
- 060.-Policía del DF.
- 065.-Cruz Roja.
- 068.-Bomberos.
- 080.-Emergencias y Auxilio: Policía, Ambulancias y Bomberos.
- 090.-Larga distancia Internacional Vía Operadora.

2.1.8.2 TELEFONIA PÚBLICA

El servicio de telefonía pública es el servicio de telefonía básica ofrecido al usuario por medio de teléfonos de uso público.

- **Teléfonos de Uso Público**.-Permiten el acceso al servicio telefónico metropolitano, provincial, nacional e internacional sin ningún tipo de limitación o restricción. Se encuentran situados en lugares de concurrencia pública e instalados sobre muebles y soportes adecuados como cabinas, semicabinas, columnas, etc. Los hay en las siguientes modalidades:
    - **Locutorios**.-Son recintos de libre acceso desde los que es posible realizar todo tipo de llamadas telefónicas. Se hallan dotados de un número variable de cabinas, equipadas cada una de ellas con un teléfono y un contador visible. Estas instalaciones ofrecen atención personalizada y en ellas se puede realizar el pago de las comunicaciones bien con monedas o con tarjeta de crédito.

- **Teléfonos de Cobro Automático de Titularidad Ajena**.-Teléfonos instalados en establecimientos de concurrencia pública, cuyos titulares contratan el servicio para ofrecérselo a sus clientes.
- **Teléfonos de Cobro Manual de Titularidad Ajena**.-Cumplen igual cometido que los anteriores, pero el cobro lo realiza el titular de forma manual, en razón de los impulsos de tarificación registrados en el contador del que van previstos.

- **Teléfono Protegido de Monedas**.-Teléfono destinado a recintos abiertos o cerrados, que acogen un gran número de personas o necesitan servicio las 24 horas del día. Consta de una carcasa de acero cementado y templado; pintura vitrificada resistente al rayado; teclado de hacer, incorporado a la placa superior; ranura única de entrada de monedas, con botón desatascador, visor de saldo disponible, etc. Se conecta directamente a la red telefónica, no necesitando de alimentación eléctrica complementaria.
- **Teléfono Regular de Monedas Autónomo**.-Teléfono para interiores, una sola línea telefónica y un único equipo terminal. Ideal para titulares de establecimientos que precisan satisfacer sus propias necesidades en comunicación, además de ofrecer un servicio a sus clientes de forma autónoma. Este teléfono es, por naturaleza, de titularidad privada y de utilización pública. Incorpora ranura de monedas con detector electrónico; cordón extensible; visor numérico digital para indicación de hora, tarifa, número marcado, saldo disponible o valor de la llamada. Permite el cambio de marcación decimal a multifrecuencia, etc.

2.1.8.3 LINEA MULTISERVICIO

Es la línea telefónica básica capacitada para soportar servicios adicionales al telefónico, que permite una mayor diversidad de facilidades y usos de este. Haciéndolo más cómodo y eficaz. Gama de servicios por línea individual:

- Consulta y conferencia a tres.
- Desvío de llamadas
  - Desvío inmediato.
  - Desvío por ausencia.
  - Desvío si esta ocupado.
  - Desvío distante.
  - Desvío por baja y/o cambio de domicilio.
- Indicación de llamada en espera.
- Línea directa sin marcación.
- Información de cambio de número.
- Llamada intercomunicada.
- Línea de salto.
- Telecomputo.

2.1.8.4 SERVICIOS SUPLEMENTARIOS SELECTIVOS (CLASS)

La palabra CLASS responde a las iniciales de Custom Local Area Signalling Servicer, denominación registrada por Bellcore (compañía USA dedicada a actividades de investigación y desarrollo en las operadoras locales de USA). No obstante, el ETSI europeo específica servicios similares. Los servicios CLASS se definen en razón de la capacidad de disponer de la identidad de la línea llamante en la central destino de llamada, y a la posibilidad de trasmitir dicha identidad a la terminal telefónica especial del abonado llamado, a través su bucle analógico.

- **Transporte de la Identidad Llamante por el Bucle Analógico**.-Para que la identidad del número llamante pueda ser transportado desde la central digital de destino hasta una terminal analógica avanzada, por el bucle del abonado. Bellcore ha especificado una señalización de abonado del tipo FSK (Frecuency Shift Keying, modulación en frecuencia 1,200/2,200Hz), que transmite dicha identidad llamante entre el primer y segundo impulso de corriente de llamada. Por lo tanto, en cada extremo del bucle del abonado, es necesario modular y demodular conforme tales características de señalización. El

mecanismo previsto por Bellcore para transportar el número llamante no es único, evidentemente, y de hecho existen otras iniciativas basadas en utilizar la señalización DTMF (Dual Tone Meltifrecuency), que requieren incluir emisores DTMF en las centrales, así como receptores DTMF en los teléfonos. También la señalización en el bucle puede ser mixta:

- Señalización FSK en el sentido red-usuario, para el envío del número llamante.
- Señalización DTMF en el sentido usuario-red, para procedimientos operativos.

En cualquier caso, el número llamante sólo será presentado en la terminal analógica de destino si la red es capaz de transportarlo previamente desde la central de origen de la llamada hasta la de destino, por lo que el ámbito geográfico donde sea posible la prestación de los servicios CLASS se circunscribe a ciertas áreas locales hasta la total modernización y digitalización de la red. No obstante lo anterior, las grandes áreas urbanas, y mayoritariamente la red de tránsito disponen de infraestructura de señalización digital por canal común PUT (en otro caso PUSI) bastante extendida, las comunicaciones entre centrales digitales transportarán el CLI (Calling Line Identification, identificación de la línea llamante).

- **Utilidades Proporcionadas por los Servicios CLASS**
  - Llamada Completada sobre Abonado Ocupado (Automatic Callback).-Con esta facilidad, si al efectuar una llamada se encuentra ocupada la línea de destino, se puede ordenar desde el teléfono analógico la realización periódica de llamadas hasta que la línea llamada quede libre, momento en el cual, se avisará a los abonados llamante y llamado.
  - Rellamada Automática (Automatic Recall).-Si en una llamada entrante, durante la conversación o terminada esta, se reponen los órganos de conexión, es posible volver a conversar con la misma persona llamante sin necesidad de conocer previamente su número, ya que el teléfono analógico memoriza automáticamente el número llamante de la última llamada recibida.
  - Presentación del Número Llamante (Calling Number Delivery).-La posibilidad de transmitir a un teléfono la identidad del número llamante resulta factible mediante procedimientos de señalización. El resto de servicios CLASS gira en torno a la capacidad de presentación de la mencionada identidad llamante, por lo que tal facilidad es esencial.
  - Restricción de Presentación del Número Llamante (Calling Number Delivery Backing).-Permite al abonado CLASS, desde su terminal indicar a la central de activación de dicho servicio para que, en llamadas salientes, se ordene la omisión al destino (abonado llamado) de su número de red (SSN 7 en la red). El cliente puede solicitar a su central la activación del servicio bajo alguna de las dos siguientes modalidades:
    1) Restricción de la presentación del número llamante para todas las llamadas.
    2) Restricción de la presentación del número llamante llamada a llamada (sólo se presenta en las llamadas realizadas a los números de red contenidos en una lista creada por el usuario).
  - Edición de Lista de Números (Screening List editimg).-La disposición de este servicio capacita al abonado para crear y modificar listas de números en la central a la que se encuentre conectado, para comprobar las identidades llamantes, en orden a seleccionar las llamadas entrantes y darles un tratamiento especial de acuerdo a sus deseos. Por marcación de un código o presionando una tecla previamente programada en el teléfono, el usuario puede activar, desactivar, añadir o borrar números y comprobar el estado de un determinado número seleccionado. Las instrucciones y verificación de acciones de los usuarios son llevadas a cabo en la central que proporciona las locuciones necesarias para ello. Bajo la denominación de este servicio, bajo la presentación del número llamante hacen atractivos los servicios CLASS, se presentan las siguientes facilidades que reciben también tratamiento de servicios individualizados:

1) Aceptación Selectiva de Llamadas (Selective Call Adcceptance).-El abonado puede dar indicación a la central desde su terminal para que esta le entregue únicamente aquellas llamadas entrantes cuyo CLI se encuentra en una lista programada por él. El resto de llamadas entrantes serán encaminadas hacia la locución apropiada o número alternativo de red, dependiendo de la selección efectuada por el abonado en tiempo de activación.
2) Rechazo Selectivo de Llamadas (Selective Call Rejection).-Permite al abonado rechazar las llamadas originadas en ciertos números y redireccionarlas a locuciones apropiadas. Las llamadas cuyo CLI no se encuentre registrado por el abonado en la lista de rechazo, recibirán un tratamiento normal en el destino. Un aspecto de esta facilidad es que permite rechazar selectivamente la última llamada recibida, sin necesidad de que previamente se reciba en la terminal la identidad de la línea llamante, añadiendo a la lista de numeraciones a rechazar (screening list editing) el último número llamante registrado en la central.
3) Desvío Selectivo de Llamadas (Selective Call Forwanding).-El abonado puede asegurar que una llamada este registrada en una lista de abonados importantes (screening list edition), sea atendido por la persona adecuada. Para ello y haciendo uso de este servicio, reencamina tales llamadas a otra posición. En el caso de que la identidad del abonado llamante no pueda ser obtenida o se encuentre en la lista anterior, será aplicado el tratamiento regular de terminación de la llamada.
4) Corriente de Llamada Personalizada (Distintive Ringing).-Permite al abonado preseleccionar a que llamadas se proporcionará un tratamiento distintivo de corriente de llamada, en razón de la identidad del abonado llamante. El registro de tales llamadas se realiza bajo el gobierno de la lista del screening list editimg.
5) Llamada en Espera Selectiva (Selective Call Waiting).-Consiste en dar dirección al abonado llamado de que una llamada entrante quiere completar sobre su línea ocupada en otra conversación. El número del segundo llamante (en espera) se muestra en el display o pantalla del teléfono, de forma tal que, el abonado puede conocer su identidad sin necesidad de interrumpir la llamada en curso. Permite seleccionar los números susceptibles de estar en espera.

2.1.8.5 SERVICIOS DE TELECONFERENCIA

Conviene indicar de que si bien en este apartado las distintas categorías de servicios de teleconferencia como pertenecientes a la familia de servicios de telefonía, la funcionalidad de estos la proporciona la propia terminal, por cuanto es intrínseco a ellos el valor añadido de los servicios. En general, se denominan servicios de teleconferencia a todos aquellos que, merced al concurso de terminales apropiadas, propiedad de los clientes, permiten a grupos de personas situadas en lugares remotos, mantener reuniones a distancia de igual manera a como lo harían de hallarse en un mismo lugar (naturalmente sin él, en ocasiones, imprescindible contacto físico). Hay cuatro modalidades:

- Audioconferencia básica.
- Audioconferencia de calidad especial.
- Multiconferencia.
- Teleconferencia audiográfica.

2.1.8.5.1 AUDIOCONFERENCIA BASICA

Permite establecer comunicaciones vocales entre dos grupos de personas a través de la Red Telefónica Básica (RTB), por medio de un equipo denominado **Terminal Básica de Audioconferencia** (TBA). El TBA facilita la amplificación de la señal vocal entrante, a fin de que

esta llegue con total claridad a todas aquellas personas situadas en el extremo receptor distante, con una potencia acústica similar a la que emite una persona cuando se halla en conversación. La utilización de la terminal precisa de cierta disciplina, dado que el propio funcionamiento impone ciertas limitaciones en la simultaneidad, por funcionar esta en modo semidúplex. Naturalmente, la audioconferencia básica, en su concepción más elemental, corresponde a la proporcionada por un teléfono manos libres. Tanto estos como el TBA existen una amplia gama, cada uno con sus propias características y funcionalidades.

2.1.8.5.2 AUDIOCONFERENCIA DE CALIDAD ESPECIAL

Se entiende por audioconferencia de calidad especial a aquella que se ofrece a través de **líneas dedicadas** a cuatro hilos. Posibilita una total interactividad en el intercambio de mensajes vocales, sin necesidad de disciplina alguna en cuanto a conversación simultánea se refiere, y a una calidad de audición superior a la normal. Normalmente, la utilización de este servicio conlleva al acondicionamiento acústico de las salas, así como el uso de ciertos equipos o facilidades especiales: video lento, telefax, teleescritura, etc. No obstante, este servicio apenas ha tenido difusión, por cuanto la evolución en la red y la aparición de nuevos equipos lo han hecho prácticamente innecesarios. Es sin embargo un servicio existente, que en su momento contribuyo excesivamente al mantenimiento de reuniones a distancia, activando el desplazamiento de personas de un lugar a otro.

2.1.8.5.3 MULTICONFERENCIA

El servicio de multiconferencia se establece en general a través de la RTB y opcionalmente por medio de líneas dedicadas. Permite la comunicación vocal entre dos o más terminales, geográficamente distanciados, y la comunicación recíproca entre cualquiera de ellos a la vez que la audición simultánea de la comunicación por el resto. Se puede ofrecer por equipos AC HOD, situados en dependencias del usuario, con cuantas líneas telefónicas estime conveniente en coincidencia con el máximo número de participantes previstos. Hay dos modalidades:
Concertada (meet-me).-Es aquella en la que los distintos participantes establecen contacto a una determinada hora, prefijada con atención, por medio de la marcación del número o números telefónicos asignados a la **terminal de multiconferencia** y unos números cables o passwords.
No Concertada (dial-up).-Es aquella en la que el moderador u operador establece contacto con todos y cada uno de los participantes, sin que sea precisa una concertación previa.

2.1.8.5.4 TELECONFERENCIA AUDIOGRAFICA

El servicio de teleconferencia audiográfica permite la comunicación multimedia a distancia y en tiempo real entre personas situadas en lugares distantes, por medio de terminales específicas autorizadas, con una calidad de audio de 7KHz y 64kbps, no condicionada por perturbaciones analógicas, así como facilidades auxiliares tales como video lento, telefax, teleescritura, etc..

2.1.8.6 PICTOGRAMAS Y SÍMBOLOS PARA AYUDAR A LOS USUARIOS DEL SERVICIO TELEFONICO

En conformidad con el proyecto de recomendación E.121 del TSB (Telecomunication Standard Buraure), UIT-T, se determinan una serie de pictogramas y símbolos para ayudar a los usuarios a identificar los servicios disponibles y a utilizarlos en cualquier lugar del mundo. Veamos algunos ejemplos:

- **Símbolo del Teléfono**.-Dicho símbolo puede utilizarse:
  - En lugar de la palabra.
  - Adjunto a un número telefónico.
  - Para indicar un lugar desde donde se puede telefonear.
  - Para referirse al servicio telefónico en general.
- **Símbolo para los Servicios de Información**.-Puede usarse para designar o localizar:

- El servicio de información telefónico general.
- La información sobre números telefónicos nacionales e internacionales.
- La asistencia de idiomas extranjeros.
- La información sobre hoteles, teatros, etc.

- **Símbolo para Facsímil**.-Puede utilizarse un símbolo de facsímil:
  - En lugar de la palabra facsímil.
  - Para indicar un lugar en el que pueda utilizarse un servicio facsímil.
  - Para aludir al servicio facsímil en general.
  - Junto al número facsímil del abonado

2.1.8.6.1 PICTIGRAMAS PARA AYUDAR A LA IDENTIFICACIÓN DE INFORMACIÓN

En algunos países existe un número general de urgencia, que puede marcarse en todas las situaciones de emergencia que se presenten. En otros, sin embargo, hay números telefónicos distintos para cada servicio de urgencia, tales como bomberos, ambulancias y policías. Siempre que se use un símbolo para indicar un número de urgencia general, este debe ser **SOS**. En el caso de que no exista un número general de urgencia, puede usarse el símbolo SOS para llamar la atención sobre la lista de números de urgencia.

2.1.8.6.2 PICTOGRAMAS PARA AYUDAR EN LA UTILIZACION DE UN SERVICIO PÚBLICO

La inclusión en los teléfonos de uso público de una secuencia o serie de pictogramas constituye un medio eficaz para instruir a los usuarios, en especial sí, como en el caso de visitantes extranjeros, no se encuentran familiarizados con el equipo o los procedimientos de utilización.

2.1.8.6.3 PICTOGRAMAS PARA AYUDAR A LA IDENTIFICACIÓN DE LOS SERVICIOS OFRECIDOS A LOS ABONADOS TELEFONICOS

Se pueden también utilizar símbolos para designar servicios ofrecidos a los usuarios telefónicos. Dichos símbolos pueden estar dibujados en el equipo del abonado, por ejemplo, en la parte superior del teclado utilizado para los servicios. En la figura 59 se muestran símbolos para funciones de telecomunicaciones y para servicios suplementarios.

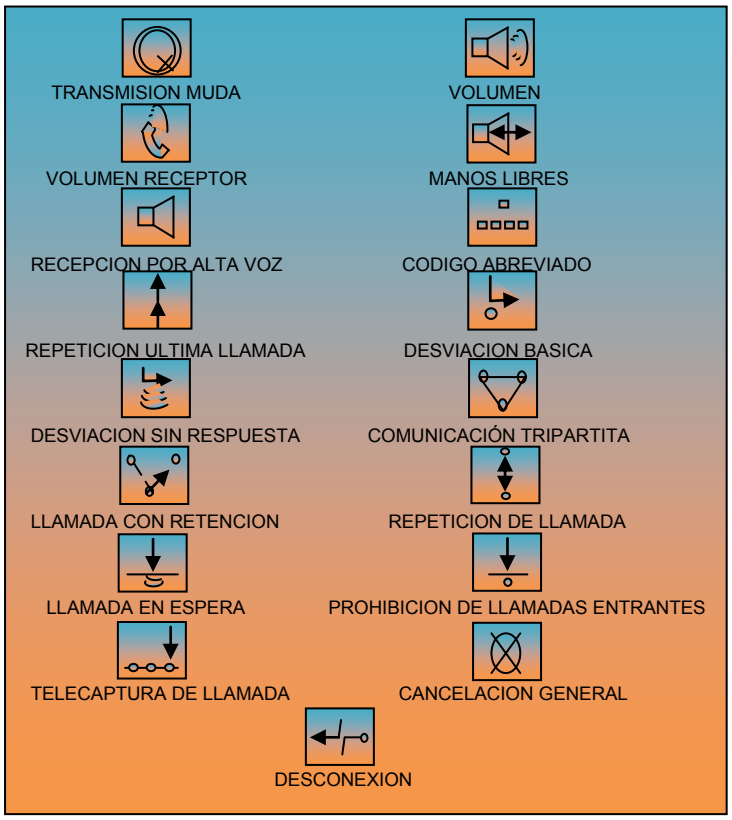


Figura 59

2.2 EVOLUCI0N DE LAS REDES TELEFÓNICAS

Anteriormente se han resaltado las fases más importantes de una comunicación telefónica: emisión de la voz, conversión de las señales sonora en señales eléctricas, envío en la línea y reconversión de las señales eléctricas en sonaras en la terminal distante. Esta comunicación corresponde a una simple conexión teléfono-teléfono, conectados por un medio portador fijo entre extremos constituido por dos hilos de cobre. De este modo, el aparato telefónico permitía comunicar dos personas distantes geográficamente, pero era necesario prefijar la hora de llamada. Para solucionar este inconveniente se incorporó al teléfono inventado por Alexander Graham Bell un dispositivo para generar corriente de llamada (magneto) y un timbre para avisar de esta, consiguiendo alcance de hasta tres kilómetros entre extremos. Con tal método, si una persona precisaba comunicarse con varias, debía disponer de otros tantos teléfonos, ya que cada línea estaba exclusivamente para dos interlocutores fijos. Para evitar este problema y satisfacer la necesidad de comunicarse a mayores distancias, se fueron ideando diversos procedimientos, hasta llegar a los modernos sistemas de conmutación automática de abonados del sistema telefónico. El primer paso consistió en conectar varios teléfonos a lo larga de un mismo portador, formando un anillo. Nuevos inconvenientes a esta primera solución: el generador de llamada debería ser potente para accionar los restantes timbres; todos los usuarios se podrían al hablar hasta comprobar a quien iba dirigida la llamada. A pesar de estos problemas, las solicitudes para disponer de estos aparatos se multiplicaron, y se ideó incorporar un anillo de teléfonos idéntico al anterior, de modo que dos teléfonos pertenecientes a ambos anillos correspondiesen a un mismo usuario, con el fin de hacer de intermediario de los avisos entre usuarios acoplados a los mencionados anillos. Estos arcaicos procedimientos escasamente podrían ser válidos para reducidos núcleos de población, incluso contando con la ventaja de mantener el funcionamiento del sistema en el caso de ruptura del medio portador en uno de los tramos, ya que la conexión entre dos aparatos estaba asegurada al poder realizarse sobre el mismo anillo pero en sentido contrario.

Lógicamente, para evitar estos inconvenientes, surgió la idea de llevar a todas las líneas telefónicas a un sólo lugar haciendo que cada una terminase sobre un enchufe, **jack**. Todos los jacks se situaban en un sólo cuadro, identificados por una pequeña chapa metálica acoplada a un electroimán, de tal forma que los abonados quedan definidos por un número. Este conjunto permanecía bajo la atención de una operadora. La llamada de un usuario provocaba la caída de la chapita y la operadora introducía en el correspondiente jack la clavija de su teléfono con vistas a conocer el número de usuario con quien el primero quería comunicarse; una llamada de la operadora al teléfono del destino y la conexión posterior de los dos jacks mediante un cordón, posibilitaba la comunicación posible. Este procedimiento de interconexión de abonados al servicio telefónico se complicaba considerablemente al incrementarse el número de usuarios y, en consecuencia, el de posiciones de operadora. Dado que las distancias del enlace telefónico deben ser mínimas ante el debilitamiento que sufre la señal en su transporte, se precisaba instalar otras posiciones de operadora en lugares diversos de una misma población y proceder a la interconexión de todas las posiciones entre sí. La complejidad del sistema indujo a sustituir la operadora por equipos automáticos, de modo que el abonado produce la llamada y selecciona el número de su interlocutor mediante un disco incorporado a su teléfono, los equipos de conmutación interpretan estas operaciones y se encargan de efectuar la llamada al otro teléfono completando la comunicación extremo a extremo: se inicia la conmutación automática de circuitos para señales de voz.

En la actualidad, tal automatismo permite que cuando un abonado descuelga el teléfono para iniciar una llamada telefónica reciba una señal, **tono de marcación**, que le invita a marcar por disco o teclado el número del abonado distante; al finalizar la marcación, la central se encarga de conectar con el teléfono destino. Establecida la comunicación, la central avisa al equipo que inicia la llamada si la terminal distante esta libre u ocupada, enviando otra señal para accionar el timbre del teléfono llamado en el supuesto de que este libre. Al finalizar la conversación, será necesario efectuar la desconexión del enlace, habiendo realizado previamente las funciones de tarificación de la llamada. A lo largo de la historia de la conmutación telefónica se ha abordado constantemente el perfeccionamiento de los equipos, con el fin de suprimir totalmente las labores manuales y conseguir la máxima calidad en el establecimiento de los enlaces telefónicos persona a persona. Dos años después de la invención del teléfono se instaló el primer centro de conmutación manual, aunque hubo que esperar ocho años más para disfrutar de las ventajas que ofrecía el primer selector de conmutación automática ideado por Strowger; la incorporación de ciertas modificaciones hizo que durante más de ochenta años estos equipos constituyesen los núcleos más importantes de las redes telefónicas. Centrales de estas características, conocidas como **sistemas paso a paso**, ofrecían no obstante ciertos inconvenientes, y fue preciso llegar a la segunda década del siglo XX para disponer de dos nuevos sistemas desarrollados en Estados Unidos por Bell System: el **sistema Panel**, especialmente implantado en el continente Americano, y el **sistema Rotary**, introducido en forma masiva en Europa. En el año de 1938 se instaló en Estados Unidos el primer equipo de una nueva generación de centrales denominadas **crosbar o barras cruzadas**; tanto en este sistema como en los anteriores ofrecían la característica común de ser electromecánicos. Este innovador sistema presentó numerosas versiones y su implementación en la red mundial fue notable.

Conviene señalar que, de modo esquemático, una central de conmutación esta formada por la **red de conexión**, conjunto de elementos por donde se encamina el tráfico .y la **unidad de control**, parte inteligente que interpreta las operaciones realizadas desde el teléfono con vistas a completar la comunicación. Los sistemas rotatorios se caracterizaban porque su red de conexión usaba selectores giratorios que se unían unos contactos situados en posición circular, físicamente en niveles o pisos. Un paso significativo en la evolución de los sistemas de conmutación telefónica fueron los desarrollados de **centrales electrónicas**. El estudio de esta nueva tecnología para el automatismo de la conmutación se inicio en los años treinta, pero hubo que esperar al año 1965 para la disponibilidad real de estos equipos. Inicialmente, los **sistemas semielectrónicos** fueron una evolución de los sistemas de barras cruzadas; los selectores matriciales incorporaban componentes electrónicos, tales como diodos de gas, relés de mercurio o de tipo reed (dos láminas encapsuladas que contactan bajo el efecto de un campo magnético).

Los sistemas de conmutación avanzada se caracterizan porque su órgano central de control esta constituido por un ordenador. **El control por Programa Almacenado (SPC, Stored Program Control)** utiliza instrucciones almacenadas en memoria que pueden modificar el programa de funcionamiento según las necesidades de la central. La red de conexión puede estar conformada por sistemas de conmutación espacial o temporal. Sistemas de estas características reducen las exigencias de mantenimiento y de espacio en planta; el dialogo desde una pantalla asociada al ordenador que controla el sistema permite dar ordenes sobre mantenimiento preventivo, supervisión, control, incorporación de facilidades, etc.. En la **conmutación espacial**, la interconexión de líneas en la central telefónica se realiza por un camino único, directo y permanentemente asociado a cada conexión, de tal forma que cada comunicación establecida dispone de un itinerario físicamente de los demás. La tecnología utilizada en los sistemas de conmutación por división en el espacio es del tipo electromecánico o electrónico. El primero utiliza selectores o relés en la conmutación y el segundo se apoya en el uso de semiconductores. El utilizar procedimientos de conexión mecánica, el ofrecer menor fiabilidad y el no permitir ampliar las centrales a gran capacidad, han descartado la incorporación de la red telefónica de centros de estas características en beneficio de sistemas de conmutación temporal. La implementación de técnicas de multiplexación en el tiempo **(PCM, Pulse Code Modulation)** permitió abordar la **conmutación temporal** sobre centrales digitales, basando su funcionamiento en asignar muy breves intervalos de información de entrada a intervalos de tiempo asociados al canal de salida. Un mismo camino físico compartido en el tiempo se utiliza a la vez por varias comunicaciones. Este procedimiento facilitó la interconexión directa entre sistemas de conmutación y transmisiones digitales, y favoreció a la vez su evolución de la red telefónica hacia configuraciones totalmente digitales.

2.3 PCM

2.3.1 INTRODUCCION

Desde sus orígenes, las comunicaciones telefónicas trataron de efectuarse ahorrando lo máximo posible, tanto en equipos como en espectro (en el rango de frecuencias empleado) con el fin de enviar la mayor información por un sólo vínculo. De esta manera nace el sistema multiplexado para enviar varios canales por un sólo medio de enlace. Dos son los sistemas frecuentes: **Multiplexación por División en el Tiempo (TDM Time División Multiplexing)** y **Multiplexación por División en Frecuencia (FDM Frequency División Multiplexing)**. El sistema de multiplexación nace con la necesidad de querer transmitir de varios canales en forma simultánea por un mismo vínculo de transmisión. Consiste en aplicar técnicas que permiten transmitir un paquete hacia un receptor y que este último pueda detectar la información recibida. En técnicas digitales se demuestra que un multiplexor permite que una entrada ingrese a la salida por medio de información aplicada a ciertas líneas de selección. Si efectuamos la selección en forma cíclica y alternada tendremos muestras correspondientes a las distintas entradas y como la transmisión se hace de forma ordenada y en sincronía, conoceremos que información corresponde a cada canal. La señal analógica del canal telefónico, es primeramente muestreada en el tiempo a una velocidad de 8,000 muestras por segundo; a continuación las muestras son codificadas en un código binario de 8 bits. Los pulsos codificados son colocados unos al lado del otro y forman un tren de pulsos que a continuación es transmitido del transmisor al receptor a través del medio de transmisión, como se ve en la figura 60.

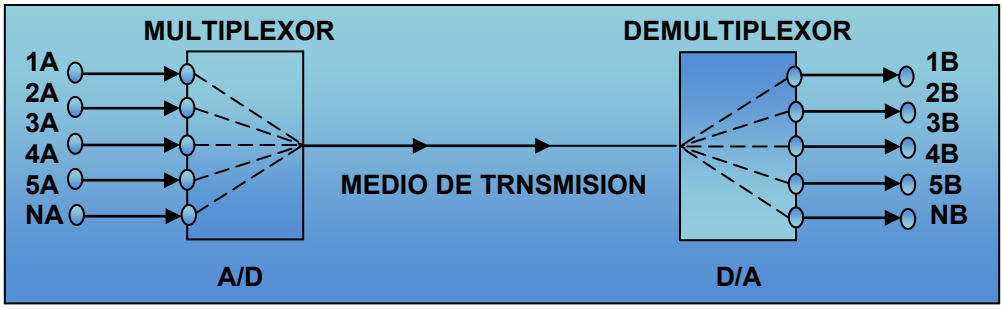


Figura 60

2.3.2 TEOREMA DEL MUESTREO

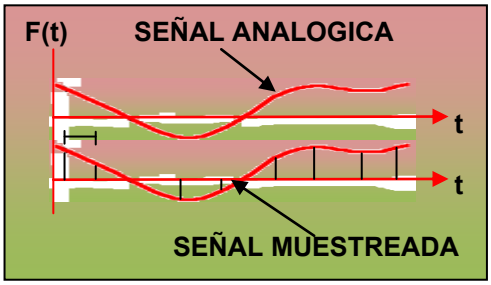


Figura 61

Es conocido a través del teorema del muestreo que una señal analógica $S(t)$ se puede convertir en una serie de impulsos, tomando los valores instantáneos de tensión en intervalos constantes equivalentes a $T = \frac{1}{2 f_M}$, con $f_M = 2 * 4000 = 8000 = 8\,KHz$ frecuencia máxima de la señal $S(t)$, como se muestra en la figura 61.

Utilizando los valores muestreados en lugar de la señal $S(t)$, se vuelven disponibles amplios espacios libres en el eje del tiempo, espacios que pueden llenarse con muestras procedentes de otras señales. Se realiza de esta manera la multiplexación TDM de señales **PAM (Pulse Amplitud Modulation)**. En realidad los impulsos PAM no se localizan directamente como en la figura 62, sino que la información de la amplitud relativa a cada impulso se codifica en un sistema binario y sucesivamente se localiza en el eje del tiempo, bajo la forma de un paquete de bits. El proceso que realiza esta transformación es conocido como PCM; se obtiene por lo tanto una Multiplexación por División en el Tiempo de señales numéricas PCM.

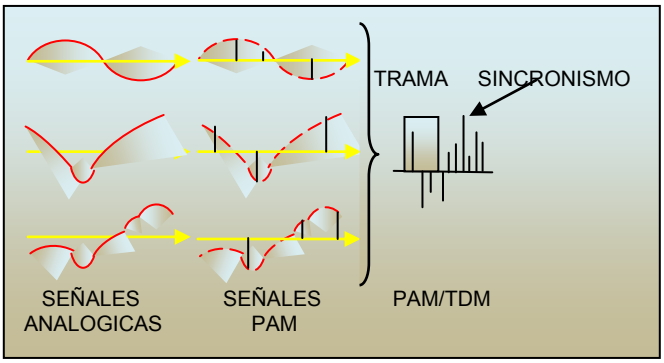


Figura 62

Para poder separar en recepción los distintos paquetes de bits de manera correcta, intercalada a los paquetes PCM se debe transmitir también una **secuencia de sincronismo (Sincronismo de Trama)**. Por lo tanto en el interior del intervalo T (que separa dos muestras consecutivas de la misma señal) se localizaran los paquetes de bits procedentes de las N señales, más la secuencia de sincronismo, como se ve en la figura 63.

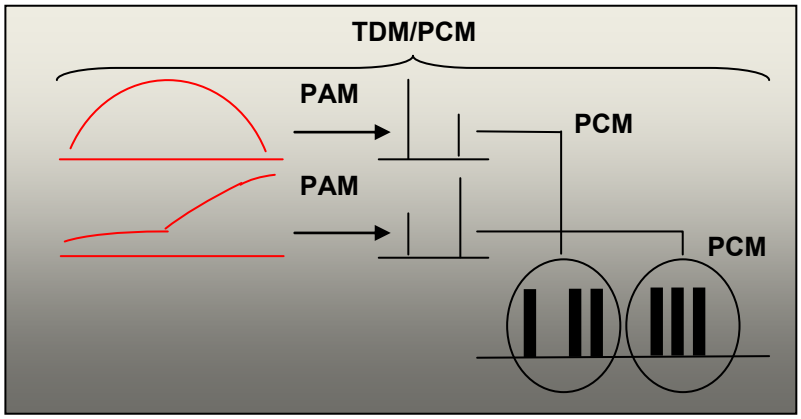


Figura 63 Multiplexacion por División en el Tiempo de señales PCM

El conjunto constituido por el sincronismo y los bits PCM se denomina **Trama**. Obsérvese que la trama tiene una duración equivalente al intervalo de muestreo T y que el tiempo T_s **(Time Slot, Ranura de Tiempo)** asignado a cada canal de muestra en el interior de la trama será inversamente proporcional al número de los canales a transmitir. Supóngase que se utilice una codificación PCM de m bits. Considérese la transmisión TDM de N señales telefónicas, en donde la secuencia de sincronismo ocupa el espacio reservado a un número S de canales PCM. Se tienen las relaciones siguientes:

$f_M = 4\,KHz$ *frecuencia máxima del canal telefónico* (*banda bruta*).

$T = \frac{1}{2 f_M} = 125\,\mu seg$ int *ervalo de muestreo* (*duración de la trama*).

$T_s = \frac{T}{(N + s)}$ int *ervalo de tiempo asignado a cada canal* (*time slot*).

$T_b = \frac{T_s}{m}$ int *ervalo de tiempo asignado a cada bit* (*bit time*).

$F_c = \frac{m}{T}$ *velocidad de transmisión del canal PCM*.

$F_b = \frac{1}{T_b}$ *velocidad de transmisión del flujo TDM / PCM*.

2.3.3 SISTEMA BASICO DE TRANSMISIÓN

En la figura 64 es un diagrama a bloques simplificado de un sistema PCM de primer orden, con capacidad de multiplexar y transmitir 30 canales telefónicos. El filtro paso banda, colocados en la entrada del canal, tiene la función de limitar la banda de frecuencias del canal de voz de manera de atender las recomendaciones del CCITT. La señal analógica aplicada a la entrada del sistema PCM ocupa un espectro de frecuencia de 20Hz a 20KHz; antes de ser transmitido, su espectro es reducido por el filtro paso banda de 0Hz a 4KHz.

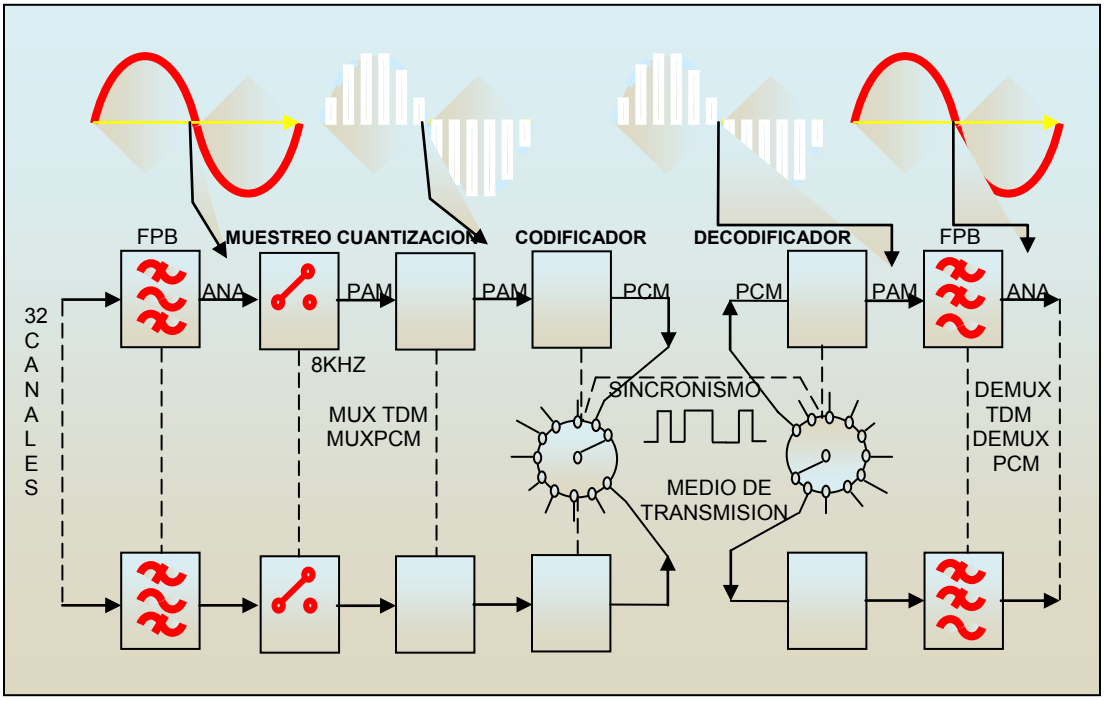


Figura 64

A pesar de que el canal telefónico ocupa una banda disponible de 0Hz a 4KHz, para una conversación telefónica dentro de los patrones internacionales sólo se ocupa en realidad el espectro de 0.3KHz a 3.4KHz, como se ve en la figura 65. La señal del canal telefónico, que ocupa el espectro de 0.3KHz a 3.4KHz, es aplicada en la entrada del circuito de muestreo.

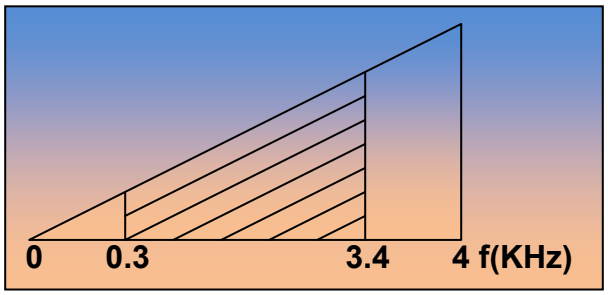


Figura 65

2.3.4 MUESTREO

El muestreo es el proceso por el cual la señal analógica es muestreada a intervalos regulares, transformándose en señales PAM. De acuerdo con el teorema del muestreo, para recuperar la señal analógica de baja frecuencia no hay necesidad de enviar toda la forma de onda de la señal analógica, sino sólo una secuencia de muestras. A través del proceso de muestreo, se obtiene una secuencia de pulsos, la amplitud de cada uno de los cuales corresponde a la amplitud de la señal analógica muestreada en ese instante. La sumatoria representa el formato de la señal analógica, como vemos en las formas de onda de la figura 66. Así podemos definir el proceso de muestreo como la sustitución de la señal del canal telefónico variable en el tiempo, por una sucesión de muestras de corta duración (pulsos y pausas) obtenidas de la señal analógica a intervalos regulares

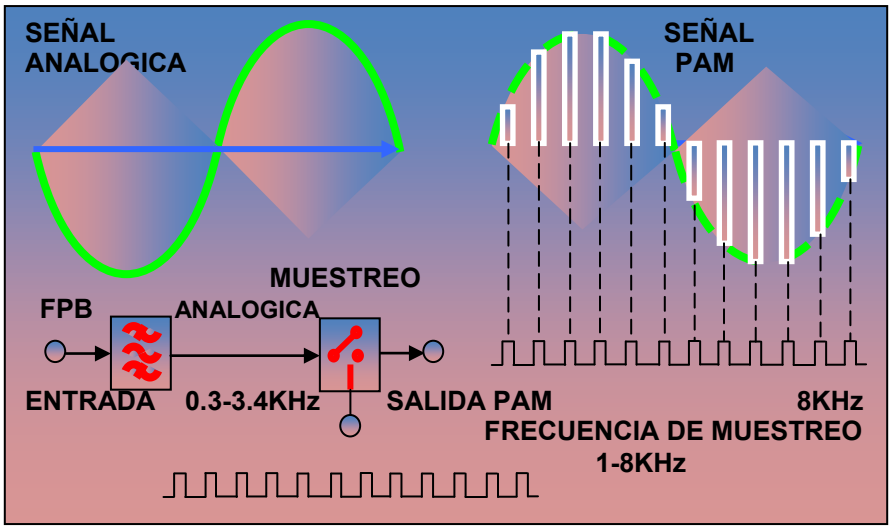


Figura 66

2.3.5 CUANTIFICACION

La cuantificación consiste en convertir una señal analógica con amplitudes infinitas, o no determinadas, en una señal digital con amplitudes finitas. La amplitud de cada pulso PAM es comparada dentro de diversos niveles discretos y, entre esos niveles, se elige el nivel más próximo de la amplitud de la señal en la entrada. En la figura 67 tenemos una señal analógica muestreada en PAM, con 8 pulsos, siendo 4 con polaridad positiva y 4 con polaridad negativa. Las amplitudes de los pulsos PAM son redondeados por el circuito de cuantificación para los niveles de cuantificación más próximos del nivel de la señal PAM en la entrada. Así, en la figura 67, donde los niveles de cuantificación son de 1V, en el pulso n°1, con amplitud de entrada aproximadamente de 0.8 V es redondeado por el circuito de cuantificación al nivel de 1V en la salida. El pulso n°2, con una amplitud de 2.54V, es redondeado para un nivel de 3V; lo mismo se hace con los demás pulsos de la entrada. En este proceso, cuando la amplitud del pulso a ser cuantificado esta ubicado exactamente entre dos niveles de decisión, por ejemplo 2.5V el redondeado se hace siempre hacia el nivel de decisión superior más próximo, o sea, hacia 3V.

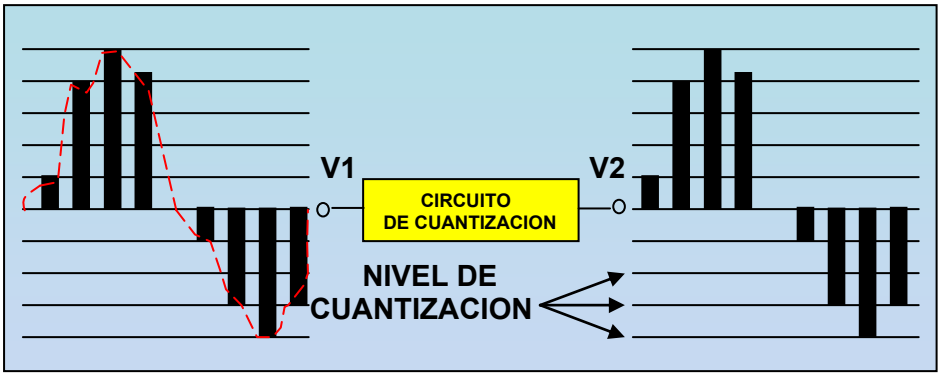


Figura 67

El proceso de cuantificación, provoca un pequeño deterioro en la calidad de la información recibida. La diferencia entre las amplitudes de los pulsos de entrada y en la salida del circuito cuantificador induce un error, conocido como **error de cuantificación** N_Q. Este error se manifiesta en la salida del sistema en la forma de ruido, llamado **ruido de cuantificación**, semejante al ruido blanco.

2.3.5.1 RUIDO DE CUANTIFICACION

El ruido (o error) de cuantificación es la diferencia entre la señal analógica y el valor cuantificado correspondiente, figura 68. La relación entre la señal S y el ruido de cuantificación N_Q depende de la amplitud de la señal, ya que el salto ΔV es uniforme en toda la entrada de la señal. Esto significa que las señales elevadas presentarán una mejor relación S/N_Q que la de las señales débiles. Para obtener una relación S/N_Q uniforme en toda la señal de entrada se recurre a la técnica de comprensión de la señal que lleva a cabo la codificación no lineal

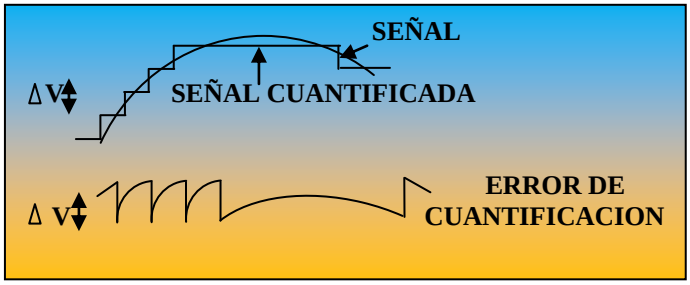


Figura 68

2.3.5.2 CURVA DE CUANTIFICACION LINEAL

En la cuantificación lineal, la graduación del eje vertical, corresponde a los niveles de cuantificación, obedece a una variación lineal, o sea, la graduación de los valores del eje Y es constante. Los intervalos son fijados en valores predeterminados, igualmente espaciados, como se observa en la figura 69. En la cuantificación lineal, la relación S/N_Q empeora para los impulsos de baja amplitud, mejorando para los impulsos de mayor amplitud. En la figura 69a tenemos una señal analógica siendo cuantificada y en la figura 69b tenemos el nivel del ruido N_Q resultante del error de cuantificación de la señal muestreada. Como podemos observar, el nivel de ruido N_Q alcanza su valor máximo en los puntos donde la señal analógica pasa por el cero, lugar donde la señal analógica presenta baja amplitud. En los puntos donde la señal analógica alcanza su máximo valor, tanto positivo como negativo, el ruido N_Q alcanza su valor mínimo. Lo expuesto puede ser ejemplificado de la siguiente manera: suponiendo que el pulso de la entrada tenga una amplitud de 0.5V, la amplitud del pulso será redondeado hacia un valor inmediatamente superior, aparecerá en la salida con 1V; en este caso hubo un error del 50%, equivalente a un ruido muy elevado. En el caso de un pulso con amplitud en la entrada de 10.5V, este aparecerá en la salida con una amplitud de 11V, correspondiente a un 5%. Como podemos ver, cuando menor sea la amplitud del pulso PAM en la entrada, mayor será la amplitud del ruido N_Q y menor será la relación S/N_Q en este punto. Esto significa que en la cuantificación lineal las muestras de baja amplitud son las más afectadas por el ruido y no los pulsos de grandes amplitudes. Por otro lado, la amplitud media de la señal de voz, en una conversación telefónica normal, aplicada a la entrada del multiplexor PCM de la figura 69, tiene un valor nominal de –15 dBm, puede llegar algunos casos a –410 dBm y comprometer el uso de la cuantificación lineal. En razón de eso, la curva con variación lineal es poco usada en el sistema PCM, la más usada es la curva de variación no lineal (hiperbólica o logarítmica). En esta última, la relación S/N_Q es constante e independiente de la amplitud de la señal en la entrada del multiplexor PCM.

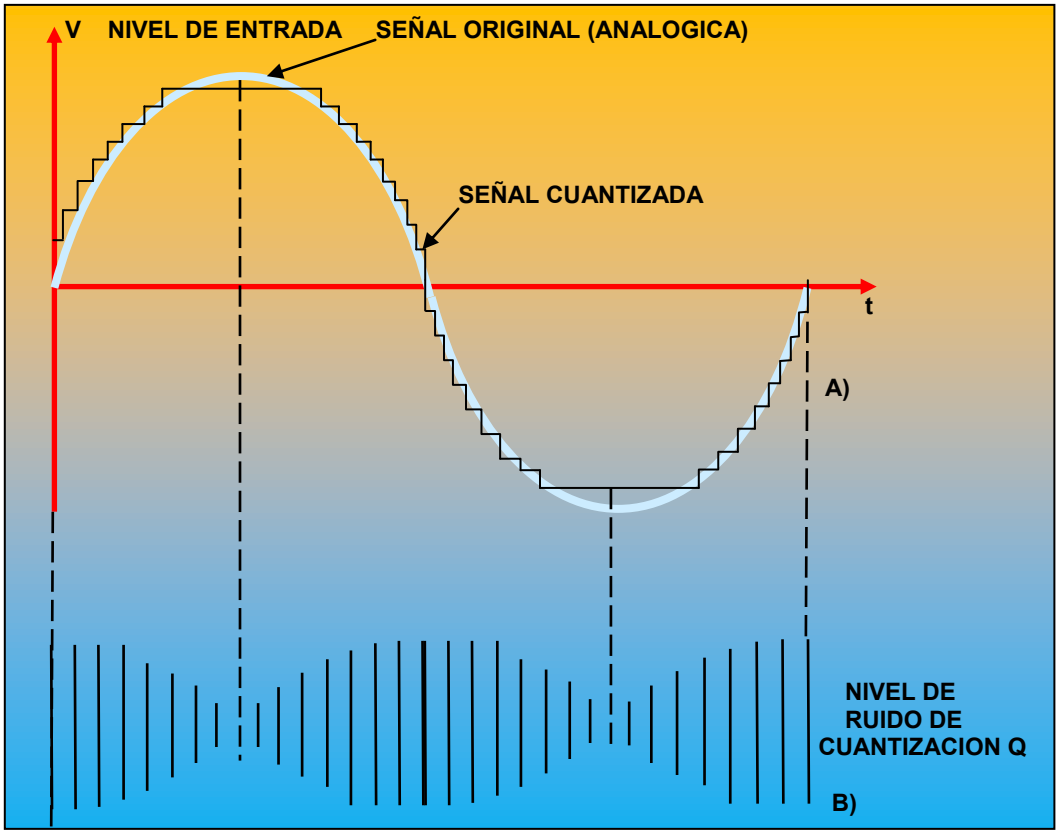


Figura 69

2.3.5.3 CUANTIFICACION NO LINEAL

El sistema de transmisión PCM debe ser capaz de transmitir señales de voz con gran variación de amplitud (60dB o más), así mantiene una relación S/N_Q constante en toda la banda de variación. Para mantener la relación S/N_Q constante, las señales PAM de baja amplitud deben ser reforzadas que las señales de mayor amplitud. Esta operación equivale a reducir la amplitud de los pulsos mayores y al mismo tiempo reforzar los pulsos de baja amplitud. En el sistema PCM esto se consigue haciéndose los intervalos entre dos niveles consecutivos más estrechos para niveles de baja amplitud y más espaciados para los niveles más altos. En la figura 70 tenemos una curva de cuantificación con variación no lineal, como podemos ver, los intervalos próximos al punto de cruce de los ejes son menores, y a medida que se alejan de los mismos los intervalos aumentan. Observe también que no sólo los intervalos son menores sino también los valores asumidos por cada intervalo.

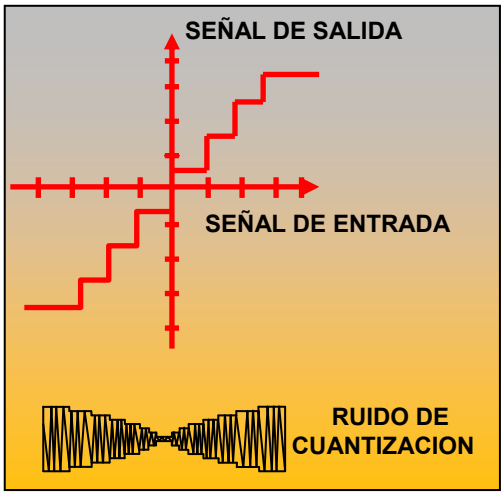


Figura 70

El nivel de ruido de cuantificación, que es mostrado en la figura 70, aumenta a medida que se aleja del punto de cruce; lo mismo ocurre con la señal PAM. Como la amplitud de los pulsos PAM y el nivel de ruido aumentan en la misma proporción, significa que la relación S/N_Q (diferencia en dB entre la amplitud de la señal y del ruido) se mantiene constante.

Otra manera de representar la curva vista en la figura 70 es a través de la gráfica de la figura 71, formado por 13 segmentos de rectas, incluyendo los dos cuadrantes. En el eje horizontal están representados los intervalos de cuantificación en un total de 256 niveles, siendo 128 positivos y 128 negativos (28=256=128+128). Los puntos de intersección de los ejes forman 6 segmentos de rectas, proyectados en el 1° y 3° cuadrante, formando un sólo segmento, totalizando 13 segmentos, de ahí la denominación de curva de los 13 segmentos.

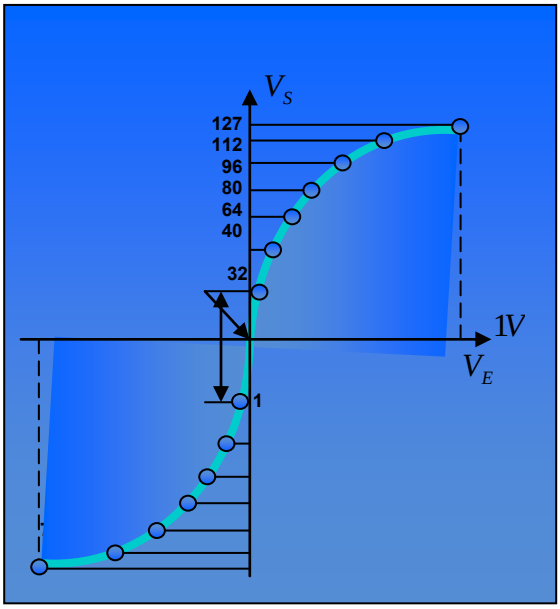
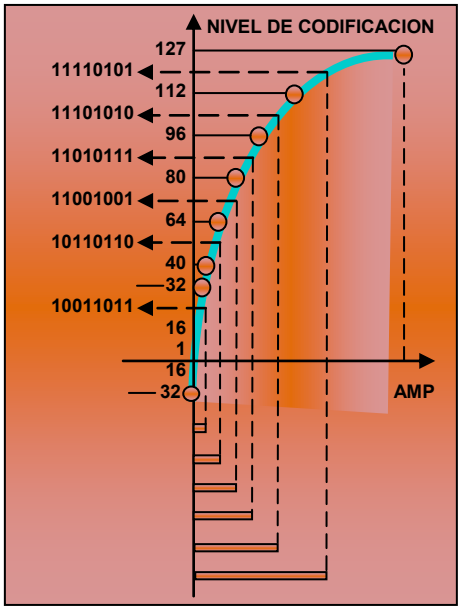


Figura 71



Como podemos observar en la figura 72, el segmento N°1, esta formado por 64 niveles, siendo 32 en el 1° cuadrante y 32 en el 3° cuadrante, lo que equivale a 64 segmentos. En el diagrama de la figura 72 esta representado con detalles sólo la parte positiva de los segmentos, o sea, la parte que esta dentro del 1° cuadrante de la figura 72. Los intervalos ubicados en el eje horizontal para señales de pequeña amplitud son menores, equivalen a una variación logarítmica aproximada. Los intervalos próximos al punto de cruce de los ejes son pequeños, aumentando a medida que se alejan del cruce. Los segmentos 1 y 2 están casi en la vertical, los pulsos de entrada, cuyas amplitudes están ubicadas en intervalos son reforzados, como por ejemplo en el pulso N°1; por lo tanto esta curva representa una variación no lineal.

Figura 72

A su vez, para el segmento de recta N°7, a pesar de que el eje horizontal en este intervalo presenta mayor variación, los pulsos cuya amplitud caen en este intervalo como por ejemplo el pulso N°6, no sufrirán casi ningún refuerzo. Como vemos en la curva de la figura 72 es una curva de transferencia no lineal, por eso es la más usada en la cuantificación de señales PAM/PCM.

2.3.6 CODIFICACION

La codificación es la operación a través de la cual la información contenida en los impulsos PAM son representados por un código binario de 8 bits. En la codificación PCM se usa la codificación binaria, formada por dos niveles discretos (1 y 0) como vemos en la columna 6 de la tabla 13.

NÚMERO DEL PULSO	POSICIÓN DE LOS PULSOS DENTRO DEL SEGMENTO	NIVEL DE CUANTIZACION	NIVEL DENTRO DE LOS 16 INTERVALOS DE CADA SEGMENTO	VALOR DEL BIT (1 2 3 4 5 6 7 8)	NIVEL TRANSMITIDO POR LA LÍNEA
1	1	28	11	1 0 0 1 1 0 1 1	
2	3	55	6	1 0 1 1 0 1 1 0	
3	4	74	9	1 1 0 0 1 0 0 1	
4	5	88	7	1 1 0 1 0 1 1 1	
5	6	107	10	1 1 1 0 1 0 1 0	
6	7	118	5	1 1 1 1 0 1 0 1	

Tabla 13

La necesidad de codificar los pulsos PAM presentes en la salida del circuito de muestreo se debe a:

- Si los pulsos fueran transmitidos en la forma original, de diferentes amplitudes serían fuertemente atenuadas debido a la distorsión provocada por los medios de transmisión.
- El circuito de identificación/detención del lado de recepción sería muy complejo, debiera reconocer las diferentes amplitudes de los pulsos PAM, que necesitan por los menos 100 niveles para representar la señal de la voz.

Usando la codificación binaria, los códigos son representados por dos niveles discretos (1 y 0), lo que simplifica mucho el proyecto del decodificador. Además, los bits "1" y "0" no son afectados por la distorsión de la línea, pues el detector los verá como simple presencia y ausencia de nivel. La señal binaria formada por "1" y "0" se obtiene a partir de la codificación de los intervalos de cuantificación y de la polaridad de los pulsos. Considerando que cada información es codificada por un bit, que asume dos valores ("1" y "0"), podemos tener 2_n códigos posibles. En la codificación PCM se adoptó $N = 8$ pues es ese el valor que mejor satisface el compromiso entre el ancho de pulsos y la banda ocupada por los mismos.

2.3.6.1 CODIFICACION DE LOS PULSOS PAM EN UNA PALABRA DE 8 BITS

Los pulsos PAM, antes de ser transmitidos, son codificados en una palabra de 8 bits como se ve en la figura 73. El primer bit es usado para codificar la polaridad del pulso, o sea, indica si el pulso codificado es negativo o positivo. Cuando el pulso a ser codificado esta por encima del cero, el primer digito es codificado como "1" y cuando el pulso esta por debajo del cero, es codificado como "0" (tabla 13 columna 5).

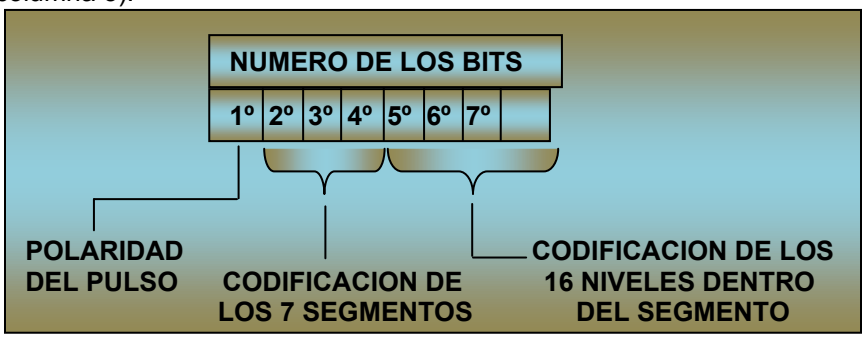


Figura 73

Los tres dígitos son usados para codificar los segmentos de la recta, numeradas de 1 a 7 como se ve en la figura 72. Como podemos ver, tenemos una tabla de 13 segmentos, siendo 6 los colocados en el 1° cuadrante, por lo tanto positivos, y 6 en el 3° cuadrante, por lo tanto negativos, además del N°1 que es común al 1° y al 3° cuadrante al mismo tiempo. Para los efectos de la codificación, sólo serán codificados los 7 segmentos positivos o los 7 negativos, pues la polaridad del pulso PAM ya fue determinada por el 1° dígito. Los segmentos son codificados por su código binario correspondiente; por ejemplo, el segmento N°1 es codificado por el código binario 001, el segmento N°7 es codificado por el código binario 111, el mismo es válido para los demás segmentos, como vemos en la tabla 13, columna 5. Los 4 dígitos restantes, o sea, los de N° 5, 6, 7 y 8, son usados para codificar los niveles de cuantificación dentro del segmento codificado por los dígitos 2, 3 y 4. Una vez que fue identificada la polaridad del pulso y el segmento en el cual esta ubicado el pulso, no hay más necesidad de identificar el nivel entre los 256 niveles, sino sólo uno entre los 16 niveles del segmento en cuestión.

Así los 16 niveles de cada segmento numerados del 1 al 16, son codificados por los 4 dígitos restantes. Pero debido al hecho de que sólo disponemos de 4 dígitos para codificar 16 niveles, el número de bits no es suficiente, pues el número decimal 16, cuando es codificado en binario ocupa 5 dígitos, o sea $(6)_{10} = (0000)_2$ Para subsanar este inconveniente, se usa el siguiente procedimiento: el nivel N°1 dentro del segmento es considerado por convención como el número cero; siguiendo el mismo razonamiento, el nivel 16 pasa a ser el nivel 15; el segmento sigue teniendo 16 niveles, pero ahora, numerados del 0 al 15. Ahora los 16 niveles son codificados en binario, usando los 4 dígitos, como vemos en la figura 74B-3.

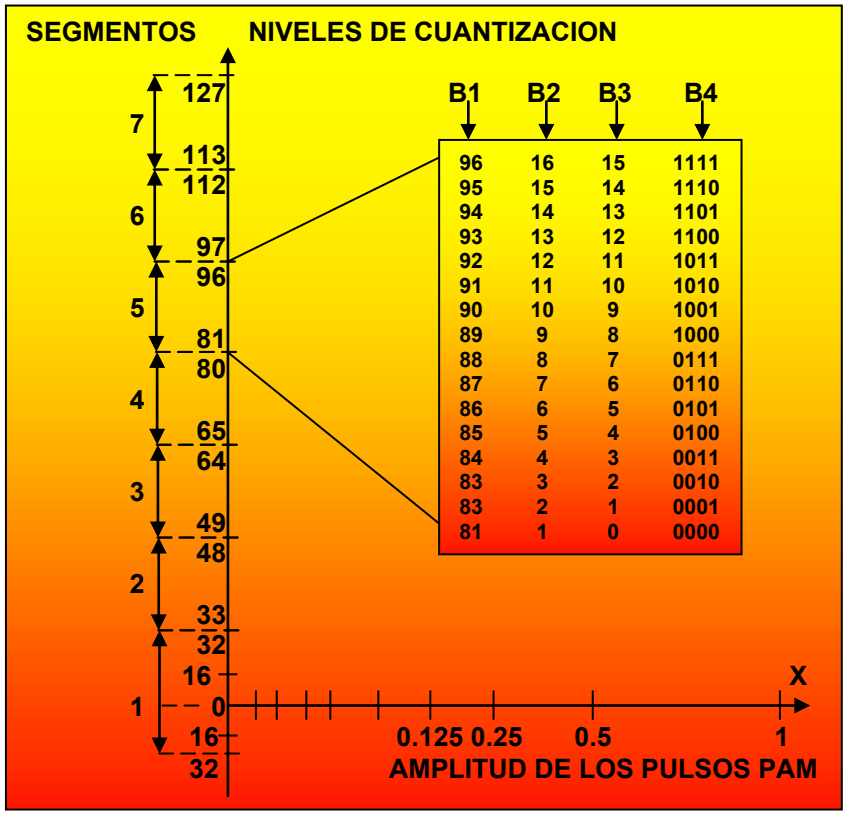


Figura 74

En la figura 72, tenemos 6 pulsos PAM de entrada, con diferentes amplitudes, todos con amplitudes positivas, y en consecuencia todos ubicados encima del eje horizontal, parte positiva de la curva de los niveles de entrada. En nuestro ejemplo, el primer dígito de codificación de los pulsos de la figura 72, será siempre “1”. En el pulso No.1, de baja amplitud, ubicado dentro del 1° segmento de la recta, tendrá su amplitud nivelada con el nivel de cuantificación 11, del primer segmento, como vemos en la columna 4 de la tabla 13. Así en el pulso No.1 es codificado dentro de la palabra de 8 bits (figura 73) con el siguiente código binario: 1-001-1011.

En la figura 74 tenemos un ejemplo de cómo se hace la codificación de los 16 niveles de cuantificación dentro de un determinado intervalo, en este caso el del No.5. Como podemos ver en la figura 74, los niveles dentro de ese segmento comienzan en el nivel 81 y termina en el nivel 96,

con un total de 16 niveles. En la columna B1 tenemos la relación entre los niveles de cuantificación numeradas del 81 a 96 y los 16 niveles correspondientes, dentro del segmento en estudio. En la columna B3 de la figura 74 tenemos los 16 niveles numerados del 0 al 15 y la columna B4 la codificación binaria correspondiente a 16 niveles. La codificación usada en la columna B4 es la misma de los 4 últimos bits de la palabra de 8 dígitos como vemos en la figura 73. Todo el procedimiento visto en la figura 74 puede usarse en la codificación de los demás niveles dentro de cualquiera de los 7 segmentos. Lo expuesto arriba es válido tanto para pulsos positivos como negativos, lo que va ha cambiar en términos de codificación es valor binario atribuido al 1° dígito. Como vemos, el código de 8 bits transporta diversas informaciones referentes a la señal PAM codificada, así como polaridad, amplitud y posición dentro del segmento.

2.3.7. PERIODO Y VELOCIDAD DE MUESTREO

Considerando la frecuencia de muestreo de 8,000Hz, el tiempo gastado para hacer un barrido completo de los 32 canales es de:

$$T_A = \frac{1}{f_M} = \frac{1}{8000} = 125\mu seg$$

Considerando que se gasta un tiempo para muestrear los 32 canales, el muestreo de cada canal tiene una duración de:

$$T_d = \frac{T_A}{32} = \frac{125}{32} = 3.9\mu seg$$

Como se muestra en la figura 75

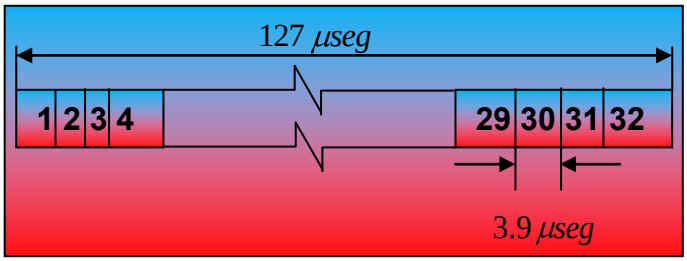


Figura 75

Se usa una frecuencia de muestreo de $f_M = 8000\,Hz$ para muestrear la señal analógica de cada canal; a su vez, cada muestra obtenida era codificada por un código de 8 bits. Así, para muestrear un canal telefónico se usa una frecuencia de muestreo de: $8000 * 8 = 64000\,bps = 64kbps$. Para muestrear los 32 canales que componen el sistema básico, o el de 1º orden, se usa una velocidad de muestreo de: $64kbps * 32 = 2048\,kbps = 2.048Mbps$

2.3.8 MULTIPLEXACION TDM DE LOS CANALES TELEFONICOS

La multiplexación por división en el tiempo es definida como el proceso que nos permite transmitir varios canales telefónicos a través del mismo medio de transmisión. Como vimos, el tiempo para muestrear los 32 canales es de $125\mu seg$, ya que cada muestra tiene una duración de $3.9\mu seg$, tiempo muy pequeño comparado al tiempo de $125\mu seg$, como vemos en la figura 76. En los intervalos entre retirar la 1° muestra de un canal dado y el retiro de la 2° muestra del mismo, son enviadas muestras de otros canales a ser transmitidos. Así, las palabras de código de 8 bits de diversos canales telefónicos son transmitidas en una secuencia cíclica a través del medio de transmisión. Entre dos palabras de código en un mismo canal son introducidas en secuencia palabras de código de otros canales, formando así una señal PCM, un tren de pulsos continuos. El circuito de muestreo o **mupltiplexador**, puede ser representado por una llave rotativa que hace un barrido completo a cada $125\mu seg$. En la primera vuelta de la llave la misma tira la primera muestra de los 32 canales; en la segunda vuelta tira la segunda muestra y esto se repite hasta complementar el muestreo de los 32 canales. Las muestras retiradas de cada canal o cada vuelta de la llave son codificadas y transmitidas en la forma de un tren de pulso.

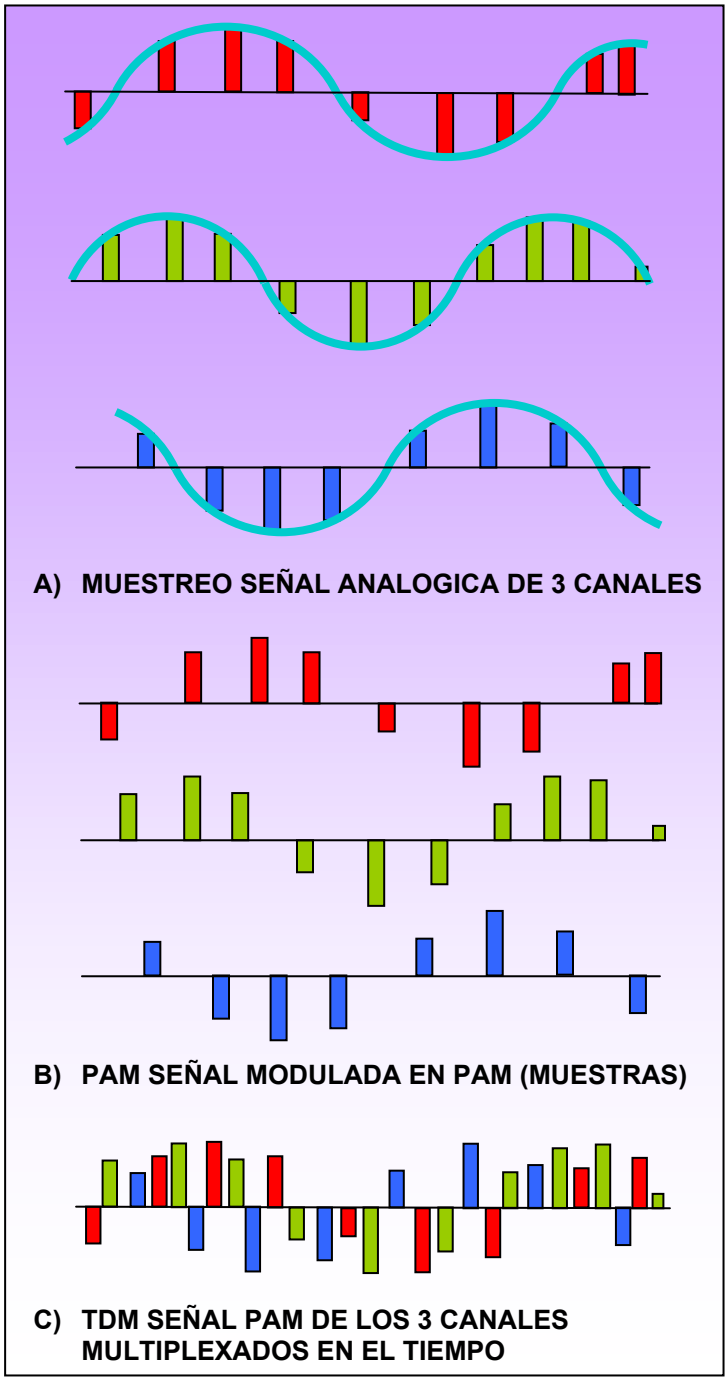


Figura 76

En la secuencia la figura 76 tenemos un ejemplo de como ocurre la multiplexación en el tiempo, tomándose como ejemplo la multiplexación de tres canales. En la figura 76A tenemos la señal analógica de los tres canales muestreados en el tiempo. No debemos olvidar que los canales son muestreados a una velocidad de 8,000 muestras por segundo. En la figura 76B tenemos los pulsos PAM correspondiente a los tres canales muestreados. Como podemos observar, las amplitudes de los pulsos representan la variación en el tiempo de las amplitudes de las señales analógicas vistas en la figura 76A. En la figura 76C tenemos los tres canales multiplexados en el tiempo, donde los pulsos retirados de uno de los canales son intercalados entre los pulsos de los otros dos canales. El procedimiento descrito en la multiplexión de los tres canales es válido para la multiplexación de

los 32 canales; lo que cambiará en este caso es que vamos a tener más muestras viajando por la línea, siendo una colocada al lado de la otra, como vemos en la figura 76C. Las muestras de los 32 canales son codificadas por el orden de llegada en la entrada del circuito de codificación, en un código de 8 bits y los bits son transmitidos secuencialmente a través del medio de transmisión.

2.3.9 DECODIFICACION DE LAS SEÑALES PCM

La decodificación de las señales PCM es el proceso inverso de la codificación; mientras la codificación convierte la señal analógica en muestras y esta en un código de 8 bits, la decodificación, a partir de los 8 bits, convierte muestras y estas en señal analógica. Primeramente los 32 canales recibidos a través del medio de transmisión son separados a través del circuito de multiplexación; la señal codificada en cada canal es enviada a su respectivo circuito de codificación. Las muestras codificadas recibidas son inicialmente convertidas en una señal PAM. Como vimos, las muestras codificadas transmitidas transportan consigo diversas informaciones, así como la polaridad de los pulsos, ubicación dentro del segmento, y del nivel dentro de ese segmento. Es a través de esas informaciones transportadas que el circuito de decodificación del lado del receptor recompondrá la señal PAM transmitida. Así, a partir de las nuestras codificadas recibidas es que la señal analógica aplicada a la entrada del canal (lado de transmisión) es reconstruida en la salida. Los pulsos PAM recuperados en la salida presentan las mismas características que poseían antes de haber sido codificados, así como la amplitud y la variación en el tiempo. En la figura 77 tenemos un diagrama básico simplificado por un decodificador, formado por 2 bloques, usado en la recepción de señales codificadas en PCM. La señal PCM, codificada en una palabra de 8 bits, es aplicada a la entrada del decodificador, donde el tren de pulsos es transformado en una señal PAM en la salida, con el mismo formato de la señal PAM aplicado a la entrada del decodificador. La señal analógica es reconstruida a partir de la señal PAM recuperada. Esta es aplicada a un filtro paso bajas con frecuencia de corte $f_c = 3.4\,KHz$, dejando pasar sólo la frecuencia fundamental de la señal muestreada (0.3KHz-3.4KHz), donde la señal PAM es convertida en la señal analógica correspondiente. Como podemos observar, el filtro hace la función inversa del circuito de muestreo, convirtiendo a la señal PAM en analógica. Así, la señal de voz aplicada en la entrada del sistema PCM es recuperada en la salida.

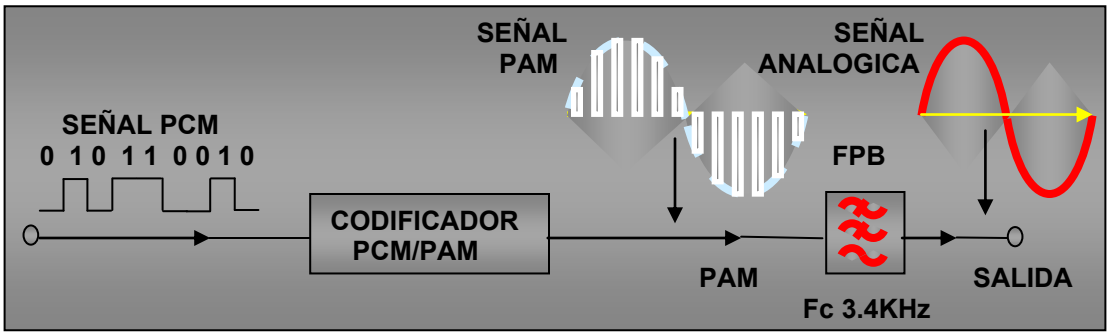


Figura 77

2.3.10 FORMACION DE SISTEMAS PCM DE JERARQUIA SUPERIOR

El equipo PCM de primer orden tiene la capacidad de multiplexar y transmitir 32 canales telefónicos con una velocidad de 2,048Kbps. Cuando hay necesidad de transmitir a través del mismo medio de un número de canales superior a este, los canales son agrupados a través de la multiplexación hasta conseguir el número de canales deseados. Para conseguir tal objetivo, se agrupan 4 sistemas de primer orden para formar un sistema de segundo orden con capacidad de 120 canales y una velocidad de 8,448Kbps; el mismo es válido para los demás sistemas, tabla 14.

PARAMETRO ANALIZADO	MAGNITUD
Frecuencia de Muestreo	8khz
Cantidad de muestras por Canal	8000/seg
Duración de 1 ciclo de barrido	$125\mu seg$
Duración de una Muestra, 1 bit	$3.9\mu seg$
Número de bits por palabra	8
Velocidad de muestreo de 1 Canal	64kbps
Velocidad de Muestreo de los 32 Canales	2048kbps

Tabla 14 Datos del sistema básico de 1º orden, 32 canales.

Como vemos, 4 sistemas de orden inferior son agrupados para formar un sistema de orden superior. A través del agrupamiento sucesivo podemos llegar hasta sistemas de quinto orden con capacidad de 7,680 canales telefónicos y una velocidad de 564,992Mbps, codificados en PCM, tabla 15

JERARQUIA DEL SISTEMA	1º ORDEN	2º ORDEN	3º ORDEN	4º ORDEN	5º ORDEN
Número máximo de canales	32	120	480	1920	7680
Velocidad de transmisión	2048Kbps	8448Kbps	34,368Mbps	139,268Mbps	564,992Mbps

Tabla 15

2.4.1. CONCEPTO DE MODEM.

2.4.1.1 INTRODUCCIÓN

MODULACIÓN DE LA INFORMACIÓN: EL MODEM.

Un módem es un dispositivo que convierte las señales digitales de la computadora en señales analógicas que pueden transmitirse a través del canal telefónico. Existen distintos sistemas de modular una señal analógica para que transporte información digital. En la figura 78 se muestran los dos métodos más sencillos la modulación de amplitud y la modulación de frecuencia. Otros mecanismos como la modulación de fase o los métodos combinados permiten transportar más información por el mismo canal.

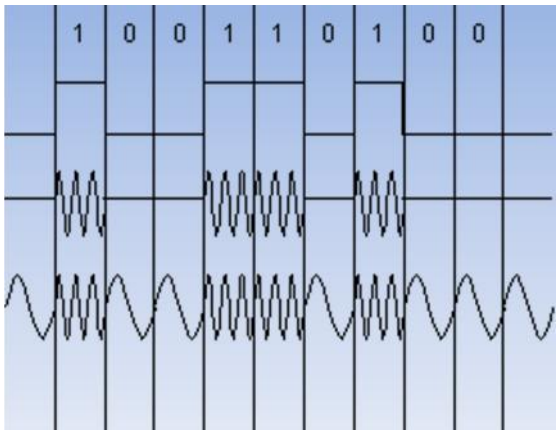


Figura 78

Baudios.-Es el número de veces de cambio en el voltaje de la señal por segundo en la línea de transmisión. Los módems envían datos como una serie de tonos a través de la línea telefónica. Los tonos se "encienden" (ON) o "apagan" (OFF) para indicar un 1 o un 0 digital. El baudio es el número de veces que esos tonos se ponen a ON o a OFF.
Bits por segundo (BPS).-Es el número efectivo de bps, que se transmiten en una línea por segundo. Como hemos visto un módem de 600 baudios puede transmitir a 1,200bps, 2,400bps ó incluso a 9,600bps.

La señal esta formada por diferentes tonos que viajan hasta el otro extremo de la línea telefónica, donde se vuelven a convertir a datos digitales.

2.4.1.2 TIPOS DE MODEMS

2.4.1.2.1 MODEMS EXTERNOS

Los módems externos tienen algunas ventajas sobre los internos. La mayoría de ellos tienen luces indicadoras que les dicen lo que está sucediendo durante una sesión de comunicación, si está recibiendo o enviando datos, si aún está conectado, y otras informaciones. Los módems externos funcionan con cualquier computadora incluyendo las que tiene micro-canal como las PS/2, las laptops y Macintosh, además estos módems se deben conectar a un puerto serial de la PC y tienen la ventaja de que se pueden mover fácilmente de un equipo a otro.

2.4.1.2.2 MODEMS INTERNOS

Traen incorporados un puerto serial para comunicarse con la computadora. Sus desventajas son que ocupan una ranura (slot) de expansión y toman la energía de la fuente de poder de la PC, lo que eventualmente aumenta la temperatura dentro de ella.

2.4.1.3 VELOCIDAD DE TRANSMISIÓN

¿Que son las velocidades de transmisión entre los módems? Existen dos tipos de velocidades para módems:

- La velocidad entre mi computadora y el módem, es decir la forma en que mi computadora le dice a mi módem que debe de transmitir, esta velocidad puede alcanzar hasta los 115,200bps, de esta forma la máquina le libera más rápido la información.
- La velocidad entre módems, esta velocidad puede llegar hasta 56,000bps (en condiciones físicas de transmisión óptimas), esta es la velocidad en que ambos módems mandan y reciben información entre ellos.

2.4.1.3.1 LIMITACION FÍSICA DE LA VELOCIDAD DE TRANSMISIÓN EN LA LÍNEA TELEFÓNICA.

Las leyes físicas establecen un límite para la velocidad de transmisión en un canal ruidoso, con un ancho de banda determinado. Por ejemplo, un canal de banda 3,000Hz, y una señal de ruido 30dB (que son parámetros típicos del sistema telefónico).

- **Throughput**.-Define la cantidad de datos que pueden enviarse a través de un módem en un cierto período de tiempo. Un módem de 9,600 baudios puede tener un Throughput distinto de 9,600bbps debido al ruido de la línea (que puede ralentizar) o a la compresión de datos (que puede incrementar la velocidad hasta 4 veces el valor de los baudios). Para mejorar la tasa efectiva de transmisión o Throughput se utilizan técnica de compresión de datos y corrección de errores.
- **Compresión de datos**.-Describe el proceso de tomar un bloque de datos y reducir su tamaño. Se emplea para eliminar información redundante y para empaquetar caracteres empleados frecuentemente y representarlos con sólo uno o dos bits.
- **Control de errores**.-La ineludible presencia de ruido en las líneas de transmisión provoca errores en el intercambio de información que se debe detectar introduciendo información de control. Así mismo puede incluirse información redundante que permita además corregir los errores cuando se presenten.

2.4.1.3.2 VELOCIDADES Y ESTANDARES

La velocidad con que los módems se comunican, enviando y recibiendo información, se mide en bits por segundo (bps). Para hacerlo más sencillo se puede decir lo siguiente:

- Un módem de 2,400bps, transmite 0.3kbps.
- Un módem de 14,400bps, transmite 1.8kbps.

- Un módem de 19,200bps, transmite 2.4kbps.
- Un módem de 28,800bps, transmite 3.6kbps.
- Un módem de 33,600bps, transmite 4.2kbps.
- Un módem de 56,000bps, transmite 7.0kbps.

2.4.1.4 ESTANDARES DE MODULACION

Dos módems para comunicarse necesitan emplear la misma técnica de modulación. La mayoría de los módems son full-dúplex, lo cual significa que pueden transferir datos en ambas direcciones. Hay otros módems que son half-dúplex y pueden transmitir en una sola dirección al mismo tiempo. Algunos estándares permiten sólo operaciones asíncronas y otros síncronas con el mismo módem. Veamos los tipos de modulación más frecuentes:
TIPO-CARACTERISTICAS
Bell 103 Especificación del sistema Bell para un módem de 300 baudios, asíncrono y full-dúplex.
Bell 201 Especificación del sistema Bell para un módem de 2,400bps, síncrono, y full-dúplex.
Bell 212 Especificación del sistema Bell para un módem de 2,400bps, asíncrono, y full-dúplex.
V.22 bis módem de 2,400bps, síncrono/asíncrono y full-dúplex.
V.29 módem de 4,800/7,200/9,600bps, síncrono y full-dúplex.
V.32 módem de 4,800/9,600bps, síncrono/asíncrono y full-dúplex.
V.32 bis módem de 4,800/7,200/9,600/7,200/12,000/14,400bps, síncrono/asíncrono y full-dúplex.
Hayes Express módem de 4,800/9,600bps, síncrono/asíncrono y half-dúplex. Sólo compatibles consigo mismo aunque los más modernos soportan V.32.
USR-HST módem de US Robotics de 9,600/14,400bps. Sólo compatibles consigo mismo aunque los más modernos soportan V.32 y V.32 bis.
Vfast es una recomendación de la industria de fabricantes de módem. La norma Vfast permite velocidades de transferencia de hasta 28,800bps.
V34 estándar del CCITT para comunicaciones de módem con velocidades de hasta 28,800 bps.

2.4.1.5 INTERFACES

La mayoría de los dispositivos utilizados para el procesamiento de datos tienen una capacidad limitada de transmisión de datos. Típicamente, generan una señal digital, como la NRZ-L, pudiendo transmitir a una distancia limitada. Consecuentemente, es extraño que dichos dispositivos (terminales y computadoras) se interconecten directamente a través de las utilidades que proporcionan la red de transmisión. La situación más habitual se muestra en la figura 79.

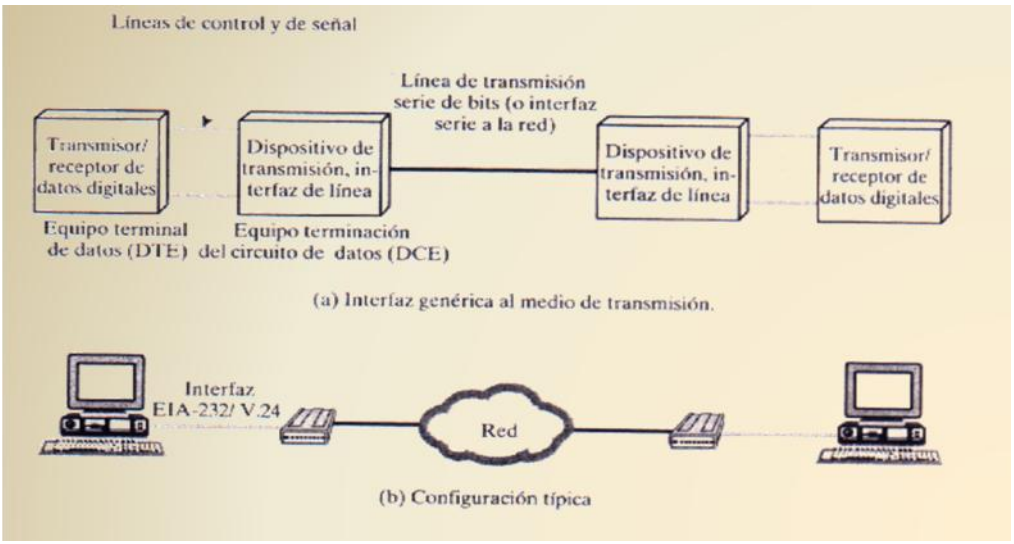


Figura 79

Los dispositivos considerados, normalmente terminales y computadoras se denominan **DTE** (**Data Terminal Equipment, Equipo Terminal de Datos**). El DTE utiliza el medio de transmisión a través del **DCE** (**Data Circuit-Terminating Equipment, Equipo de Terminación del Circuito de Datos**). Un ejemplo de esto último es un módem. Por un lado el DCE es responsable de transmitir y recibir bits, de uno en uno, a través del medio de transmisión o red. Por el otro, el DCE debe interaccionar con el DTE. En general, esto exige que se intercambien tanto datos como información de control. Esto se lleva a cabo a través de un conjunto de cables que se denominan circuitos de intercambio. Para que este esquema funcione, se necesita un alto grado de cooperación. Los dos DCE's que se intercambian señales a través de la línea de transmisión o red deben entenderse el uno con el otro. Es decir, el receptor de cada DCE debe usar el mismo esquema de codificación (por ejemplo Manchester o PSK) y la misma razón de datos que el transmisor del extremo. Además cada pareja DTE-DCE se deben diseñar para que funcionen tanto a los usuarios como a los fabricantes de equipos para el procesamiento de datos, se han desarrollado normalizaciones que especifican exactamente la naturaleza de la interfaz entre el DTE y el DCE. La especificación de la interfaz tiene cuatro características importantes:

- Mecánicas.
- Eléctricas.
- Funcionales.
- De procedimiento.

Las características de procedimiento están relacionadas con la conexión física entre el DTE y el DCE. Típicamente, los circuitos de intercambio de control y cable con un conector, macho o hembra, a cada extremo. El DTE y el DCE deben tener conectores de distinto género a cada extremo del cable. Esta situación es análoga al suministro de energía eléctrica. La energía se facilita a través de una toma de corriente o enchufe, y el dispositivo que se conecte debe tener el conector macho (con dos polos, dos polos con polaridad o tres polos) que corresponden a cada toma. Las características eléctricas están relacionadas con los niveles de tensión y su temporización. Tanto el DTE como el DCE deben usar el mismo código, deben usar los mismos niveles de tensión y deben utilizar la misma duración para los elementos de señal. Estas características determinan la razón de datos así como las máximas distancias que se puedan conseguir. Las características funcionales especifican la secuencia de eventos que se deben dar en la transmisión de los datos, basándose en las características funcionales de la interfaz. Los ejemplos que se dan a continuación pueden clarificar este concepto. Existen varias normalizaciones para la interfaz. En esta sección se presentan 2 de las más significativas:

- **V.24/EIA-232-E.-**La interfaz que más se utiliza es la especificada en el estándar V.24 de la UIT-T. De hecho, este estándar específica sólo los aspectos funcionales y de procedimiento de la interfaz; V.24 hace referencia a otros estándares para los aspectos eléctricos y mecánicos. En los Estados Unidos está la correspondiente especificación que cubre los cuatro aspectos mencionados: EIA-232. La correspondencia es:
  - Mecánicos: ISO 2110.
  - Eléctricos: V.28.
  - Funcionales: V.24.
  - De procedimiento: V.24.

  El EIA-232 fue establecido primeramente como RS-232 por la EIA (Electronic Industries Association) en 1962. Las versiones V.24 y V.28 se establecieron en 1993. Esta interfaz se utiliza para conectar dispositivos DTE a módems a través de líneas de calidad telefónica para ser utilizados en sistemas de telecomunicaciones analógicos públicos. También se utiliza en otras muchas aplicaciones de interconexión.
  - **Especificaciones mecánicas.-**En la Figura 80 se muestran las especificaciones mecánicas del EIA-232-E. para el que se usa un conector de 25 contactos metálicos distribuidos de una manera específica según se denomina en el ISO 2110. Este conector es el terminador del cable que va desde el DTE (la terminal) al DCE. En la práctica, en la mayoría de las aplicaciones se usa un número menor de circuitos.

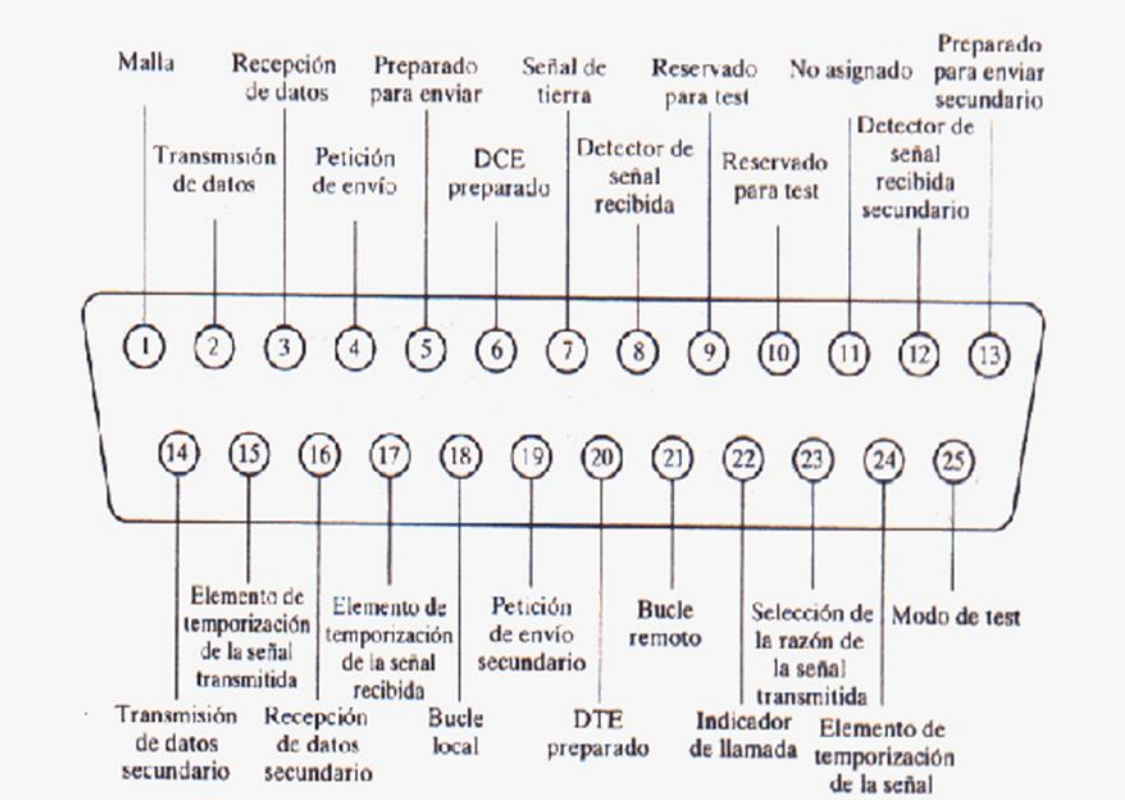


Figura 80

- **Especificaciones eléctricas.-**Aquí se define la señalización entre el DTE y el DCE. Se utiliza señalización digital en todos los circuitos de intercambio. Los valores eléctricos se interpretarán como binarios o como señales de control, dependiendo de la función del circuito de intercambio. Esta normalización específica que, respecto a una referencia de tierra común, una tensión menor de -3 volts se interprete como un “1” binario, mientras que una tensión mayor de 3 volts se interprete como un “0” binario. Esto corresponde al código NRZ-L. La interfaz se utiliza a una razón de menos de 20kbps para una distancia menor de 15 metros. Con un diseño adecuado se pueden conseguir mayores distancias y mayores razones de bits, pero es prudente suponer que estos límites funcionan tanto en la práctica como en teoría. Para las señales de control se aplican los mismos niveles de tensión: una tensión menor de -3 volts se interpreta como OFF y una tensión mayor de 3 volts se interpreta como ON, tabla 16.

V.24	EIA-232	NOMBRE	DIRECCION HACIA	FUNCION
SEÑALES DE DATOS				
103	BA	Transmisión de datos	DCE	Transmitidos por el DTE.
104	BB	Recepción de datos	DCE	Recibidos por el DTE.
118	SBA	Transmisión de datos secundario	DCE	Transmitidos por el DTE.
104	SBB	Recepción de datos secundario	DTE	Recibidos por el DCE.
SEÑALES DE CONTROL				
105	CA	Petición de envío	DCE	El DTE desea transmitir.
106	CB	Preparado para enviar	DTE	El DCE esta preparado para recibir; respuesta a la petición de envío.
107	CC	DCE preparado	DTE	El DCE esta preparado para funcionar.
108.2	CD	DTE preparado	DCE	El DTE esta preparado para funcionar.
125	CE	Indicador de llamada	DTE	El DCE esta recibiendo la señal de llamada por la línea.
109	CF	Detector de señal recibida	DTE	El DCE esta recibiendo una señal dentro de los límites apropiados de la línea.
110	CG	Detector de señal de calidad	DTE	Indica si la propiedad de error es alta en los datos recibidos.
111	CH	Selector de la razón de datos de la señal	DCE	Selecciona una entre dos razones de datos.
112	CI	Selector de la razón de datos de la señal	DTE	Selecciona una entre dos razones de datos.
133	CJ	Preparado para recibir	DCE	Control de flujo ON/OFF.
120	SCA	Petición de envío secundario	DCE	El DTE desea transmitir en el canal inverso.
121	SCB	Preparado para enviar secundario	DTE	El DCE esta preparado para recibir en el canal reverso.
122	SCF	Detector de señal recibida	DTE	Igual que el 109, pero por el canal reverso.
140	RL	Bucle remoto		Solicita al DCE remoto que devuelva las señales
141	LL	Bucle local	DCE	recibidas.
			DCE	Solicita al DCE que devuelva las señales recibidas.
142	DA	Modo de test	DTE	El DCE se pone en modo de test.
SEÑALES DE TEMPORIZACION				
113	TM	Temporización del elemento de señal de transmisión	DCE	Señales de reloj; aparecen señales a ON y OFF en el centro de cada señal.
114	DB	Temporización del elemento de señal transmitido	DTE	Señal de reloj; tanto el 113 como el 114 están relacionados con el circuito de la señal 103.
115	DD	Temporización del elemento de señal recibido.	DTE	Señal de reloj para el circuito 104.
TIERRA				
102	AB	Señal de tierra/retorno		Referencia de tierra común para todos los circuitos.

Tabla 16

- **Especificaciones funcionales**.-En la tabla 16 se resumen las especificaciones funcionales de los circuitos de intercambio, y en la figura 80 se muestran la localización de estos circuitos en el conector. Los circuitos se agrupan en los datos de control, los de temporización y los de tierra. Hay un circuito en cada dirección, por lo que se permite el funcionamiento full-dúplex. Es más, hay dos circuitos de datos secundarios que son útiles cuando el dispositivo funciona en semi-dúplex. En el caso de funcionamiento semi-dúplex, el intercambio de datos entre dos DTE's (a través de DCE's y el enlace de comunicaciones correspondiente) se realiza en un instante dado en una única dirección. No obstante, puede que se necesite enviar una petición de parada o un mensaje de control de flujo al dispositivo transmisor. Para llevar a cabo esto, el enlace de comunicaciones se dota de un canal en sentido inverso, normalmente a una razón de datos muy inferior que el canal primario. En la interfaz DTE-DCE el canal en sentido inverso se establece en una pareja de circuitos de datos independientes. Hay quince circuitos de control. Los 10 primeros, relacionados con la transmisión de datos sobre el canal primario, se listan el la tabla 16. Para transmisión asíncrona se utilizan seis de estos circuitos (105, 106, 107,108.2, 125, 109). La utilización de estos circuitos se explica en la subsección relativa a las especificaciones de procedimiento. Además de estos seis circuitos, en la transmisión síncrona se utilizan otros tres circuitos de control. El circuito detector de la calidad de la señal (Signal Quality Detector) se pone a 0N por el DCE para indicar que la calidad de la señal de entrada a través de la línea telefónica se ha deteriorado por encima de un determinado umbral. La mayoría de los módems de alta velocidad admiten más de razón de transmisión por lo que si la línea se vuelve ruidosa, con 0N se solicita reducir la

velocidad de transmisión. Los circuitos de selección de la razón de 1° señal de datos (**Data Signal Rate Detector**) se utilizan cambiar de velocidad; tanto el DTE como el DCE pueden comenzar la modificación. Los siguientes tres circuitos de control (120, 121, 122) se utilizan para controlar el uso del canal secundario, ya que puede ser utilizado como canal 1° de sentido inverso o para algún propósito auxiliar. El último grupo de señales de control esta relacionado con la verificación de la conexión entre el DTE y el DCE. Estos circuitos permiten que el DTE haga que el DCE realice un test de la conexión. Estos circuitos son útiles sólo si el módem o el DTE de que se trate permiten un bucle de control; si bien esto es últimamente una característica común de todos los módems. En la función de bucle local, la salida del transmisor del módem se conecta con la entrada del receptor, desconectando al módem de la línea de transmisión. Al módem se le envía una cadena de datos generados por el dispositivo del usuario que se devuelven al usuario formando un bucle. En el bucle remoto, el módem local se conecta a la línea de transmisión en la forma habitual, y la salida del receptor del módem remoto se conecta a la entrada del transmisor del módem. Durante los intervalos de test, el DCE pone a 0N el circuito de Modo de Test. En la Tabla 17 se muestran los valores de todos los circuitos que están relacionados con el bucle de test y en la figura 81 se muestra como se usan.

VALORES DE LOS CIRCUITOS EN BUCLE PARA V.24/EIA-232

BUCLE LOCAL

CIRCUITO	VALOR
DCE Preparado	ON
Bucle Local	ON
Bucle Remoto	OFF
Modo de Test	On

BUCLE REMOTO

CIRCUITO	INTERFAZ LOCAL	INTERFAZ REMOTA
DCE Preparado	ON	OFF
Bucle Local	OFF	OFF
Bucle Remoto	ON	OFF
Modo de Test	ON	ON

Tabla 17

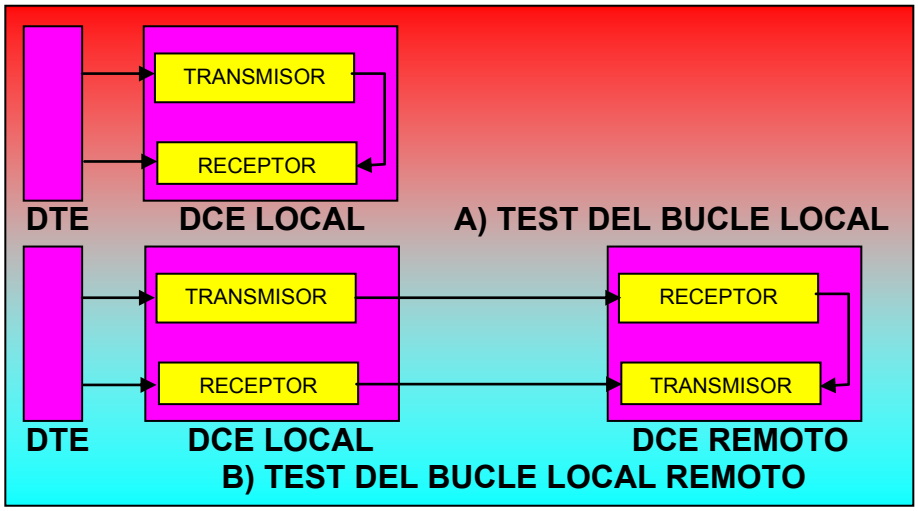


Figura 81

Las señales de temporización proporcionan los pulsos de reloj en la transmisión síncrona. Cuando el DCE envía datos síncronos a través del circuito de Recepción de Datos (l04), a la vez envía transiciones de “0” a “1” ó de “1” a “0” por el circuito de temporización del receptor (115), con transiciones en la mitad de cada elemento de señal del circuito de recepción de datos (BB). Cuando el DTE envía datos síncronos tanto el DTE como el DCE pueden proporcionar los pulsos de temporización, dependiendo de las circunstancias. Finalmente, la señal de retomo de tierra común (l02) sirve como un circuito de retorno para todos los circuitos de datos. Por tanto, la transmisión no esta balanceada, teniendo sólo un cable activo.

- **Especificaciones de procedimiento.-**Las características de procedimiento definen la sucesión de cómo se utilizan los diferentes circuitos en una aplicación determinada. Para tal fin, se pondrán algunos ejemplos. El primer ejemplo es muy habitual y se trata de la conexión de dos dispositivos una distancia corta dentro de un edificio, éstos se denominan módems de línea privada o módems de distancia limitada. Como su propio nombre indica, los módems de distancia limitada admiten señal del DTE, como por ejemplo, una terminal o una computadora, las convierte en señales analógicas y las transmite a una distancia corta a través de un medio, como por ejemplo un par trenzado. En el otro extremo de la línea hay otro módem de distancia limitada que acepta las señales digitales de entrada, las convierte a digital y las transfiere a la terminal o computadora remota. Se da por supuesto que el intercambio de información es en los dos sentidos. En esta aplicación se necesitan solamente los siguientes circuitos de intercambio:
    1) La señal de tierra (102).
    2) Transmisión de datos (103).
    3) Recepción de datos (l04).
    4) Petición de envío (105).
    5) Preparado para enviar (106).
    6) DCE preparado (107).
    7) Detector de señal recibida (109).

  Cuando el módem (DCE) se enciende y está listo para funcionar, activa la línea CE Preparado (aplicando una tensión negativa y constante). Cuando el DTE está preparado para enviar datos (por ejemplo, cuando el usuario de una terminal ha introducido un carácter), activará la línea Preparado para Enviar. El módem responde, cuando esté preparado, activando el circuito Preparado para Enviar. Si la transmisión es semi-dúplex, el circuito de Petición para enviar, a su vez, inhibe el modo de recepción. El DTE puede ahora transmitir datos a través de la línea de Transmisión de Datos. Cuando se reciben datos del módem remoto, el módem local activa la línea Detector de Señal Recibida para indicar que el módem remoto está transmitiendo, y además transfiere los datos a través de la línea Recepción de Datos. Obsérvese que no es necesaria la utilización de circuitos de temporización, ya que se trata de transmisión asíncrona. Los circuitos mencionados anteriormente son suficientes para los módems punto a punto sobre líneas privadas, no obstante para transmitir datos a través de una línea telefónica convencional se necesitan otros circuitos adicionales. En este caso, el que inicie la conexión debe llamar al destino a través de la red. Se necesitan dos circuitos adicionales:
    1) DTE Preparado (108.2).
    2) Indicador de Llamada (125).

  Con estas dos líneas adicionales, en módem DTE puede usar la red telefónica de una forma análoga a como se hace en una conversación convencional.

  Cuando se realiza la llamada, tanto manualmente como automáticamente, el sistema telefónico envía la señal de llamada. Un teléfono respondería a esta llamada haciendo sonar su timbre; un módem responde activando el circuito Indicación De Llamada. Una persona responde a la llamada descolgando el auricular; el DTE responde activando el circuito Terminal de Datos Preparado. Una persona que contestara una llamada escucharía la otra voz, y si no escuchar nada, colgaría. Un DTE intentara escuchar el Detector de Portadora, que será activado por el módem cuando una señal este presente; si este circuito no se activa, el DTE desactivará la Terminal de Datos Preparado. Nos podemos preguntar, ¿bajo que circunstancias puede darse este último caso? Una situación habitual es, por ejemplo, si una persona accidentalmente marca el número del módem, pero al no recibir portadora, el problema se resuelve como ya se ha indicado.
  Es ilustrativo considerar la situación en que la distancia entre los dispositivos sea tan pequeña que permita a los DTE's conectarse directamente. En este caso, los

circuitos de intercambio de V.24/EIA-232 se pueden usar, pero sin necesidad de usar DCE's. Para que este esquema funcione, se necesita una configuración de módem nulo, consistente en conectar los circuitos de tal manera que se engañe a ambos DTE's haciéndolos creer que están respectivamente conectados a un módem. En la figura 82 se muestra un ejemplo de configuración de módem nulo; el por qué de las conexiones particulares indicadas en la figura deben ser evidentes para el lector que haya seguido perfectamente los razonamientos anteriores.

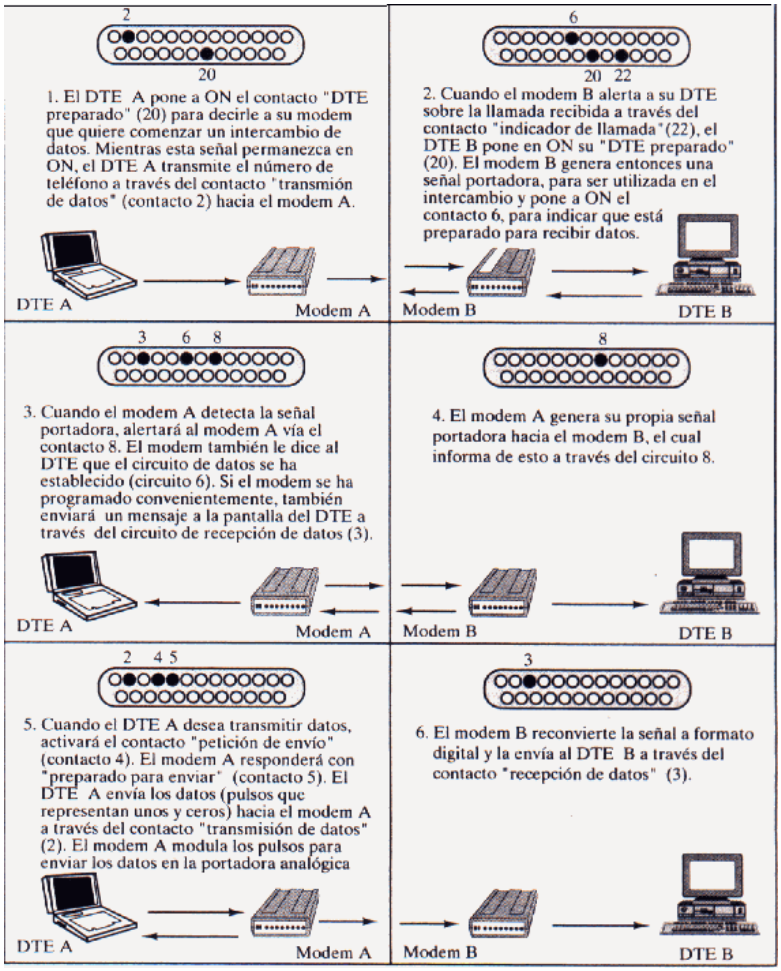


Figura 82

2.4.1.6 CODIFICACIÓN DE LA INFORMACIÓN

La información de la computadora se codifica siempre en unos y ceros, que son los valores elementales que la computadora es capaz de reconocer. La combinación de "1" y "0" permite componer números enteros y números reales. Los caracteres se representan utilizando una tabla de conversión. La más común de estas tablas es el código ASCII que utilizan las computadoras personales. Sin embargo existen otras y por ejemplo las grandes computadoras de IBM utilizan el código EBCDIC. La información codificada en binario se transmite entre las computadoras. En las conexiones por módem los bits se transmiten de uno en uno siguiendo el proceso descrito en el apartado modulación de la información. Pero además de los códigos originales de la información, los equipos de comunicación de datos añaden bits de control que permiten detectar si ha habido algún error en la transmisión. Los errores se deben principalmente a ruido en el canal de transmisión que provoca que algunos bits se mal interpreten. La forma más común de evitar estos errores es añadir a cada palabra (conjunto de bits) un bit que indica si el número de "1" en la

palabra es par o impar. Según sea lo primero o lo segundo se dice que el control de paridad es par o impar. Este simple mecanismo permite detectar la mayor parte de errores que aparecen durante la transmisión de la información. La información sobre longitud de la palabra (7 u 8 bits) y tipo de paridad (par o impar) es básica en la configuración de los programas de comunicaciones. Otro de los parámetros necesarios son los bits de paro. Los bits de paro indican al equipo que recibe que la transmisión se ha completado (los bits de paro pueden ser uno o dos).

2.4.1.7 ESTANDARES DE LA CORRECCIÓN DE ERRORES

El problema de ruido puede causar pérdidas importantes de información en módem a velocidades altas, existen para ello diversas técnicas para el control de errores. Cuando se detecta un ruido en un módem con control de errores, todo lo que se aprecia es una breve inactividad o pausa en el enlace de la comunicación, mientras que si el módem no tiene control de errores lo que ocurre ante un ruido es la posible aparición en la pantalla de caracteres "basura" o, si se esta transfiriendo un fichero en ese momento, esa parte del fichero tendría que retransmitirse otra vez. En algunos casos el método de control de errores está ligado a la técnica de modulación:

- Módem Hayes V-Serie emplea modulación Hayes Express y un esquema de control errores llamado Link Access Procedure-Modem (LAP-M).
- Módem US Robotics con protocolo HTS emplea una modulación y control de errores propios de US Robotics

Hay otras dos técnicas para control de errores bastante importantes:

- Microcom Network Protocol (MNP-1, 2, 3, 4).
- Norma V.42 (procedente del CCITT e incluye el protocolo MNP-4)
- Norma MNP 10. Corrección de errores recomendada para comunicaciones a través de enlaces móviles.

2.4.1.8 ESTANDARES DE LA COMPRESIÓN DE DATOS

La compresión de datos observa bloques repetitivos de datos y los envía al módem remoto en forma de palabras codificadas. Cuando el otro módem recibe el paquete, lo decodifica y forma el bloque de datos original. Hay dos técnicas para la compresión muy extendidas:

- **Microcom Network Protocol (MNP-5,7)**.-Este protocolo permite compresiones de dos a uno, es decir podemos enviar el doble de información utilizando la misma velocidad de modulación.
- **Norma V.42 bis (procedente del CCITT)**.-Con esta norma de compresión se consiguen ratios de 4:1.

Estas tasas son las máximas que se pueden conseguir. Las mejores tasas se consiguen con ficheros de tipo texto o gráficos generados por computadora. Si la información esta ya comprimida con alguna utilidad tipo arj o zip, estos protocolos no pueden ya comprimir más la información y en éstos casos, incluso se pierde capacidad. Si se envía información ya comprimida en la computadora, el módem ya no podrá comprimirla más, y en estos casos los protocolos de compresión perjudican el rendimiento del módem.

2.4.1.9 CONEXION RS-232 ENTRE PC Y MODEM

Los módems se conectan con la computadora a través de un puerto de comunicaciones del primero, figura 83 Estos puertos siguen común mente la norma RS-232. A través del cable RS-232 conectado entre la computadora y el módem estos sé comunican. Hay varios circuitos independientes en la interfaz RS-232. Dos de estos circuitos, el de transmisor datos (TD), y el de receptor de datos (RD) forman la conexión de datos entre la PC y el módem. Hay otros circuitos en la Interfaz que permiten leer y controlar estos circuitos. Vamos a ver como se utilizan estas señales para conectarse con el módem:

- **DTR (Data Terminal Read)**.-Esta señal indica al módem que la PC está conectada y lista para comunicar. Si la señal se pone a OFF mientras el módem esta en on-line, el módem termina la sesión y cuelga el teléfono.

- **CD (Carrier Detect)**.-El módem indica a la PC que esta on-line, es decir conectado con otro módem.
- **RTS (Request to send)**.-Normalmente en ON. Se pone OFF si el módem no puede aceptar más datos de la PC, por estar en esos momentos realizando otra operación.
- **CTS (Clear to send)**.-Normalmente en ON. Se pone OFF cuando la PC no puede aceptar datos del módem.

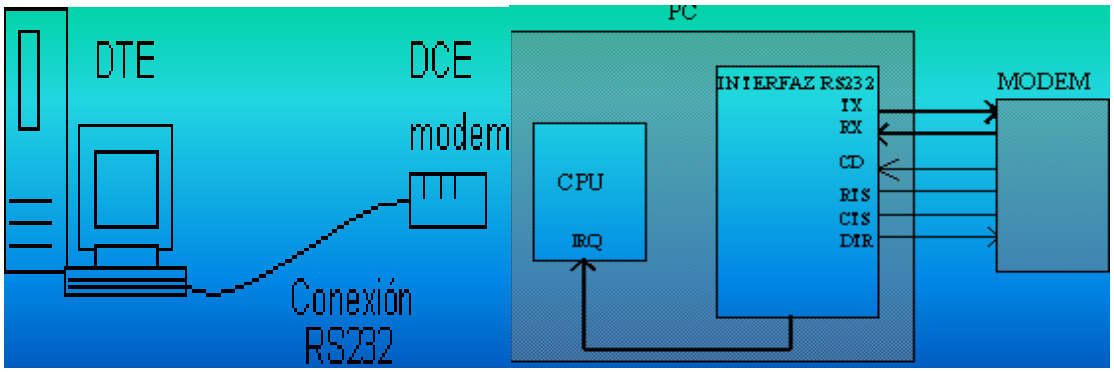


Figura 83

2.4.1.10 CONTROL DE FLUJO

El control de flujo es un mecanismo por el cual el módem y la computadora gestionan los intercambios de información. Estos mecanismos permiten detener el flujo cuando uno de los elementos no puede procesar más información y reanudar el proceso no más vuelve a estar disponible. Los métodos más comunes de control de flujo son:

- **Control de flujo hardware**.-RTS y CTS permiten a la PC y al módem parar el flujo de datos que se establece entre ellos de forma temporal. Este sistema es el más seguro y el que soporta una operación adecuada a altas velocidades.
- **Control de flujo software (XON/XOFF)**.-Aquí se utilizan para el control dos caracteres especiales XON y XOFF (en vez de las líneas hardware RTS y CTS) que controlan el flujo. Cuando a la PC quiere que el módem pare su envío de datos, envía XOFF. Cuando la PC quiere que el módem le envíe más datos, envía XON. Los mismos caracteres utilizan el módem para controlar los envíos de la PC. Este sistema no es adecuado para altas velocidades.

2.4.1.11 COMANDOS DE CONTROL DE MODEM

La mayoría de los módems se controlan y responden a caracteres enviados a través del puerto serie. El lenguaje de comandos para módem más extendido es de los comandos Hayes que fue inicialmente incorporado a los módems de este fabricante. Existen dos tipos principales de comandos:

- Comandos que ejecutan (ATD marcación, ATA contestación o ATH desconexión)
- Comandos que cambian algún parámetro del módem (por ejemplo ATS7=90)

2.4.1.12 MODOS DE OPERACION DEL MODEM

El módem tiene dos modos de funcionamiento:

- El módem esta en estado de comandos el módem responde a los comandos que envíala computadora. En este modo es posible configurar el módem o realizar las operaciones de marcado y conexión. Antes de que se puedan enviar un comando al módem este debe estar en el "estado de comandos".
- Cuando el módem se conecta con otro módem pasa al modo en línea. En este modo cualquier información que reciba de la computadora será enviada al módem distante. En este modo el módem no procesa la información y simplemente la trasmite a través de la

línea de comunicación. Para salir del modo en línea y pasar de nuevo al modo comandos se envía al módem +++ (petición de atención) precedidos por un segundo de inactividad.

2.4.1.13 NUEVAS TECNOLOGÍAS

2.4.1.13.1 NUEVAS TECNOLOGÍAS DE MODEMS A 56 KBPS

Los modelos de 56kbps permiten obtener información de Internet de una manera más rápida, acelerando las transmisiones de datos que usted necesite de la red. Esta tecnología requiere de líneas telefónicas digitales en el lado del proveedor Internet, lo cual reduce el ruido. Este tipo de módem es asimétrico, esto quiere decir que la velocidad de transmisión es diferente a la de recepción: mientras que puede obtener 56kbps en el flujo de datos desde el proveedor de servicio hacia el usuario, la transmisión del usuario hacia el proveedor se limita a 33.6kbps como máximo. Puesto que en una conexión de Internet típica la recepción representa el 85% del tráfico, se obtendrán mejoras contra un módem de 33.6 kbps. Sin embargo, existen condiciones que deben cumplirse para que su módem pueda enlazarse a estas velocidades. De no cumplirse alguna de estas, la velocidad máxima de transferencia se limitará a 33kbps o menos. A continuación se describen dichos requisitos:

- Su línea telefónica debe estar conectada a una central telefónica digital.
- No debe haber ninguna conversión en el formato de la codificación de la línea. Esto significa que posiblemente algunas líneas que pasan por conmutador no puedan alcanzar la velocidad deseada.
- El módem debe ser compatible con la tecnología V.90 (K56Flex). Este último punto es sumamente importante, ya que por ser ésta una tecnología x2 de la compañía U.S. Robotics y K56Flex, lo cual significa que si usted cuenta con un módem del tipo x2 su velocidad quedará limitada a 33.6 kbps. Si planea adquirir un módem de 56kbps, es altamente recomendable que seleccione uno que pueda ser actualizable a V.90, así no tendrá problemas de conexión con esta nueva tecnología.

2.4.1.13.2 MODEM INALÁMBRICOS, TENDENCIA DE LOS MODEMS PCS

Ahora los nuevos usuarios de la tecnología móvil tendrán acceso a redes de transmisión de datos a través de dispositivos instalados en sus laptops. Estos dispositivos son los modelos PCS los cuales son desarrollados para que funcionen en un ambiente de redes móviles. Lo que más destaca de esto es que se tendrá una red que cubrirá todo el globo y cualquier persona en cualquier lugar del mundo podrá enviar y recibir correo electrónico, faxes, etc., a cualquier lugar y a cualquier usuario que este en la red. Las redes inalámbricas existentes son propietarias, es decir no existe un organismo que las regule de forma de establecer estándares, cuando esto se haga será el primer paso para la globalización de este tipo de redes. Uno de los factores limitantes para estar conectado a través de módems inalámbricos es que solamente pocos módems se encuentran disponibles, y el costo de estos dispositivos es elevado cuando se compara con los módems convencionales. Existen otros factores también, pero mientras las redes inalámbricas no expandan su alcance, el software se encuentre disponible y más usuarios potenciales decidan que es hora de utilizar la tecnología inalámbrica, existirá la dificultad para que los usuarios potenciales encuentren que hacer con los nuevos módems inalámbricos y quien los distribuye. En la actualidad existen diferentes tipos de fabricantes de modelos PCS, pero basados en la misma tecnología, es decir se están diseñando de una vez con una tecnología compatible de forma de no tener ningún problema a la hora de implementar sistemas globales de transmisión inalámbrica. Los sistemas de transmisión inalámbricos más utilizados son los basados en los sistemas celulares, los cuales cubren la mayoría de los centros poblados en las ciudades más importantes a nivel mundial. Los módems utilizados por este tipo de tecnología tienen las siguientes características:

- Interfaz DTE: PCMCIA (TIPEII).
- Se basan en los comandos AT.
- Se pueden transmitir y recibir correo electrónico y faxes donde quiera, siempre y cuando exista roaming del operador celular al cual se está suscrito.

- Tiene comunicación Full-dúplex o Half-dúplex, dependiendo de la calidad de la tarjeta.
- Velocidad de transmisión: 9,600bps máximo.
- La conexión se realiza desde la tarjeta conectada a la laptop, directamente al teléfono celular a través de un cable.

Existen otros tipos de módems los cuales están diseñados también para instalarlos a una laptop directamente al puerto PCMCIA, pero este no se conecta a un teléfono celular, este esta conectado a un sistema de radiofrecuencias, es decir, se conecta directamente a una red privada a través de los siguientes componentes: la tarjeta que se conecta a la laptop, la antena de RF y la red inalámbrica a la cual la persona se suscribe. La empresa Motorola es la líder en la fabricación de este tipo de dispositivos inalámbricos los cuales tienen las siguientes características:

- Status Send II: es una aplicación de los módems de la serie 500 para funciones de telemetría sin periféricos adicionales. Con esta característica, nuevos puertos seriales bidireccionales le permiten a los módems comunicarse con dispositivos seriales, de esta forma se pueden tener dispositivos de monitores directamente conectado a estos módems sin que interfiera con su capacidad de transmisión.
- Diagnósticos internos: esta característica le permite a los fabricantes realizar pruebas de los módems sin desensamblar el producto, incluyendo pruebas de capacidad de recepción y memoria del dispositivo y establecen las frecuencias de transmisión y recepción.
- Ciclo útil de transmisión elevado: el tiempo de transmisión es elevado de 5% a 20%, permitiendo frecuentes reportes de estatutos.

Motorola está dirigiendo sus estrategias de mercadeo a mercados corporativos donde se verá la aceptación del gran potencial que ofrece la tecnología inalámbrica de paquetes de datos. Estos esfuerzos de mercadeo están dirigidos a mercados que tengan la necesidad de alternativas inalámbricas referentes a sus tradicionales métodos de conducir sus negocios en el campo de trabajo. Motorola anuncio montó una red de datos inalámbrica en Indonesia, de manera de proveer un sistema para comunicaciones móviles de datos en dos vías. El sistema DataTAC, el cual será el que se instaló en Indonesia, permitió transferencia electrónica de fondos y transacciones de puntos de ventas tales como autorizaciones de tarjetas de crédito on-line. El sistema también permitió acceso de correo electrónico, mensajes, acceso a bases de datos, despacho automático y mantenimiento de campo móvil para ventas y servicio de soporte técnico sin la necesidad de conectarse a una línea telefónica. Las laptops y terminales de datos pueden comunicares remotamente con redes corporativas y usuarios móviles sobre la red DataTAC utilizando un **Messenger Wireless Módem Card**, un módem inalámbrico de la serie 500 o un 660 Mobile Radio Módem, los dos de Motorola. Esta red opera a una velocidad de 19.2kbps. Como se observa los módems PCS todavía no han sido desarrollados para adaptase a una red global pública, sin embargo las redes privadas inalámbricas se están expandiendo para que los usuarios puedan acceder a sus servicios de valor agregado en cualquier lugar del planeta. Las redes de datos implantadas en la actualidad se sitúan en dos continentes específicamente: América y Europa. En USA están funcionando actualmente varias redes privadas inalámbricas, una de ellas pertenece a Motorola y la otra es manejada por Ericcson La primera es conocida como ARDIS, esta cubre a más de 10,700 ciudades en USA, Islas Vírgenes, ciudades urbanas en Alaska, Hawaii, Puerto Rico. Las empresas Bell de Canadá proveen alcance de la red ARDIS en Canadá.

La red utiliza dos tipos de protocolos de comunicación: el MDC4800 para velocidades de 4,800 bps y RDLAP (Radio Data-Link Access Protocol) para la velocidad de 19,200 bps. La tarjeta utilizada para esta red es la IBM ARDIS Módem, la cual se basa en estándares de PCMCIA y es compatible con los dos protocolos de comunicaciones utilizados para esta red. Para la laptop IBM ThinkPAD IBM ofrece una versión de este módem el cual se puede instalar en el lugar que ocupa el floppy. La potencia de RF de este dispositivo es de 0.8 watts. Este módem es distribuido con un software llamado ARDIS Personal Messaging, esta es una aplicación gráfica que provee conectividad para mensajería, paging, fax. Los mensajes son entregados tan pronto como el receptor del módem es puesto en operación y la aplicación de software es activada.

Otra red es la RAM Mobile Data Network, la cual es manejada por Ericsson. Según Ericcson esta red cubre más de 7,700 ciudades en USA, con una penetración de un 90% en las ciudades urbanas industrializadas. La tarjeta para esta red también la distribuye IBM y tiene las siguientes características: Es una tarjeta PCMCIA tipo III con una extensión que termina en la antena y la batería. La potencia de RF es de 2 watts. El software de aplicación para esta tarjeta es llamado RAD I/O y RAD AT, ambos proveen una interfaz gráfica, pero el segundo ofrece un set de instrucciones basados en los comandos estándar AT, que utilizan los módems convencionales. Como ejemplo de este tipo de módems observa la figura 84.

Figura 84

Aquí se observa una tarjeta PCMCIA US ROBOTIC, esta también es utilizada para las redes RAM. Una de las características más importantes de estas redes es que manejan el roaming de forma como se maneja el de telefonía celular, es decir a medida que el usuario se mueva, el sistema va adaptando la señal a la frecuencia correspondiente al sitio donde se encuentre, sin que pueda ser detectado ningún cambio en la señal. Esta red también estará en la capacidad de dejar entrar a sus usuarios a la Intranet corporativa de la compañía donde laboran, estableciendo así VPN's lo que implica un gran avance en las comunicaciones de los frecuentes viajeros de las empresas a un costo relativamente bajo, en comparación a tener que hacer una llamada internacional cada vez que quiera, por ejemplo, acceder la base de datos de la compañía para consultar los precios de los productos que distribuye. Otra característica importante de este tipo de redes es que no habrá tiempo de conexión, es decir se estará conectado constantemente a la red siempre y cuando la computadora, el módem y el software de interfaz estén encendidos. Se están diseñando tarjetas de forma que soporten navegación a través del World Wide Web, esto se hace más que todo mirando a futuro debido a que todavía no se ha desarrollado una red que interconecte a todas las que son propietarias y conectarlas a Internet. Estas redes privadas ofrecen acceso a Internet como un valor agregado, siendo lo principal la conexión a la red, es decir, la forma de conectarse pasará a un segundo plano. Motorola a través de su proyecto Iridium planea montar la red que es posible que se convierta en la líder de todas estas redes privadas. Construirá una red espacial la cual soportará acceso a nivel mundial, acceso on-demand, servicios de comunicación de voz y datos, etc.. La red tiene un costo estimado de 3.8 billones de dólares y operará con 66 satélites de baja órbita que rodearán la superficie de la tierra con enlaces de comunicación inteligentes. La configuración de este tipo de red sería algo como esto:
Aquí el sistema de satélites está representado por un sólo satélite y existen hosts así como computadoras portátiles conectadas a la red. Con esta red Motorola pasará a ser el líder y la competencia de alguna u otra forma se tendrá que adaptar a esta red la cual será más robusta y tendrá un mayor alcance que cualquier red jamás concebida. La cuestión es si tendrá el auge que los directivos de Motorola esperan que tenga o las redes más pequeñas seguirán funcionando sin ningún problema debido a que existen usuarios que prefieren estar conectados a una pequeña red debido al radio de acción que esperan tener.

2.4.2 EL MODELO CLIENTE –SERVIDOR

2.4.2.1 INTRODUCCION

En el modelo cliente-servidor, los usuarios trabajan en computadoras denominadas **sistemas frontales (front-end)** e interaccionan con sistemas servidores denominados **posteriores (back-end)** que proporcionan servicios, tales como el acceso a una base de datos, la gestión de red y el almacenamiento de archivos. Una red de computadoras ofrece la plataforma de comunicación en la que numerosos clientes pueden actuar con uno o más servidores. La interacción entre la aplicación que ejecutan los usuarios en el front-end y el programa (generalmente una base de datos o un sistema operativo de red) en el back-end se denomina relación cliente-servidor. Esto implica que el usuario dispone de una computadora con su propia capacidad de procesamiento, que ejecuta un programa que puede efectuar la interacción con el usuario y la presentación de la información. En el modelo cliente-servidor, el sistema cliente ejecuta una aplicación que interacciona con otro programa que se ejecuta en el servidor. El modelo cliente-servidor se aplica en sistemas operativos y aplicaciones. Los sistemas operativos de red, como NetWare de Novell están orientados a este modelo, puesto que los usuarios situados en las estaciones de trabajo realizan peticiones a los servidores NetWare. El cliente ejecuta un programa que redirecciona las peticiones de obtención de los servicios de la red al servidor adecuado, además de enviar las peticiones de servicios locales al sistema operativo local. En los sistemas gestores de bases de datos que siguen el modelo cliente-servidor, los clientes realizan las consultas a través de una aplicación front-end que atienden los servidores.

En una relación cliente-servidor el procesamiento se divide entre las dos partes. El sistema cliente ejecuta una aplicación que muestra una interfaz de usuario. Da formato a las peticiones de los servicios de la red y muestra la información o los mensajes enviados por el servidor. El servidor realiza el procesamiento posterior, como por ejemplo una clasificación de datos a la realización de un informe. Debido a que los datos se encuentran perfectamente accesibles, el cliente realiza este proceso de forma eficiente. Después de la clasificación, realización del informe o de cualquier otra tarea solicitada por un usuario, el servidor envía los resultados al cliente. El tráfico en la red se reduce debido a que el cliente únicamente obtiene la información que solicito, no todo el conjunto de datos para clasificar, según el ejemplo anterior. Los servidores en un entorno cliente-servidor son a menudo potentes sistemas superservidores, minicomputadoras o computadoras centrales, capaces de gestionar adecuadamente las múltiples y simultáneas peticiones que reciben de los clientes, además de realizar tareas de seguridad y de gestión de la red. Algunas organizaciones han reemplazado sus computadoras centrales, que proporcionaban cinco millones de instrucciones por segundo (MIPS, Millón Instructions Per Second), por un grupo de servidores capaces de ejecutar 1,000 MIPS. Las diversas estrategias cliente-servidor ofrecen una forma de crear plataformas informáticas relativamente asequibles y fáciles de configurar según las necesidades específicas de las aplicaciones. El software de un sistema cliente-servidor habitualmente consiste de un sistema gestor de bases de datos **(DBMS, Data Base Management System)** instalado en un servidor back-end, hacia el que los clientes dirigen sus peticiones a través de un lenguaje de consulta estructurado **(SQL, Structured Query Language)**. Es particularmente deseable disponer de un sistema de procesamiento de transacciones interactivo **(OLPT, On-line Transaction Processing)** en el modelo cliente-servidor. Mientras que los servidores de archivos y los servidores de bases de datos son más comunes, un servidor back-end también puede proporcionar comunicaciones dedicadas y servicios de impresión.

2.4.2.2 ARQUITECTURA CLIENTE-SERVIDOR

La arquitectura cliente-servidor define una relación entre el usuario de una estación de trabajo (el front-end) y un servidor back-end de archivos, impresión, comunicaciones o fax u otro tipo de sistema proveedor de servicios. El cliente debe ser un sistema inteligente con su propia capacidad de procesamiento para descargar en parte al sistema back-end (esta es la base del modelo cliente-servidor). Esta relación consiste en una secuencia de llamadas seguidas de respuestas. Situar

servicios de archivos (u otro tipo de servicios) en sistemas back-end dedicados tienen muchas ventajas. Es más sencillo realizar el mantenimiento y la seguridad de unos servidores situados en un mismo lugar, y más simple el proceso de realización de copias de seguridad, siempre que los datos se encuentren en una única ubicación y una misma autoridad los gestione.

Existen numerosas configuraciones cliente-servidor posible. En la figura 85 varios clientes acceden a un único servidor, Esta es la configuración usual de una pequeña red de área local.

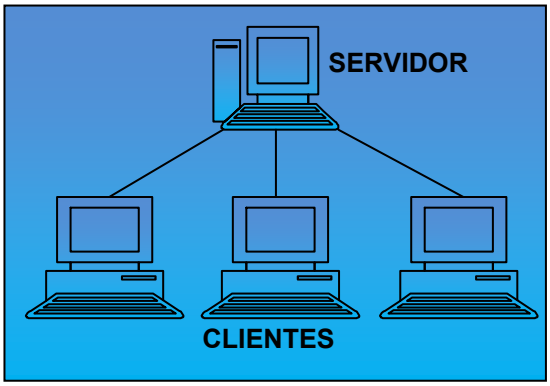
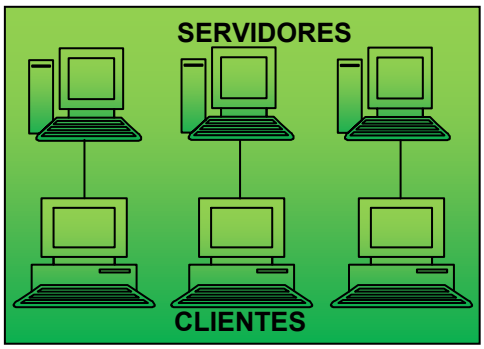


Figura 85 Configuración cliente/servidor con un único servidor



La figura 86 representa un modelo de base de datos distribuida en el que los clientes acceden a los datos ubicados en varios servidores.

Figura 86 Configuración cliente/servidor con servidores distribuidos

En un entorno de red par a par, tal como Windows para trabajo en grupos de Microsoft, NetWare Lite, LANtastic de Artisoft, o NFS (Network File System), las estaciones de trabajo pueden ser tanto clientes como servidores, figura 87. Un usuario puede compartir los archivos ubicados en su disco duro con otros usuarios de la red. Así, la estación de trabajo de dicho usuario se convierte en un servidor de otro cliente. Al mismo tiempo, nuestro usuario puede acceder como cliente a los archivos compartidos de otras estaciones de trabajo.

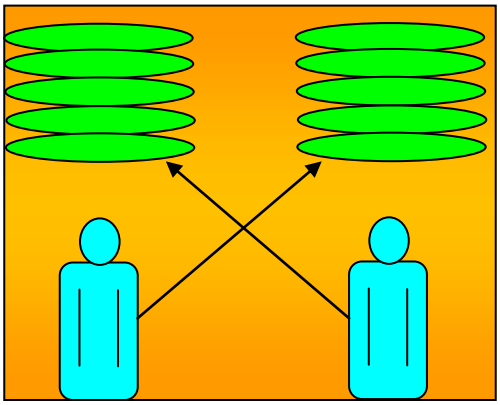


Figura 87 Configuración cliente/servidor entre pares

Internamente, el cliente y el servidor se dividen en varios procesos, representados en la figura 88. Hay que tener en cuenta que el software de redirección de los clientes determinan si las peticiones de los clientes van dirigidas hacia un servicio local o hacia un servidor de red.

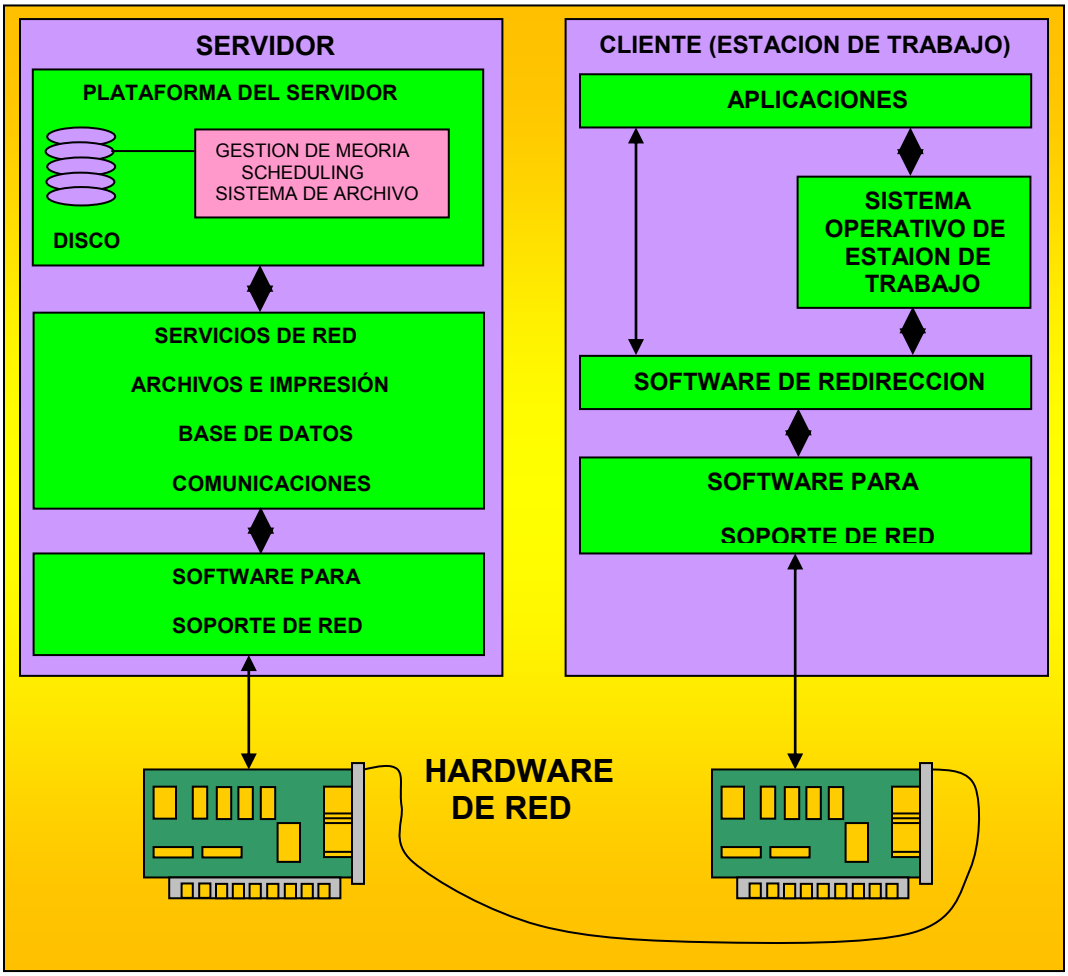


Figura 88 Relación cliente/servidor

En función del sistema operativo o de la aplicación, existen variaciones en la cantidad de trabajo que realiza el servidor. En algunos casos, el servidor realiza el menor trabajo posible con objeto de optimizar sus prestaciones hacia un grupo de clientes en aumento continuo. En otros casos, el servidor trabaja con toda su potencia y gestiona la mayor parte de procesamiento. Servidores de acceso centralizado se denominan servidores de empresa. Los servidores también pueden situarse en lugares remotos, de modo que los usuarios deben acceder a ello a través de un enlace de telecomunicaciones. En función del tipo de enlace utilizado, el tiempo de respuesta entre el cliente y el servidor remoto puede ser considerable.

2.4.2.3 EL CLIENTE

El usuario genera una petición en el front-end. El cliente ejecuta una aplicación que:

- Presenta una interfaz al usuario.
- Formatea las peticiones de datos.
- Muestra los datos recibidos del servidor.

En un entorno cliente-servidor el servidor no contiene el software de interfaz de usuario. El cliente es responsable de presentar los datos en un formato que resulte útil. El usuario introduce las instrucciones desde el equipo cliente. El equipo cliente prepara la información para el servidor. El equipo cliente envía una información específica a través de la red. El servidor procesa la petición, localiza la información adecuada y la devuelve al cliente a través de la red. El equipo cliente envía entonces la información a la interfaz, que representa la información al usuario. El equipo cliente también puede procesar adicionalmente la información, utilizando su propio CPU y software.

2.4.2.3.1 USO DEL FRONT-END

Los front-end pueden presentar a los usuarios la misma información de formas distintas, dependiendo de la petición.

2.4.2.3.2 HERRAMIENTAS DEL FRONT-END

Existen varias herramientas, aplicaciones y utilidades disponibles para el front-end para hacer que el proceso cliente-servidor sea más eficiente. Estas herramientas incluyen:

- **Herramientas de consulta**.-Estas herramientas utilizan consultas predefinidas y capacidades propias de generación de informes para ayudar a que los usuarios accedan a datos del servidor.
- **Aplicaciones de usuario**.-Microsoft Excel, pueden ofrecer acceso front-end a bases de datos situados en servidores. Microsoft Access, incluyen su propio SQL para ofrecer una interfaz para sistemas de gestión de bases de datos de diversos fabricantes.
- **Herramientas de desarrollo de programas**.-Se dispone de herramientas de desarrollo de programas, Visual Basic, para ayudar a los programadores a desarrollar herramientas front-end para acceder a datos de servidores.

2.4.2.4 EL SERVIDOR

El servidor se dedica a almacenar y gestionar datos. El servidor también es denominado como el back-end del modelo cliente-servidor porque responde a las peticiones del cliente. El servidor recibe las peticiones estructuradas de los clientes, las procesa y envía la información solicitada al cliente de nuevo a través de la red. El procesamiento back-end incluye la ordenación de los datos, la extracción de los datos solicitados y la devolución de los datos al usuario. El software servidor gestiona los datos de una base de datos, incluyendo operaciones de:

- Actualización.
- Inserción.
- Seguridad.

2.4.2.4.1 PROCEDIMIENTOS ALMACENADOS

Los procedimientos almacenados son pequeñas rutinas de procesamiento de datos preescritas que ayudan a los detalles del procesamiento de datos. Los procedimientos son almacenados en el servidor, y pueden ser usados por el cliente. Los procedimientos almacenados ayudan a procesar los datos. Un procedimiento almacenado puede ser usado por cualquier número de clientes, evitando la necesidad de incorporar la misma rutina en el código de cada programa.

- Realizan parte del procesamiento llevado a cabo generalmente en el cliente.
- Reduce el tráfico de la red.
- Pueden incluir controles de seguridad para evitar que usuarios no autorizados ejecuten algunos de los procedimientos.

2.4.2.4.2 HARDWARE DEL SERVIDOR

Deben ser potentes y rápidos. Además de un procesador de alta velocidad, necesitan gran cantidad de RAM y de espacio en unidades de disco. Deben ser capaces de gestionar:

- Múltiples peticiones.
- Seguridad.
- Tareas de gestión de la red.

2.4.2.5 VENTAJAS DE LA ARQUITECTURA CLIENTE-SERVIDOR

El modelo cliente-servidor ayuda a las organizaciones a redimensionarse a partir de sus computadoras centrales y minicomputadoras hacia servidores y estaciones de trabajo sobre LAN,

que se constituyen así como plataformas de comunicaciones corporativas. La carga de trabajo asociada a las aplicaciones se divide entre las distintas computadoras. Los sistemas cliente realizan parte del procesamiento, que se distribuye sobre todos los sistemas de escritorio. Los sistemas servidores realizan la distribución de la información centralizada hacia unidades de almacenamiento conectados directamente hacia ellos, reduciéndose así la información que envía a través de la red. Un porcentaje importante de información se ubica directamente en la memoria del servidor, no en la memoria de cada estación de trabajo que lo necesite. El tráfico en la red se reduce, ya que el servidor envía al cliente únicamente la información solicitada, no grandes bloques de información que deba procesar. Los grandes sistemas servidores pueden descargarse de aplicaciones que se gestionan mejor en estaciones de trabajo personales. Los datos están más seguros si su ubicación es única. Los sistemas de almacenamiento de datos proporcionan una forma de suministrar datos específicos a servidores de grupos de trabajo, al mismo tiempo que mantienen control sobre aquellos. En un almacenamiento centralizado de datos, los administradores pueden aplicar controles de seguridad para restringir el acceso a los datos y utilizar mecanismos de supervisión de dicho acceso. El entorno cliente-servidor favorece el procesamiento paralelo múltiple. En este esquema, numerosas computadoras cooperan para realizar una tarea de procesamiento de forma conjunta. Cada sistema realiza una parte de la tarea, combinándose los resultados. La tarea se completa más rápidamente que si fuera realizada por un sistema autónomo.

2.4.2.6 INPLANTACION DE APLICACIONES CLIENTE-SERVIDOR

En un entorno distribuido de red, el objetivo es proporcionar datos de forma compartida a todos los usuarios de la organización. La realización de un entorno compartido de datos engloba normalmente las siguientes funciones:

- **Medidas de seguridad**.-Necesarias para el control de acceso a los datos.
- **Medidas de integridad**.-Requeridas para asegurar que las transacciones se realizan o no en función de su corrección.
- **Medidas de concurrencia y disponibilidad**.-Necesarias para permitir a los usuarios acceder y actualizar los datos.
- **Necesidad de seguridad y recuperabilidad de los datos**.-Mediante copias de seguridad y utilerías de tolerancia a fallas.

Los servidores deben proporcionar acceso a los datos, pero también preocuparse de la concurrencia en dicho acceso.

2.4.2.7 SERVIDORES ESPECIALIZADOS

2.4.2.7.1 SERVIDORES DE ARCHIVOS E IMPRESIÓN

Los servidores de archivo e impresión gestionan el acceso de los usuarios y el uso de recursos de archivos e impresión. Los servidores de archivos e impresión se utilizan para el almacenamiento de archivos y datos.

2.4.2.7.2 SERVIDORES DE APLICACIONES

En un servidor de aplicaciones, la base de datos permanece en el servidor y sólo se envían los resultados de la petición a equipo que realiza la misma.

2.4.2.7.3 SERVIDORES DE CORREO

Los servidores de correo funcionan como servidores de aplicaciones, en el sentido de que son aplicaciones servidor y cliente por separado, con datos descargados de forma selectiva del servidor a cliente.

2.4.2.7.4 SERVIDORES DE FAX

Los servidores de fax gestionan el tráfico de fax hacia el exterior y el interior de la red, compartiendo una o más tarjetas módem fax.

2.4.2.7.5 SERVIDORES DE COMUNICACIONES

Los servidores de comunicaciones gestionan el flujo de datos y mensajes de correo electrónico entre las propias redes de los servidores y otras redes, equipos mainframes o usuarios remotos que se conectan a los servidores utilizando módems y líneas telefónicas.

2.4.2.7.6 SERVIDORES DE SERVICIO DE DIRECTORIO

Los servidores de servicios de directorio permiten a los usuarios localizar, almacenar y proteger información en la red. Por ejemplo, cierto software servidor combina los equipos en grupos locales (llamados dominio) que permiten que cualquier usuario de la red tenga acceso a cualquier recurso de la misma. La planificación para el uso de servidores especializados es importante con una red grande. El planificador debe tener en cuenta cualquier crecimiento previsto de la red, para que el uso de esta no se vea perjudicado si es necesario cambiar el papel de un servidor específico.

2.4.4 SNA (SYSTEM NETWORK ARCHITECTURE)

2.4.4.1 INTRODUCCION

En Septiembre de 1973 la multinacional IBM presentó **SNA** (**System Network Architecture**), lo que constituye su red distribuida de comunicación y proceso de datos. Esta arquitectura nació para compatibilizar en un entorno de comunicaciones de datos todos los diversos equipos, integrándolos en un sólo sistema. Antes de que apareciera SNA, IBM tenía múltiples productos de comunicación, utilizando 35 métodos de acceso de teleproceso, con más de una docena de protocolos de enlace. La idea, al crear SNA, consistió en eliminar este caos y proporcionar una infraestructura coherente para el proceso distribuido débilmente acoplado. Su primera versión en el año 1974 sólo permitía redes centralizadas, es decir, redes en forma de árbol con un sólo host. Tras unos comienzos lentos, en 1976 ya permitía tener varios hosts con sus respectivos árboles, con la posibilidad de comunicaciones entre esos árboles a través de sus raíces, ese año existían unas 350 instalaciones basadas en SNA. A finales de 1978 principios de 1979 existían unas 1,250 instalaciones y se había conseguido eliminar la restricción anterior, teniendo la capacidad para poder comunicarse de manera más general y no sólo a través de sus raíces. Ya en 1980 se superaban las 2,500 instalaciones y en 1985 se incluyó la aparición de topologías arbitrarias de hosts y LAN. El modelo OSI se configuró tomando como base a la SNA, incluyendo el concepto de estratificación, número de capas y sus funciones aproximadas. SNA es una arquitectura de red que permite que los clientes de IBM construyan sus propias redes privadas. Un banco, por ejemplo, puede tener una o más CPU’s en un departamento y numerosas terminales en cada una de sus sucursales. Con el uso de SNA todos estos componentes aislados pueden transformarse en un sistema coherente. La arquitectura SNA resulta más complicada de lo que debiera haber sido, ya que los clientes iniciales de IBM deseaban mantener la compatibilidad de los programas anteriores al nacimiento de SNA, por eso SNA nació ya, con ciertas limitaciones.

2.4.4.2 CONCEPTOS GENERALES

La documentación de IBM dice "el SNA es una amplia especificación para redes distribuidas de procesamiento de datos. Define los formatos de mensajes usados en una red y define las reglas que gobiernan la interacción entre los componentes de la red". El SNA como arquitectura, identifica y define los posibles elementos dialogantes de una red y describe los protocolos que deben regir su diálogo. Dichos protocolos consisten en unos formatos de información a intercambiar y las reglas que deben seguir los interlocutores. Ello implica, a parte de los formatos, unas funciones de

establecimiento y terminación del diálogo, control del flujo de datos, así como procedimientos para detectar y corregir cualquier tipo de error. Tales funciones vienen también definidas en la descripción formal del SNA. Esta arquitectura es independiente de productos y arquitecturas hard/software y en continua evolución. En realidad, se desarrollaron dos formas de SNA:

- Subáreas (SNA Clásico), manejada por una estructura principal.
- APPN (nueva SNA), basada en redes de minicomputadoras.

En su diseño original esta red resultó cara, puesto que la idea era centrar las redes de comunicaciones en minicomputadoras dirigidas por una computadora central mainframe. Las minicomputadoras corrían en un sistema especial llamado NCC. Cada NCC dirige una comunicación en nombre de todas las terminales, estaciones de trabajo y PC's conectados a ella. Por ejemplo: en una red de bancos, la NCC podría dirigir todas las terminales y máquinas de una sucursal en un área metropolitana específica. El tráfico es dirigido entre las máquinas NCC y eventualmente en la estructura central.

La estructura principal estaba a cargo de un producto IBM llamado **VTAM (Virtual Telecomunications Access Meted Método de Acceso Virtual de Telecomunicaciones)**, que controla la red. Aunque los mensajes individuales de un NCC a otro corren sobre la línea telefónica, VTAM mantiene una tabla de todas las máquinas y enlaces telefónicos de la red. Selecciona las rutas y los caminos alternativos que los mensajes pueden tomar entre los distintos nodos NCC's. Una subárea es una colección de terminales, estaciones de trabajo, y líneas telefónicas dirigidas por un NCC. Generalmente, el NCC es el responsable de dirigir el tráfico ordinario que corre dentro de la subárea, y VTAM dirige las conexiones y uniones entre las subáreas. Cualquier subárea de red debe tener un mainframe. En un sistema clásico (3270), cada terminal (3278 o 3279) se conecta a un controlador de un conjunto de terminales (3174 o 32749) por medio de un cable coaxial. El controlador del conjunto actúa como una central reuniendo todos los mensajes de las terminales para una transmisión más eficiente hacia el mainframe. Se conectan varios controladores de grupo mediante una línea telefónica a otro dispositivo mayor llamado controlador de comunicaciones o procesador de front-end **(FEP Frond End Processor)**. La rápida evolución en las minicomputadoras y en estaciones de trabajo, obligó a IBM a desarrollar un segundo tipo de SNA. Los clientes construían redes basadas en minicomputadoras AS/400 que no tenían mainframe o VTAM que soportaran el control de la red. La nueva SNA se llamó **APPN (Advanced Peer to Peer Networking)**. APPN y subárea SNA tienen diferentes estrategias para encaminar y dirigir la red. Sólo tienen en común que soportan las aplicaciones y mecanismos utilizando el protocolo APPC (LU6.2). Aunque IBM continua diciendo que SNA es una arquitectura, es más exacto describirla como dos arquitecturas compatibles que pueden intercambiar datos. APPC es un protocolo dentro de SNA que establece las condiciones que permiten a diferentes programas comunicarse a través de la red.

Los productos que realmente implementan las especificaciones APPC son APPC/PC y APPC/LU 6.2. Sin embargo, estos programas son largos e incómodos y no se manejan con facilidad y rapidez. En la red SNA, un cliente y un servidor no pueden intercambiar mensajes a menos que el primero establezca una sesión. En una subárea de la red, el programa VTAM en el ordenador principal consigue envolverlo creando todas las sesiones. Además hay bloques de control describiendo la sesión en el NCC a los cuales se dirige el cliente y el NCC al cual se dirige el servidor. Los NCC's intermedios no tienen los bloques de control para la sesión. En APPN SNA, hay bloques de control para la sesión en todos los nodos intermedios a través de los cuales pasan los mensajes. La arquitectura APPN fue diseñada originalmente para minicomputadoras. APPN tiene dos buenos nodos. El nodo final (EN) contiene programas cliente-servidor. Los datos fluyen fuera de ellos, no van a través de los nodos finales, y un nodo de red (NN) que contiene programas cliente-servidor pero a menudo proporciona rutas para el resto de la red.

La mayoría de los APPN son el grupo de preguntas y respuestas que dirigen nombres, encaminamientos y sesiones. Como el resto de SNA es complicado. Obviamente las estaciones de trabajo no pueden mantener una tabla dinámica de una red de gran distancia. La solución a este problema está en romper la red APPN en pequeñas unidades locales, cada una con un identificador de red **(NETID)**. El NETID identifica un grupo de estaciones de trabajo (un edificio, un

campus, una ciudad). El tráfico a una red remota es encaminado basándose en el NETID, y el tráfico en grupos locales es encaminado basándose en el LUNAME. Pero tenemos que tener en cuenta, que todos los diseños tienen ventajas e inconvenientes. El diseño SNA trabaja bien al construir redes comerciales seguras. De cualquier manera, se requiere de un personal técnico central entrenado, dispuesto, y capaz de responder a problemas, así como a hacer informes para el equipo de la red. Por tanto SNA depende de una red segura. Cuando algún paquete de datos se mueve entre nodos, deben ser chequeados los errores y los paquetes serán aceptados o retransmitidos. Sólo después de que hayan sido aceptados pueden ser enviados al siguiente nodo. Para conseguir esta seguridad, SNA depende de protocolos **orientados a conexión** dentro de la familia HDLC. HDLC es un estándar internacional desarrollado en los años 70's, para suministrar comunicaciones entre módem, fáciles y seguras. Como todos los estándares internacionales, tienen una extensa definición para todas las cosas. IBM tiene una política de refinamiento sobre cualquier estándar internacional ambiguo. Adoptando como un estándar corporativo interno un específico juego de respuestas. Cuando un sistema tolera varias respuestas a una situación, IBM adopta un estándar por el que todos los dispositivos IBM deben generar una respuesta específica, los demás tienen que tolerar todas las respuestas válidas de dispositivos producidos por otros vendedores. La respuesta a HDLC fue seleccionar opciones específicas, aclarar dudas, y generar un subconjunto más preciso del protocolo, que IBM denominó "SDLC".

2.4.4.3 TOPOLOGIA

La arquitectura de sistemas de redes fue la primera en desarrollar suministros fiables, comunicaciones seguras centralmente dirigidas a redes de grandes naciones, para las compañías más grandes de USA. La red central estaba basada en controladores dedicados a correr un programa llamado NCC. Desde que las minicomputadoras fueron controladas, dirigidas y programadas por usuarios finales, éstos, no tenían permiso para ser parte de la red central fiable. Una minicomputadora podía contener programas clientes-servidor. Este podría ser la fuente o destino de mensajes, pero no podría encaminar mensajes en nombre de otras máquinas, y no podría participar en la red dirigida. Las estaciones de trabajo y las PC's heredaron el rol de la minicomputadora como un **nodo periférico**. Como el nodo sugiere, tal nodo es exterior a la red misma. En la arquitectura se denomino como un capa de protección entre los nodos periféricos y los NCC's **llamada función límite**. El NCC establece la dirección de cada mensaje en la red, y lo reemplaza por una señal de byte antes de pasarlo a través del límite hacia un nodo periférico. Esto garantiza que la minicomputadora no pueda generar falsos mensajes a través de sesiones establecidas por el ordenador principal. SNA se basa en el concepto de dominio, que consiste en un conjunto de nodos dependientes de un nodo principal al que están conectados por medio de sistemas diversos de comunicaciones y a través de nodos auxiliares. Este sistema dispone en sus nodos principales y tributarios de puertas de acceso para los usuarios finales, es decir, programas de aplicación u operadores de terminales, estas puertas de acceso reciben el nombre de **Unidades Lógicas (LU Logic Units)**. Se trata de un programa SNA que actúa como un puente entre el usuario final y la red. El usuario final comunica con la LU y la LU comunica con la red. Cada LU tiene un único nombre de red. La SNA emplea este nombre para determinar una dirección de la red y la situación real en que se encuentran los recursos que necesita el usuario. Los aspectos físicos de la red resultan transparentes al usuario final. Puede haber varios usuarios finales conectados a una LU. La SNA define los protocolos necesarios para iniciar un diálogo (sesión) entre dos LU's, mantenerlo y terminarlo en un momento dado. La LU viene a ser una especie de nodo lógico, que puede estar agrupado dentro de los productos hardware y software (nodos físicos) que constituyen la red.

Cada nodo físico dispone de un nodo adicional de control, se le denomina **Unidad física (Physical Unit, PU)**, tiene capacidad de gestionar sus propios recursos y ayudar a sus LU a establecer sesiones. La red utiliza una PU para poner al nodo en línea, dejarlo fuera de línea, probarlo y ejecutar funciones parecidas a la administración de redes. La unidad física es un programa similar a la LU excepto que no interactúa con un usuario final, en cambio, interactúa con el hardware físico en que está incluido. Todos estos nodos lógicos (PU y LU) de un dominio están controlados por un único nodo lógico de control, denominado **SSCP (System Services Control**

Point, Punto de control en los servicios de sistemas). El SSCP tiene un conocimiento completo y un control sobre todos los procesadores, controladores y terminales unidas o ligados al host. Este control lo ejerce mediante una serie de comandos que el SSCP intercambia con los PU y LU mediante sesiones, que son requisitos previos para el establecimiento de sesiones entre LU's. Vemos, entonces que un nodo físico puede llegar a tener hasta tres tipos diferentes de nodos lógicos, figura 89.

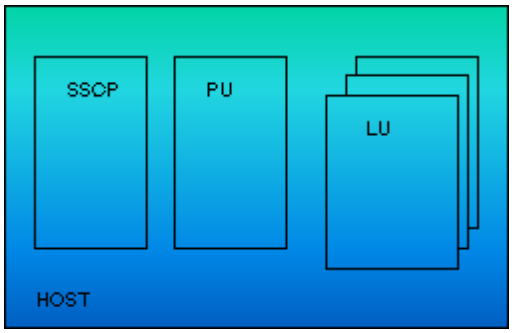


Figura 89 Ejemplo de nodo SNA: tipo 5

LU.-Un número variable en cada nodo físico con interfaz a usuarios finales.
PU.-Uno por cada nodo físico.
SSCP.-Uno en el nodo principal de cada dominio.
Las diferentes agrupaciones de estos dan lugar a los tipos de nodos físicos siguientes, figura 90.

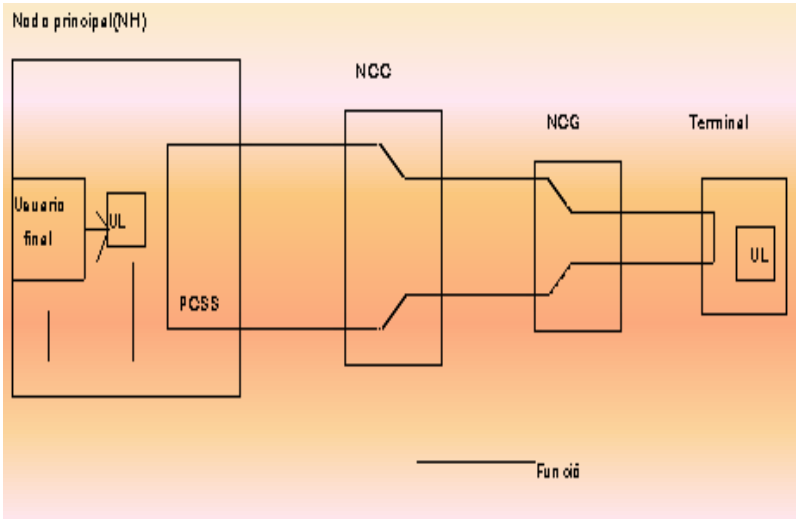


Figura 90 Estructura Básica de la red SNA, concepto de dominio.

1.- Nodos tipo 5 (mainframe), Host, contiene un SSCP una PU y un número variable de LU.
2.- Nodos tipo 4, Controlador de comunicaciones (NCC), constituyen un nodo intermedio de la red cuya función consiste en reducir la carga del CPU principal y realizar el manejo de interrupciones asociadas con la comunicación de datos. En la red SNA es el procesador 3750 de IBM.
3.- Nodos tipo 2 (los nodos periféricos), son los Controladores, también conocido como **nodo de control de grupo (NCG)**, contienen una única PU y una LU para cada usuario final que lo comparte, son los encargados del manejo de las distintas operaciones específicas que pueden montarse sobre la red, siendo un equipo diferente según se trate de aplicaciones bancarias, científicas o puntos de venta al por mayor.
4.- Nodos tipo 1, Terminales, generalmente asimilando a una terminal no inteligente monoestación. En este caso contiene una PU y una LU.
Curiosamente no hay nodos tipo 3.

En la nomenclatura SNA, a la LU, PU y al SSCP se les conoce como **NAU's (Unidades Direccionables de Red)**, y son como hemos explicado anteriormente, una pieza software a través del cual se permite que un proceso utilice la red. Además de los cuatro nodos descritos anteriormente, la arquitectura SNA distingue entre nodos subárea y nodos periféricos:

- Un nodo subárea puede encaminar datos de usuario por toda la red.
- Un nodo periférico tiene una orientación más local. No encamina datos entre nodos subárea.

Los nodos están conectados por enlaces de los concesionarios, y dichos enlaces están controlados por el SDLC (Synchronous Data Link Control).

2.4.4.4 NIVELES DE SNA

Figura 91

Capa 1 Control de enlace físico.-Transporte físico de los bits de una máquina a otra. Este nivel está disponible en RS-232-C y X.21.
Capa 2 Capa de control de enlace.-Construye tramas a partir del flujo de bits original, detectando y recuperando errores de transmisión de una manera transparente para las capas superiores. El nivel de enlace de datos está implementado con SDLC (Control de enlace de datos síncrono). La SNA soporta el mecanismo de acceso de paso de testigo en anillo de una LAN, en esta capa.
Capa 3 Control de ruta.-Consiste en establecer una trayectoria lógica de la NAU fuente a la NAU destino. Este nivel tiene dos responsabilidades fundamentales: control de flujo y encaminamiento. El encaminamiento se lleva a cabo gracias al control del camino, examinando los destinos de la red en el mensaje y determinando la línea apropiada para que el mensaje alcance su destino. El control de camino también realiza la división en segmentos del mensaje. La arquitectura SNA permite diferentes tamaños de segmento para cada enlace o grupo de enlaces. Además el control de camino también agrupa mensajes, figura 91.

El nivel contiene asimismo un mecanismo de control de flujo, denominado control de **ruta virtual**, para limitar el flujo de datos desde un nodo de subárea transmisor. El SNA asigna rutas virtuales a las 2 subáreas envueltas en una sesión de figura 92.

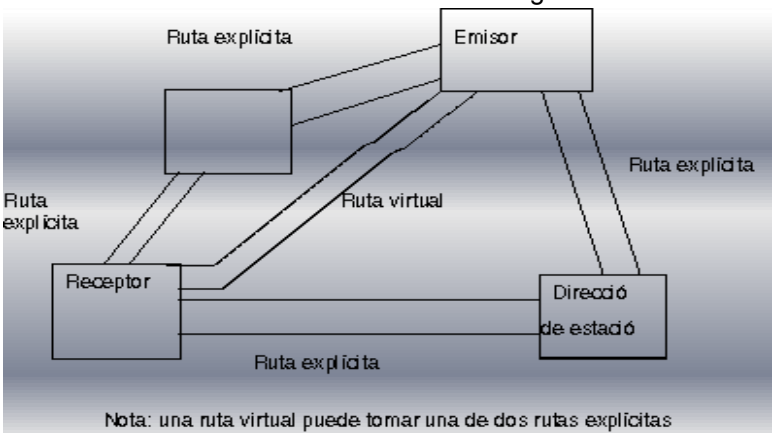


Figura 92 Rutas Explícitas y Virtuales

Capa 4 Control de transmisión.-Localizada encima de la capa de control de ruta, tiene bajo su responsabilidad la creación, el manejo, y la liberación de las conexiones de transporte (sesiones). Todas las comunicaciones en SNA utilizan sesiones y no soportan comunicaciones sin conexión. El propósito de la existencia de una sesión en la SNA, consiste en proveer a las capas superiores con un canal libre de error que sea independiente de la tecnología del hardware de las capas inferiores.
Capa 5 Control del flujo de datos.-Tiene como objeto el seguimiento de a que extremo de la sesión le corresponde hablar a continuación. Esta capa está muy relacionada también con la recuperación de errores. Una característica poco común, es la ausencia de una cabecera específica para comunicarse con el software correspondiente del otro extremo. En lugar de dicha cabecera, la información que normalmente se comunicaría a través de ella, se pasa al control de transmisión como parámetros y se incluye en la cabecera de transmisión.

Capa 6 Servicios NAU.-Provee dos clases de servicios a los procesos de usuarios: **Servicios de presentación**, proporcionan formatos comunes entre los usuarios finales y caracteres de control entre dispositivos diferentes. Los servicios de presentación proporcionan funciones de compresión y compactación y **Servicios de sesión** para el establecimiento de conexiones.
Además existen los Servicios de sesión de red que están divididos en 3 categorías:

- Servicios de operador de red, facilitan la comunicación entre operadores y SSCP de la red.
- Servicios de configuración, responsables de la activación/desactivación de enlaces, la carga de programas en los nodos SNA y el mantenimiento de tablas dentro de los SSCP.
- Servicios de sesión, responsables de la conversión de los nombres lógicos de la red proporcionados por los LU en sus correspondientes direcciones de red, tabla 18.

Nombre del nivel---------- Función del nivel

OSI	SNA	OSI	SNA
Aplicación	Gestor de servicios UDR	Puente del usuario hacia los niveles. Gestión de ficheros. Gestión de elementos de servicio.	Intercambio de datos entre UL; gestión de dispositivos y de for-compactación; mapas compactación; mapas
Presentación	Servicios NAU	Gestión de formato, alfabeto, sintaxis. Cierta gestión de ficheros.	y sintaxis comunes gestión de ficheros conversión de direcciones
Sesión	Control de flujo datos	Sincronización de diálogos de usuario, gestión de intercambio de datos, servicio de garantía.	Sincronización de intercambio de información; encadenamiento y agrupamiento; gestión de respuestas.
Transporte	Control de Transmisión	Control de errores, conversión de direcciones, segmentación, agrupamiento de prioridades, calidad de servicio.	Tráfico de datos; cifrado de datos; gestión del estado de la sesión.
Red	Control de Camino	Interfaz de paquetes DTE-DCE (X.25)	Control de flujo y encaminamiento; conversión de direcciones segmentación y agrupamiento de mensajes.
Control de Enlace de Datos	Control de Enlace de Datos	Gestión del flujo de datos a través de un enlace (HDLC)	Gestión del flujo de da-tos a través de un enlace (SDLC).
Físico	Físico	Interfaz eléctrica, física, hacia la red (X.21).	Interfaz eléctrica, física hacia la red (X.21, RS-232-C).

Tabla 18

2.4.4.5 COMPARACION ENTRE LOS NIVELES OSI Y SNA

Desde el punto de vista de las funciones y capacidades que ambas redes proporcionan al usuario final, estás tienen muchos puntos en común. Sin embargo, la manera de llevar a la práctica dicha implementación es netamente diferente. En 1981, IBM anunció algunos productos que permiten enlazar componentes SNA con las redes de conmutación de paquetes X.25. Las funciones de soporte residen en el PCR del procesador de comunicaciones o en un dispositivo remoto. Los productos que conectan el enlace SDLC y el circuito virtual X.25 y el Adaptador de Interfaz de Red, terminan el sondeo de forma local. La interfaz de IBM soporta tanto circuitos virtuales permanentes como conmutados. IBM dispone además de productos para soportar la X.21 conmutada o no conmutada.

2.4.4.6 SESIONES

Hemos visto que una sesión es un intercambio temporal de información entre dos NAU. Existen distintos tipos de sesiones:

- LU-LU.-Utilizada para comunicación entre usuarios finales.
- SSCP-PU/LU.-O sea, el SSCP con las NAU de su dominio. Su misión básicamente es la gestión y control de los recursos de la red. Por ejemplo SSCP-PU para permitir que el SSCP inicie, controle y pare a las PU. SSCP-LU se utiliza fundamentalmente para que la LU solicite del SCCP el establecimiento de sesión con otro LU.
- SSCP-SSCP.-Para control entre dominios y gestión de mensajes, por ejemplo para coordinar la activación de sesiones LU-LU de dominios distintos.
- PU-PU.-Para la administración de redes.

Para poder establecer sesiones entre dos NAU es preciso que ambas soporten subconjuntos compatibles entre sí. Las sesiones de control, SSCP-SSCP, SSCP-PU, SSCP-LU, requieren unos subconjuntos predefinidos, implantados originalmente en el diseño de cada subsistema. Para establecer una sesión, un proceso debe decírselo al gestor de control de sesiones de su dominio. Si el destino es local (está en el mismo dominio), ésta se puede establecer directamente. Sin embargo, si el destino está en un dominio remoto, el SSCP deberá contactar primero al SSCP correspondiente que controla el dominio distante. Las rutas virtuales y explícitas también se deberán seleccionar. Al inicio de la sesión entre dos LU, es necesario el intercambio entre ellas de la descripción de sus posibilidades funcionales. Este intercambio se realiza mediante un comando de inicio de sesión llamado **BIND** que envía una de las LU a la otra, en el caso de que la LU receptora esté de acuerdo, responde positivamente, o bien, si no coinciden los perfiles con alguno de los subconjuntos que puede procesar responde negativamente. En el momento en que ambas LU estarán de acuerdo, la sesión queda establecida. Una vez que se establece la sesión, la capa de control de transmisión se encarga de regular la velocidad del flujo entre los procesos, de controlar las asignaciones de memoria. Para soportar una sesión, cada una de las LU debe reservar una determinada cantidad de recursos, entre ellos, áreas de control para mantener la descripción de los protocolos utilizados, los distintos estados que los reflejen, numeración de secuencia y parámetros para construcción de cabeceras. El conjunto de los recursos reservados para cada uno de los interlocutores de una sesión recibe el nombre de **semisesión (Half Session, HS)**. Podemos imaginar una LU estructurada tal como se representa en la figura 93. En ella existen unas funciones comunes a la LU agrupadas bajo el nombre de **Gestor de Servicios (Service Manager)**, cuyas misiones principales son: activar y desactivar sesiones, diferenciar los flujos de datos correspondientes a dos sesiones simultáneas, etc.. Además, hay una semisesión establecida entre la LU y el SSCP, y una semisesión más para cada sesión simultanea que nuestra LU mantiene con otras LU de la red. Estas semisesiones podemos considerarlas como tareas paralelas de ejecución de los protocolos realizados en esta LU, adaptadas a las características específicas de los perfiles negociados con las otras LU.

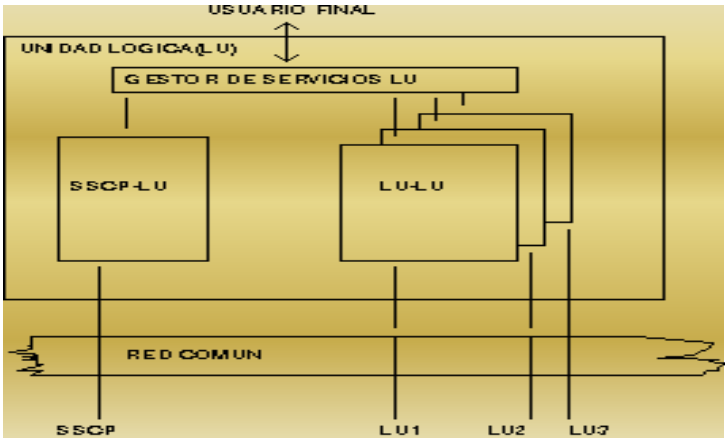


Figura 93 Estructura general de una LU

2.4.4.7 FORMATO DE DATOS

Cada mensaje que entra o sale de la red es denominado SAN, una **solicitud**, o una **respuesta**. Puede llegar a existir una respuesta por cada solicitud, pero esto no es preciso, ya que tales respuestas tienen como significado la de que una solicitud o una serie de ellas hayan llegado correctamente a su destino. Es decir, son una información de control generada por la LU receptora, a petición de la emisora, indicando la llegada correcta de la solicitud enviada. La respuesta en forma de datos del usuario final receptor será introducida en la red en forma de una nueva solicitud con destino a la originaria de la primera. La unidad de información, que denominaremos **RU (Request/Response Unit)** viaja a través de la red acompañada de información de control, estructurada en una serie de cabeceras, figura 94.

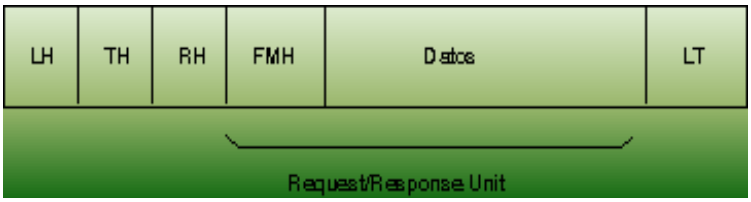


Figura 94 Formato básico de un mensaje sin segmentación.

- **LH/LT (Link Header/Trailer Header)**.-Información de control requerida para la transmisión con protocolo SDLC, por línea telefónica. Es añadida y eliminada, en transmisión y recepción respectivamente. Su única misión es asegurar la transmisión sin errores de la RU en un determinado tramo del camino.
- **TH (transmission Header)**.-Utilizado dentro de la red común por las distintas PC's para encaminar las unidades de información a través de los nodos de la red.
- **RH (Request/Response Header)**.-Cabecera de uso end-to-end, generado por la semisesión de la LU emisora para transmitir información de protocolos a la receptora.
- **FMH (Function Management Header)**.-Constituyen el mecanismo que una LU utiliza para seleccionar alguna de las funciones que la semisesión interlocutora puede realizar en su favor, sin involucrar directamente al usuario final.

Son opcionales en la mayoría de sesiones de usuarios.

La respuesta a una RU por parte de la LU receptora puede ser positiva o negativa, en ese caso dentro de la respuesta se inserta una información condensada del tipo de error detectado.
Las respuestas positivas no suelen ir acompañadas de datos. La LU originalmente de una RU puede elegir entre tres protocolos distintos de respuesta:

- **Respuesta definida**.-La semisesión emisora desea estar segura de la correcta recepción de la RU por parte de la receptora. Se generará una respuesta positiva o negativa cuando le llegue tal RU.
- **Respuesta de excepción**.-La semisesión emisora sólo esta interesada en tener noticia de las transmisiones erróneas.
- **No respuesta**.-La emisora no desea recibir respuesta en ningún caso. Sólo es aplicable cuando la información transmitida no es crítica.
- **Tratamiento de cadenas.-**Hay casos en que una unidad de información debe ser transmitida en forma de múltiples RU. Esto puede ser debido a:
    - Una limitación en el tamaño máximo de la RU por parte de una o ambas LU dialogantes acordada al establecer la sesión.
    - A la comodidad del usuario final en la preparación de los datos que ha de enviar, que prefiere hacerlo por partes.

  En cualquiera de los casos el conjunto de estas RU tiene tal entidad que, en caso de error en cualquiera de ellas, es necesario reenviar todo el conjunto nuevamente. Por ejemplo, la repetición de una línea de una página estropearía el conjunto de la misma.

Para resolver esta necesidad, las LU pueden utilizar un protocolo end-to-end de encadenamiento de RU, que consiste en indicar en los RH correspondientes la calidad del elemento inicial, intermedio, final o único de una cadena. Esto asociado con los mecanismos de respuestas definidas, excepción o no respuesta a nivel de cadena y de recuperación global, permite efectuar cómodamente cualquier tratamiento conjunto de toda la cadena para el usuario final del receptor. Antes hemos dicho que una unidad de información puede ser transmitida **a trozos**, por un límite de tamaño máximo debido a tamaños físicos de buffers o bien debido a la calidad de una línea, a este proceso se le denomina **segmentación**. El **bloqueo** es la función absolutamente inversa, es decir, aquella que permite que, dada la buena calidad y características de buffers de un determinado enlace, sea posible transmitir como una sola unidad de transmisión el conjunto de varias RU, constituyendo un único bloque de información. Esta función sólo está arquitecturada entre hosts y controladores de comunicaciones. La segmentación, bloqueo y el encadenamiento son protocolos a niveles claramente diferenciados. El segundo es un protocolo implantado para que el usuario final pueda preparar cómodamente una unidad de información por partes independientes y enviarla con toda integridad a otro usuario final, bajo su propio control, mientras que el primero es un protocolo transparente a la LU, utilizado en determinados tramos de la ruta de una RU, sólo entre nodos adyacentes.

2.4.4.7.1 FLUJO NORMAL Y FLUJO EXPEDITO

El flujo normal entre semisesiones lo constituyen las RU de datos, algunas de comando y sus respectivas respuestas. Este flujo se gestiona en algoritmo FIFO. Un flujo independiente denominado flujo expedito consiste en unas determinadas solicitudes/respuestas que se saltan las colas de flujo normal y secuencias de protocolo. Este flujo está reservado para determinados comandos SNA con características de urgencia. A tiempo de establecimiento de sesión, con el comando BIND, es posible especificar que **modos de control** se van a utilizar para regular el tráfico de datos y gestionar de forma más adecuada las situaciones de recuperación. Tales modos se eligen por separado e independientemente para los flujos en ambos sentidos de una sesión. Estos modos son:

- **Solicitud inmediata**.-Con las reglas:
    - Después de enviar una transmisión que requiere una respuesta definida, es necesario esperar antes de enviar otra solicitud.
    - En cualquier momento es posible que haya pendientes múltiples transmisiones de RU sin petición de respuesta o de respuesta de excepción, pero sólo en el caso de que no haya ninguna solicitud pendiente de respuesta definida.
- **Solicitud desfasada.-**Sin restricción alguna en el envío de RU de datos o comandos en flujo normal.
- **Respuesta inmediata**.-Las respuestas son devueltas siempre en el orden en que se reciben las correspondientes solicitudes.

- **Respuesta desfasada**.-Significa que las respuestas se pueden enviar en cualquier orden.

El flujo normal utiliza ambos modos de respuesta. El flujo expedito requiere modo de respuesta inmediato.

2.4.4.7.2 MODOS DE TRANSACCIÓN

Desde el punto de vista de diálogo lógico entre usuarios finales es posible elegir modalidades distintas de protocolos, que son lo que llamaremos modos de transacción. Estos consisten en los criterios por los cuales ambos interlocutores de una sesión saben en un momento determinado quien debe enviar y quien debe recibir. Una semisesión debe estar en estado de transmisión para poder enviar RU de datos o comandos en flujo normal, en el estado opuesto, llamado de recepción, sólo puede enviar comandos de flujo expedito y todo tipo de respuestas. Los protocolos para estos dos estados vienen determinados por los modos de transacción siguientes:

- **Dúplex (FDX)**.-Ambos interlocutores pueden enviar y recibir datos simultáneamente. El tráfico de la sesión en un sentido es independiente del tráfico en el sentido opuesto.
- **Semidúplex (HDX)**.-Cualquiera de los interlocutores puede iniciar el envío de una cadena. Pueden ocurrir dos cosas: que el otro no inicie una idéntica acción de modo simultáneo, en cuyo caso continuará el flujo de RU en el mismo sentido hasta el fin de la cadena. En segundo lugar puede ocurrir un intento inicial de envío simultáneo por ambos interlocutores, se producirá una situación de contención, que se resolverá según se acordó al tiempo de establecimiento de sesión, esta decisión se debe de tomar de acuerdo con la capacidad de almacenamiento temporal y último reintento que ofrezcan cada uno de ellos.
- **Semidúplex Flip-Flop (HDX-FF)**.-Cuando uno de los interlocutores ha tomado la iniciativa de envío, la conservará hasta que decida ceder la vez al otro. A partir de ahora, el otro transmitirá hasta que decida devolver la iniciativa al primero.

Estas modalidades de transacción entre usuarios finales son absolutamente independientes de las modalidades de transmisión que se utilicen por un enlace determinado dentro de la ruta a seguir por las RU de una sesión. Por ejemplo, un protocolo dúplex puede ser adecuado para comunicar una LU que controle una lectora de cinta y una impresora con otra LU remota que sirva de puerta de acceso a un sistema operativo. Un protocolo de contención semidúplex puede ser útil para aplicaciones de conmutación de mensajes o bien para comunicación entre procesos remotos de igual categoría. Un protocolo flip-flop es el más típico para una aplicación de consulta y actualización de base de datos.

2.4.4.8 PROTOCOLOS

- **Protocolo bracket (paréntesis o corchetes)**.-Este protocolo está diseñado con el fin de prever la posibilidad de que un usuario final (en términos SNA), pueda tener iniciativas de diálogo paralelas e independientes entre sí. El caso más claro de este protocolo lo constituyen múltiples procesos paralelos accedidos por una única LU, con la que puede estar en sesión otra LU remota en un momento dado. Si cada uno de los procesos paralelos, iniciase por separado diálogos paralelos con la segunda LU, podría crearse un caos absoluto para ésta. Para evitar tal consecuencia, el protocolo bracket permite dividir cada proceso en estructuras de duración discreta y, al inicio de cada una de ellas, abrir un paréntesis (bracket), durante el cual, otro proceso paralelo no puede iniciar diálogo con la misma LU remota hasta que se cierre. La implantación de los protocolos de inicio y terminación consiste en unas reglas, indicadores y comandos, previstos para tal fin.
- **Protocolo Pacing.-P**odríamos denominar protocolo marcapasos. Es una función que es posible utilizar cuando la LU que envía RU puede hacerlo a un ritmo más rápido del que puede seguir en su proceso la LU receptora. Un nodo con múltiples LU podría ver saturados sus recursos de almacenamiento intermedio, con RU de una sola sesión LU-LU. Para evitarlo es posible definir un valor “N” para cada una de las LU, de tal forma que la transmisora sólo le enviará como máximo hasta “N” solicitudes de flujo normal.
- **Protocolos de interrupción**.-Por los que un interlocutor puede solicitar del otro que deje de enviarle datos y se quede en estado de espera. Existe también un comando para reactivar una sesión interrumpida de esta forma.

- **Protocolos de comunicación**.-Al interlocutor de situaciones locales que afectan a la sesión (permiso para enviar datos, estado de la transmisión, etc.).
- **Compresión y compactación de datos**.-Es decir, reconocimiento de caracteres repetidos y sustitución de ellos por un código de uno o dos bytes u octetos, y reestructuración de porciones del string de caracteres.
- **Recuperación de errores**.-Un error según se defina en SNA es un quebrantamiento de:
  - Una regla de la arquitectura.
  - Una regla de sesión.
  - Una regla establecida por medio de una cabecera funcional dentro de una sesión.
  - Una regla pendiente de un estado de la sesión.

  Cualquiera de los interlocutores puede ser responsable de la recuperación de errores. Los protocolos relacionados con la recuperación de errores son:
  - Petición de eliminación de la transmisión errónea.
  - Terminación de la sesión.
  - Petición de recuperación y/o terminación de la sesión por parte del interlocutor.
  - Cancelación de una cadena incompleta.
  - Resincronización de secuencia.
  - Reanudación de tráfico, etc.
- **Protocolos de desactivación de sesión**.-En caso de terminación normal, de forma inmediata, o bien de forma ordenada, al término de la transmisión del tráfico pendiente.
- **SDLC.-**El SDLC permite que un mensaje sea enviado por una estación primaria a varias estaciones secundarias, tal y como se muestra en la figura 95. Esto es llamado comunicación multipunto. El mensaje de la estación primaria es transmitido eléctricamente a todas las secundarias, pero sólo es dirigido a una. La estación destino, habiendo obtenido el permiso para utilizar el enlace, responde a la estación maestra.

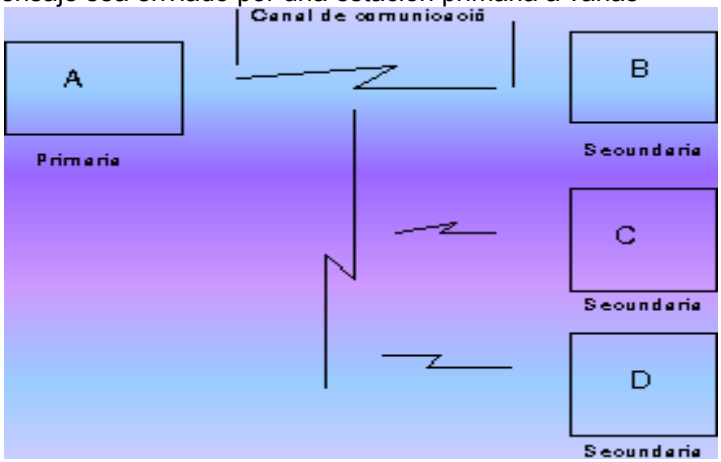


Figura 95. Comunicación multipunto SDLC.

El SDLC permite tanto comunicación half-dúplex como full-dúplex. Sin embargo, cuando la PC actúa como una terminal 3270, la comunicación es punto-a-punto half-dúplex; el 3705 es la estación primaria y la PC es la única estación secundaria. Para comprender el SDLC, debemos entender la comunicación síncrona, como la que utilizaban el telégrafo multiplexado y los sistemas multiplexados de división de tiempo. La comunicación síncrona de datos moderna no tiene que intercalar caracteres de diferentes mensajes, pero tienen que mantener los bits en orden. El bit 1 debe siempre acabar como bit 1. Una señal síncrona externa es práctica sólo con conexiones directas. Hay varios esquemas para llevar a cabo una autosincronización. El SDLC usa un esquema llamado inserción de bit cero y un método de codificación llamado NRZI- Inversión sin vuelta hasta cero. Este método garantiza suficientes transiciones cero/uno para que los circuitos del receptor puedan reconstruir la señal entrante

La figura 96 muestra una estructura SDLC, usada para enviar una unidad de mensaje por un enlace de datos. Los flags del principio y del final son representados por la secuencia de bits 01111110 que, rompe la regla de inserción de un cero en una cadena de cinco o más unos. Así es como el receptor reconoce los límites de la estructura. El campo de dirección, de sólo 8 bits, indica la dirección de destino si la estructura es enviada a una estación secundaria, o de enlace controlado.

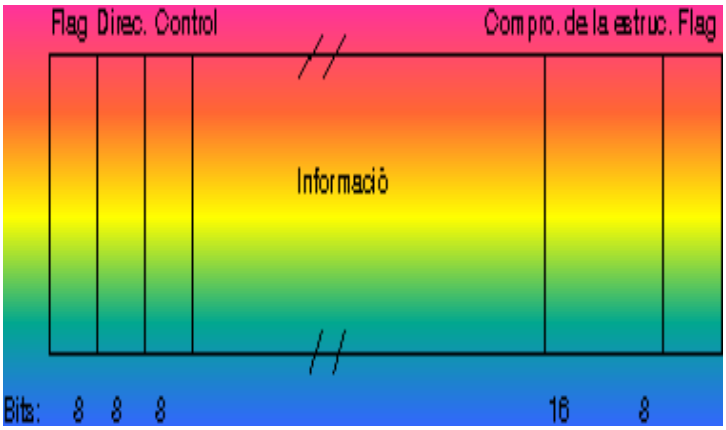


Figura 96. Estructura SDLC

La dirección es la dirección fuente si la estructura es enviada a la estación primaria o controladora de enlace. El campo de control, también de 8 bits, se usa para numerar las estructuras en orden secuencial. El campo de información, de cualquier longitud, múltiplo de 8 bits, contiene los datos a ser transferidos por el enlace. La secuencia de comprobación de la estructura es un chequeo cíclico redundante (CRC) de 16 bits, usado para comprobación de errores.

2.4.4.9 TCP/IP o SNA

Es difícil entender algo a menos que tengas algo con qué compararlo. Esto sugiere una comparación obvia: SNA no es TCP/IP. Estas aplicaciones están en el diseño de todos los niveles de las 2 arquitecturas de redes. Siempre que IBM diseña algo propio, TCP/IP diseña lo contrario. Como resultado existen dos protocolos de redes incompatibles, se forman de manera complementaria. Una organización que corre con ambas posibilidades, SNA y TCP/IP puede, probablemente solucionar algunos tipos de problemas de comunicación. Una red IP encamina los paquetes de manera individual. La red reparte cada paquete basándose en el número de dirección que identifica la máquina destino. La red no ha mirado la sesión. Cuando traes un documento, por ejemplo de Internet, las diferentes piezas pueden terminar encaminándose a través de diferentes ciudades. TCP es responsable de volver a reunir las piezas una vez recibidas. En la red SNA, un cliente y un servidor no pueden intercambiar mensajes a menos que el primero establezca una sesión. En una subárea de la red, el programa VTAM en el ordenador principal consigue envolverlo creando todas las sesiones. Además hay bloques de control describiendo la sesión en el NCC a los cuales se dirige el cliente y el NCC al cual se dirige el servidor. Los NCC's intermedios no tienen los bloques de control para la sesión. En APPN SNA, hay bloques de control para la sesión en todos los nodos intermedios a través de los cuales pasan los mensajes. El diseño IP trabaja bien en redes experimentales. El diseño SNA trabaja bien en la construcción de redes comerciales seguras. Pero como ya hemos mencionado se requiere de un personal técnico entrenado, dispuesto, y capaz de responder a problemas, así como realizar informes para el equipo de la red. Hoy, cuando compramos una PC y la conectamos a una LAN, su configuración central ha llegado a ser difícil de manejar. Una solución formal, está proporcionada por la arquitectura APPN diseñada originalmente para minicomputadoras. APPN tiene dos buenos nodos, el nodo final y el nodo de red, a los que ya nos hemos referido anteriormente. TCP/IP es un simple protocolo. El código origen de programas está generalmente disponible. SNA está asombrosamente completo, y sólo IBM tiene el grupo completo de programas. Es construido en el AS/400. Otros importantes productos de estaciones incluidos son:

- NS/DOS para Dos y Windows.
- Director de comunicaciones para OS/2.
- Servicios SNA para AIX.

- Servidor SNA para Windows (de Microsoft).

La programación original de interfaces para la moderna red SNA es la interfaz común de programación para comunicaciones (CIPC). Este provee un común conjunto de subrutinas, servicios y códigos de retorno para programas escritos en COBOL, C o REXX. Está documentado en la publicación IBM SC26-4399, pero está también disponible en CD-ROM. Bajo el anteproyecto de comunicación de IBM, SNA llegó a ser una de las opciones intercambiables de "transporte". La tradicional red SNA fue instalada y dirigida por un personal técnico central en una corporación grande. Si la red caía, una compañía como Aetna Insurance era temporalmente excluida de los negocios. TCP/IP es diseñada para ser cauteloso con los errores y simplemente descarta mensajes de error. No es posible construir una red para cada protocolo que pueda encontrar demanda de corporaciones. Internet está formada por algunas docenas de servidores centrales y proveedores y 10,000 redes privadas conectadas. Las cosas cambian todo el tiempo. No es lógico intentar implantar un control central sobre cambios e inmediatamente responder a todos los programas. No es posible construir Internet utilizando SNA, pero IP diseña buenos servicios la mayoría del tiempo.

2.4.4.10. LINK STATION

Para cada terminal de la línea telefónica o LAN, la computadora necesita guardar rastro de unos pocos ítems. Éstos van a formar lo que es el número que sería asignado a la siguiente trama transmitida, que será el número de la última trama recibida. Pero, ¿ha sido aceptada ya?.
Hay tiempos límites para detectar muchos mensajes, y un contador para mantener la ventana de tramas no reconocidas. El estándar 802.2 llama a esto **connection component**. En SNA es una **Link Station**. La estación de enlace o Link station controla la corriente de datos entre dos nodos de red. Sucesivas I-tramas pueden pertenecer a la misma sesión, o pueden pertenecer a diferentes programas o terminales. Cuando una trama es reconocida en la LAN o línea SDLC, esto no significa que el dato sea correcto o haya sido procesado. La Link station almacena un montón de datos en los buffers y colas para después procesarlos. El mainframe basado en la red SNA no permite minicomputadoras para hacer de encaminadores intermedios para los mensajes de otros nodos. En otros protocolos de comunicación no existe esta regla, y con el poder de los microprocesadores, éstos fueron integrados en otros dispositivos de red, la restricción de SNA llega a ser intolerable. El resultado es que los dispositivos de IBM empezaron a ser un fraude. Ellos violaban la arquitectura puesta en marcha con las estaciones Link activas. Si un dispositivo permite I-tramas, los paquetes RR, y RNR corren por él, esto es un puente. Los puentes son requeridos para construir grandes redes Token Ring. El protocolo IEEE 802 está configurado para los dispositivos SNA que permiten demoras causadas por un cierto número de puentes entre dos nodos. Cuando el dispositivo es conectado a dos diferentes medios con diferentes velocidades, como es el caso en el que dos LAN's son conectadas por una línea telefónica, entonces las I-tramas pueden tardar demasiado en llegar a su destino. La solución es crear una falsa estación Link en cada LAN para recibir y reconocer las I-tramas antes de encolarlas hacia la transmisión remota. Como los buffers, se llenan, el paquete de control de receptor no preparado (RNR) puede ser usado temporalmente hasta que los datos anteriores hayan sido enviados.

Para entender este truco, es importante darse cuenta de que una estación Link reconoce la recepción de una I-trama, esto no implica que los datos de la I-trama hayan sido procesados. Un adaptador Token-Ring de IBM reconoce las tramas como son recibidas por la tarjeta del adaptador. Pueden entonces hacer cola y pueden ser procesados en segundos o algunos minutos más por los programas de la PC. Así, el reconocimiento de la estación Link sólo implica que los mensajes se consiguen hasta la tarjeta del adaptador. Muchos clientes IBM tienen algunas versiones de la estación Link, sin darse cuenta de que es técnicamente una violación de la arquitectura SNA. Por ejemplo, todas las unidades de control (3174) que actúan como un gateway (pasarela) de Token-Ring (aún siendo remoto a una línea SDLC o local a un canal mainframe) está esencialmente creando una falsa estación Link. La pasarela (3270) SNA funciona en una PC, y también es un truco de estación Link (redireccionando los números LU de los paquetes antes de enviar los datos). APPN suministra una herramienta propia para uso de microcomputadoras como encaminadores.

La decisión inicial de IBM, tenía restricciones poco razonables, entonces se suspende la actualización de la arquitectura, y se resuelve el problema por la supervivencia del diseño original de red. Finalmente se engaña a los clientes para rechazar la admisión de la confusión subrayada por todos los errores cometidos con el mantenimiento de la tecnología.

2.4.4.11 MULTISYSTEM NETWORKING FACILITY (MSNF)

El MSNF (Facilidad Multisistema de Conexión de Redes), es una posible implementación de la arquitectura SNA: Permite la interconexión de diversas SNA's de un sólo nodo principal y sus respectivos dominios formando una red multiprincipal de mayor tamaño. MSNF proporciona una estructura de proceso distribuido de gran tamaño que permite compartir recursos entre los distintos puntos de la red. Las terminales pueden acceder a cualquier aplicación controlada por el MSNF en cualquier nodo, accediendo directamente a través de los procesadores de comunicaciones local y remoto. Además, dos programas de aplicación pueden comunicarse a través de los dominios, empleando MSNF. El MSNF contiene unas tablas con los recursos que pertenecen a los dominios y que se comparten con otros dominios. La tablas son parte del **Punto de Control de Servicios del Sistema y del Gestor de Recursos de Dominio Cruzado (GRDC Cross-Domain Resource Manager)**. Una sesión de dominio cruzado se inicia por medios de dos GRDC's intercambiando mensajes de protocolo, determinando la validez de la petición de sesión determinando si los recursos pedidos están disponibles y agrupando juntos a todos los usuarios de la sesión. Los recursos de dominios cruzados se almacenan en las **Tablas de Recursos de Dominios Cruzados (Cross-Domain Resources Tables**). Cada entrada contiene el nombre una LU o un programa de aplicación y el nombre del GRDC que posee el recurso

2.4.4.12 MODENAME, LIMITES DE SESION Y CLASES DE SERVICIO

SNA define **MODENAME** como un método de selección entre los diferentes caminos del mismo servidor. Esto, normalmente no es importante, en máquinas AIX o PS/2 tienen sólo un camino posible SNA hacia el host. Además SNA permite limitar el número de respuestas concurrentes entre el mismo cliente y el servidor LU's, aunque esto generalmente no es nada provechoso. Clases de servicio. Dos departamentos se conectan por una red SNA. Dos teléfonos unidos son capaces de llevar el tráfico, cada uno a una velocidad distinta. Uno corre a una velocidad de 19,299 bits por segundo, y el otro va a alta velocidad (1.5 millones de bits por segundo) pero por medio de satélite. La señal lleva unos pocos segundos, se pondría en marcha hacia el satélite, así si dos mensajes cortos empiezan por las dos líneas al mismo tiempo, la línea telefónica ordinaria enviaría el mensaje más rápidamente. Cuanto mayor cantidad de información, la mayor velocidad de la línea por satélite hace más sencilla la transmisión si el primer bit se retrasa unos pocos segundos antes de llegar a su destino. Este tipo de problema es comúnmente referido como Clase de servicio. Son las líneas de salida de la versión de red de mercado. Algunas líneas son de 12 ítems o menos, y permiten un rápido procesamiento de preguntas triviales. Las otras líneas son diseñadas para un volumen de procesamiento (que es generalmente llamado throughput rendimiento el total aumento del volumen de datos procesados en horas extraordinarias).

MODENAME. En SNA, la Clase de servicio es diseñada seleccionando el MODENAME. Aunque en su intento original de la arquitectura, MODENAME incluye el significado de muchas cosas diferentes.

- Puede ser un informe de prioridad. Uno podría usar MODENAME para distinguir entre datos en tiempo real importantes y prioridad baja de un volumen de datos transferidos en Background.
- Puede seleccionar una estrategia para responder. Si una conversación envuelve pequeños cambios (RPC), elegiría el camino más rápido. Cuando una gran cantidad de datos sea transferida, una corriente de información throughput sería el objetivo.
- Puede responder a un nivel especial de seguridad. Por ejemplo, una velocidad baja para un enlace punto a punto, se puede preferir a LAN's de alta velocidad, si la LAN contiene inseguridad en las terminales de usuario o estaciones de trabajo.

- En SNA Clásica, MODENAME fue utilizada para distinguir diferentes tamaños de pantalla y color o monocromo de 3270. En tráfico programa a programa, MODENAME es un parámetro sobre la sesión que la aplicación cliente puede escoger y la aplicación servidor puede preguntar. Por otro lado, un grupo de valores MODENAME idénticos, podrían ser configurados para que tengan un significado concreto para la familia de programas.

Algunas máquinas MODENAME deben estar configuradas para todos los nodos clientes-servidor de SNA. En OS/2 el gerente de comunicaciones sustituye unos pocos nombres, incluyendo un nombre por defecto BLANK. Así, si hay un mainframe, podrías necesitar tener espacio para los nombres de programadores VTAM originalmente creados.

2.4.4.13. CNOS Y SESIONES LIMITE

.

Una característica clave de APPC es que estas sesiones son establecidas entre subsistemas en dos computadoras, en lugar de entre programas de aplicación. Por la misma razón, SNA considera importante limitar el número de sesiones concurrentes. Esto tiene una gran influencia en los antiguos sistemas que estaban más limitados en memoria. Si un programa de aplicación empieza y todas las sesiones permitidas están en uso por otras aplicaciones, entonces un nuevo programa espera hasta que una sesión existente sea desasignada cuando una de las transacciones previas termine. Si una máquina está siempre actuando como cliente, y la otra máquina es siempre el servidor, entonces no hay conexión para las sesiones. Aún así, cuando ambas computadoras contienen una mezcla de clientes y servidores, entonces el problema puede aparecer. Si suponemos que un número máximo de sesiones han sido creadas y una de las sesiones no está actualmente en uso. Suponemos entonces que un programa cliente empieza para las dos computadoras. ¿Quién consigue utilizar la sesión?, y ¿quién tiene que esperar?. Cada sesión tiene una política distinta. Cuando una sesión es creada, uno de las dos computadoras es declarada para estar en contienda ganadora. Cuando el programa cliente empieza simultáneamente en las dos computadoras, la utilización de la sesión será dar primero el cliente a la computadora que está conectada como contienda ganadora para esta sesión. La primera vez que los subsistemas APPC en dos computadoras establecen una conexión, ellos tienen que negociar el número permitido de sesiones y la distribución de contiendas ganadoras de varias sesiones. Si los programadores han sustituido los mismos parámetros sería un problema. Aún así, si una computadora ha sido configurada para muchas más sesiones que la otra computadora, entonces las modificaciones se deben realizar. Este proceso es llamado **CNOS**.CNOS funciona por el intercambio de información en una sesión de control especial entre los dos subsistemas. Esta sesión de control se mantiene activa. Más tarde, el operador puede cambiar de forma dinámica el número de sesiones permitidas. Hasta es posible drenar la conexión entre las computadoras enviando una sesión límite a 0, después de esto, cuando cada transacción activa finalice, las sesiones que se estaban usando serán cerradas, y ninguna sesión o transacción podría empezar.

2.4.5 X.25

2.4.5.1 INTRODUCCIÓN

La norma X.25 es el estándar para redes de paquetes recomendado por CCITT, el cual emitió el primer borrador en 1974. Este original sería revisado en 1976, en 1978 y en 1980, y de nuevo en 1984, para dar lugar al texto definitivo publicado en 1985. El documento inicial incluía una serie de propuestas sugeridas por Datapac, Telenet y Tymnet, tres nuevas redes de conmutación de paquetes. X.25 es un conjunto de protocolos usados para establecer la conexión entre el **equipo terminal de datos (Data Terminal Equipment o DTE)** y el **equipo de terminación de circuito de datos (Data Circuit Terminating Equipment o DCE)** de una red de **conmutación de paquetes (Packet Switched Data Network o PSDN)**. Es decir, X.25 se utiliza como protocolo en la interfaz de acceso a una red de conmutación de paquetes. X.25 trabaja sobre servicios basados en **circuitos virtuales (VC)**. Un circuito virtual o canal lógico es aquel en el cual el usuario percibe la existencia de un circuito físico dedicado exclusivamente a la computadora o equipo que el maneja, cuando en realidad ese circuito físico **dedicado** lo comparten muchos usuarios. Mediante diversas

técnicas de multiplexado estadístico, se entrelazan paquetes de distintos usuarios dentro de un mismo canal. Las prestaciones del canal son lo bastante buenas como para que el usuario no advierta ninguna degradación en la calidad del servicio como consecuencia del tráfico que le acompaña en el mismo canal, esta ventaja sólo es apreciada en el tráfico de voz ya que en audio y video a cierta degradación. Para identificar las conexiones en la red de los distintos DTE, en X.25 se emplean **Números de Canal Lógico (LCN)**. Pueden asignarse hasta 4,095 canales lógicos y sesiones de usuario a un mismo canal físico. Para que las redes de paquetes y las estaciones de usuario se puedan interconectar se necesitan unos mecanismos de control, siendo el más importante desde el punto de vista de la red, el C**ontrol de Flujo**, que sirve para evitar la congestión de la red. También el DTE ha de controlar el flujo que le llega desde la red. Además deben existir procedimientos de **Control de Errores** que garanticen la recepción correcta de todo el tráfico. X.25 proporciona estas funciones de control de flujo y de errores.

El estándar X.25 no incluye algoritmos de encaminamiento, pero conviene resaltar que aunque las interfaces DTE/DCE de ambos extremos de la red son independientes uno de otro, X.25 interviene desde un extremo hasta el otro, ya que el tráfico seleccionado se encamina desde el principio hasta el final. A pesar de ello, el estándar recomendado es asimétrico ya que sólo se define un lado de la interfaz con la red (DTE/DCE). En general, X.25 se utiliza como infraestructura de Red de Area Extensa (WAN), permitiendo establecer conexiones entre diferentes localizaciones de una Organización donde sean necesarias muchas conexiones simultáneas entre pares de computadoras que cooperan entre sí para ejecutar ciertas aplicaciones. Entre estas aplicaciones podemos encontrar: correo electrónico (e-mail), acceso remoto a ficheros o transferencia de ficheros, acceso remoto a bases de datos para su actualización o para realizar una consulta, etc.. En muchos casos puede resultar prohibitivo utilizar líneas alquiladas entre cada par de computadoras. El hecho de tener acceso a una red de conmutación de paquetes (PSDN) da a la Organización una gran flexibilidad a la hora de añadir o quitar computadoras centrales con interrupciones mínimas del servicio.

X.25 también puede usarse como una WAN para interconectar Redes de Area Local (LAN), lo cual aumenta las posibilidades de explotación de la conexión a la PSDN. Las redes de conmutación de paquetes (PSND) y las LAN tienen diferentes velocidades de transmisión, siendo la velocidad de una PSDN significativamente menor, de ahí que las velocidades de transmisión deban ser limitadas cuando se establece una conexión a través de una PSDN. X.25 puede usarse como protocolo de WAN para establecer comunicaciones con socios comerciales, otras organizaciones, proveedores y clientes, tanto a nivel nacional como internacional. Sin embargo, las comunicaciones abiertas a nivel internacional sólo son posibles si existe un servicio público de PSDN en cada uno de los países que intervienen en la comunicación. X.25 podría usarse eficazmente ahí donde exista la necesidad de transmitir volúmenes relativamente pequeños de información durante conexiones de larga duración, como es el caso de algunas sesiones remotas, dependiendo de la estructura de tarifas. Sin embargo, no debería usarse X.25 para aplicaciones en tiempo real que requieran velocidades de transmisión de datos muy altas o tengan unos requisitos de funcionamiento muy exigentes, como puede ser el caso de las aplicaciones de diseño/fabricación asistidos por ordenador "CAD/CAM" (computer aided design/computer aided manufacturing), igualmente para la transmisión de audio y video en tiempo real. X.25 proporciona un probado método de transmisión de información muy fiable, eficaz, seguro y económico, utilizado ampliamente por empresas telefónicas. Las razones por las que se hace aconsejable la utilización de la norma X.25 son las siguientes:

- La adopción de un estándar común a distintos fabricantes nos permite conectar fácilmente equipos de distintas marcas.
- La norma X.25 ha experimentado numerosas revisiones y hoy por hoy puede considerarse relativamente madura.
- El empleo de una norma tan extendida como X.25 puede reducir sustancialmente los costos de la red, ya que su gran difusión favorece la salida al mercado de equipos y programas orientados a tan amplio sector de usuarios.
- Es mucho más sencillo solicitar a un fabricante una red adaptada a la norma X.25 que entregarle un extenso conjunto de especificaciones.

- El nivel de enlace HDLC/LAP-B sólo maneja los errores y lleva la contabilidad del tráfico en un enlace individual entre el DTE/DCE, mientras que X.25 va más allá, estableciendo la contabilidad entre cada DTE emisor y su DCE y entre cada DTE receptor y su DCE, es decir, el servicio extremo a extremo es más completo que el de HDLC/LAP-B.

El servicio que ofrece es orientado a conexión (previamente a usar el servicio es necesario realizar una conexión y liberar la conexión cuando se deja de usar el servicio), fiable, en el sentido de que no duplica, ni pierde ni desordena (por ser orientado a conexión), y ofrece multiplexación, esto es, a través de una única interfaz se mantienen abiertas distintas comunicaciones. El servicio X.25 es un diálogo entre dos entidades DTE Y DCE. Estudiaremos en X.25 desde el nivel Físico al nivel de Red. En primer lugar veamos cuál es la forma más común de conexión y lo que abarca cada nivel:

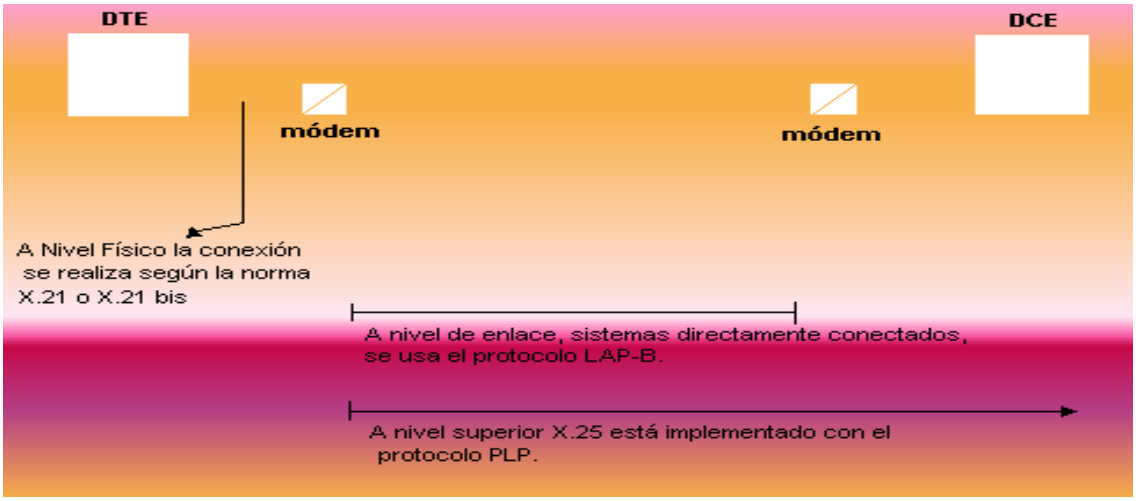


Figura 97 Conexión a X.25. Imagen enlace

Nomenclatura:
DTE (Data Terminal Equipment): Es lo que utiliza el usuario final (PC con placa X.25 por ejemplo). Es el equipo terminal de datos. Incorpora los niveles 2 y 3.
DCE (Data Circuit Terminating Equipment): Podemos interpretarlo como un nodo local. A nivel de enlace (LAP-B) las conexiones se establecen DTE-DCE. Ahora con el nivel de red, ampliamos las comunicaciones más allá del DCE, que hace de interconexión. Sólo incluye el nivel 1.

Con X.25 no hay conexiones multipunto. Es un servicio punto a punto, por lo que sólo se puede conectar un DTE con otro DTE. La recomendación X.25 para el nivel de paquetes coincide con una de las recomendaciones del tercer nivel OSI. X.25 abarca el tercer nivel y también los dos niveles más bajos. La interfaz de nivel físico recomendado entre el DTE y el DCE es el X.21. X.25 asume que el nivel físico X.21 mantiene activados los circuitos **T** (transmisión) y **R** (recepción) durante el intercambio de paquetes. Asume también, que X.21 se encuentra en estado **13S** (enviar datos), **13R** (recibir datos) o **13** (transferencia de datos). Supone también que los canales **C** (control) e **I** (indicación) de X.21 están activados. Por todo esto X.25 utiliza la interfaz X.21 que une el DTE y el DCE como un **conducto de paquetes**, en el cual los paquetes fluyen por las líneas de transmisión (T) y de recepción (R). El nivel físico de X.25 no desempeña funciones de control significativas. Se trata más bien de un conducto pasivo, de cuyo control se encargan los niveles de enlace y de red.

2.4.5.2 SEGURIDAD

En X.25 se supone que el nivel de enlace es LAP-B. Este protocolo de línea es un conjunto de HDLC. LAP-B y X.25 interactúan de la siguiente forma: En la trama LAP-B, el paquete X.25 se transporta dentro del campo **I** (información). Es LAP-B el que se encarga de que lleguen correctamente los paquetes X.25 que se transmiten a través de un canal susceptible de errores, desde o hacia la interfaz DTE/DCE. La diferencia entre paquete y trama es que los paquetes se

crean en el nivel de red y se insertan dentro de una trama, la cual se crea en nivel de enlace. Para funcionar bajo el entorno X.25, LAP-B utiliza un subconjunto específico de HDLC. Los comandos que maneja son: Información (I), Receptor Preparado (RR), Rechazo (REJ), Receptor No Preparado (RNR), Desconexión (DSC), Activar Modo de Respuesta Asíncrono (SARM) y Activar Modo Asíncrono Equilibrado (SABM). Las respuestas utilizadas son las siguientes: Receptor Preparado (RR), Rechazo (REJ), Receptor No Preparado (RNR), Asentimiento No Numerado (UA), Rechazo de Trama (FRMR) y Desconectar Modo (DM). Los datos de usuario del campo **I** no pueden enviarse como respuesta. De acuerdo con las reglas de direccionamiento HDLC, ello implica que las tramas **I** siempre contendrán la dirección de destino con lo cual se evita toda posible ambigüedad en la interpretación de la trama. X.25 exige que LAP-B utilice direcciones específicas dentro del nivel de enlace. En X.25 pueden utilizarse comandos SARM y SABM con LAP y LAP-B, respectivamente. No obstante se aconseja emplear SABM, mientras que la combinación SARM con LAP es poco frecuente. Tanto X.25 como LAP-B utilizan números de envío (S) y de recepción (R) para contabilizar el tráfico que atraviesan sus respectivos niveles. En LAP-B los números se denotan como N(S) y N(R), mientras que en X.25 la notación de los números de secuencia es P(S) y P(R).

2.4.5.3 NIVELES DE X.25

2.4.5.3.1 NIVEL FISICO

La interfaz de nivel físico regula el diálogo entre el DCE y el DTE. Se describe desde 3 puntos de vista distintos:

- Mecánico
- Eléctrico.
- Funcional.

Existen dos posibilidades para la interfaz a nivel físico:

- **X.21**.-Se utiliza para el acceso a redes de conmutación digital (similares a las de telefonía digital.)
- **X.21bis**.-Se emplea para el acceso a través de un enlace punto a punto (Similar a RS-232 en modo síncrono.).

En cuanto la interfaz mecánica, se usan conectores Canon DB15 (de 15 pines, para X.21) o DB25 (de 25 pines para X.21 bis). En cuanto a la interfaz eléctrica X.21 utiliza X.26, que es una interfaz no balanceada, por lo que se suele usar mejor X.27 que es balanceada y, por tanto, permite tasas de transmisión superiores. La interfaz eléctrica de X.21bis está recogida en la norma V.28. Las velocidades se mueven entre los 64kbps y los 2Mbps, velocidades que pueden parecer bajas y, de hecho, así son. X.25 presenta un problema de baja eficiencia por la exagerada protección contra errores que implementa.

2.4.5.3.2 NIVEL DE ENLACE (LAP-B)

Ya sabemos que el objeto del nivel de enlace es garantizar la comunicación entre dos equipos directamente conectados. En X.25, este nivel queda implementado con el protocolo **LAP-B (*L*ink *A*ccess *P*rocedure - B)** que es un protocolo HDLC 2,8, es decir, con rechazo simple, indicado por el 2, y en el cual las tramas de información pueden ser utilizadas como tramas de control, indicado esto último por el 8. El servicio que ofrece el nivel 2 al nivel superior es orientado a conexión, fiable y en modo paquete. El nivel 2 sólo ofrece una conexión al nivel superior. El nodo local es el que presta servicio al DTE conectado a él. El nivel de enlace no resuelve el servicio extremo a extremo. La comunicación extremo a extremo la resuelve el nivel de red. El diálogo entre entidades de enlace es salto a salto. Por tanto, existen tantas conexiones de enlace como unidades tengamos entre el DTE local y DTE remoto.

El nivel de enlace recibe peticiones del nivel de red, mediante primitivas, para que transmita un bloque de información. Se pasa una **SDU** del nivel de red al nivel de enlace. El nivel de enlace le añade una cabecera y un trailer con objeto de detectar y evitar errores. Todo junto es una trama del nivel de enlace, figura 98.

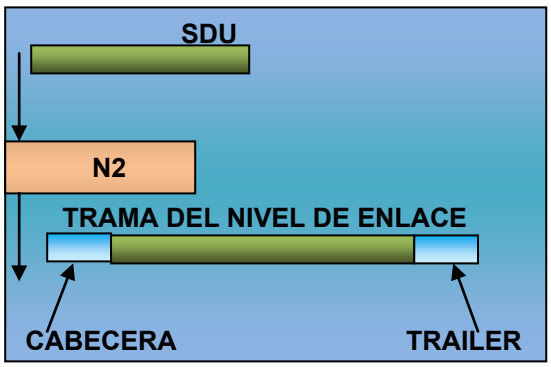


Figura 98

Hemos de distinguir aquí entre lo que es una **SDU** y lo que es una **PDU**:

- SDU.-Bloque de información que se intercambian dos niveles consecutivos.
- PDU.-Estructura de datos que se intercambian dos entidades gemelas.

La trama del nivel de enlace pasa al nivel físico, quien la transforma en binario y la pasa como señal al medio físico, por donde se transmite. Si la trama no sufre errores llega a destino perfectamente. La entidad gemela puede reconstruir la trama porque sabe donde empieza y termina gracias a la información de control que metimos en la cabecera y el trailer. La parte central de la trama (campo de información) es extraída por la entidad de protocolo del nivel de enlace y se entrega al nivel superior. Esto ocurre en ausencia de errores. Por tanto el nivel de enlace permite que los niveles de red de las entidades gemelas puedan intercambiar PDU's.

2.4.5.3.3 EL NIVEL DE RED

2.4.5.3.3.1 INTRODUCCION

Este nivel está especificado por el protocolo **PLP (Packet Layer Protocol)** que es un protocolo de acceso a nivel de red y que proporciona un servicio al nivel superior:

- De subred (SNACP).
- Modo paquete
- Orientado a conexión.
- Fiable.
- Multiplexión: uso de una conexión para varias comunicaciones simultáneas. El DTE origen dialoga con su nodo, pero **virtualmente** lo hace con todos los DTE's multiplexados.

2.4.5.3.3.2 Circuitos virtuales (CV)

Podríamos definirlos como la asociación lógica entre usuarios para comunicarse entre ellos. En X.25 hay 2 tipos de CV:

- **Conmutados (CVC)**.-Hay que realizar un diálogo previo a la transmisión con el nodo local para establecerlos y para liberarlos.
- **Permanentes (CVP)**.-Están establecidos de antemano (por contrato), así que no hace falta **fase de establecimiento, ni de liberación**. Se preconfiguran los nodos de tal forma que, por contratación, el circuito está permanentemente establecido. Son muy útiles si se transmite mucho y con mucha frecuencia hacia un mismo destino.

Se identifican dentro de cada DTE por el número de canal lógico (NCL), que se negocia en la fase de establecimiento (sólo CVC's). Podría además tener, por ejemplo, varios CV's establecidos con la misma máquina (cada uno con distinto NCL evidentemente). En la figura 99 se muestra como la multiplexión que se ofrece al nivel de transporte, no es tal a nivel de enlace: en LAP-B sólo hay una conexión. La multiplexión se resuelve a nivel de red, aunando las diferentes conexiones (asimilables a CV's) que aparecen en el **NSAP (Punto de Acceso al Servicio a Nivel de Red)**, en la que se ve desde el nivel de enlace en el **LSAP**.

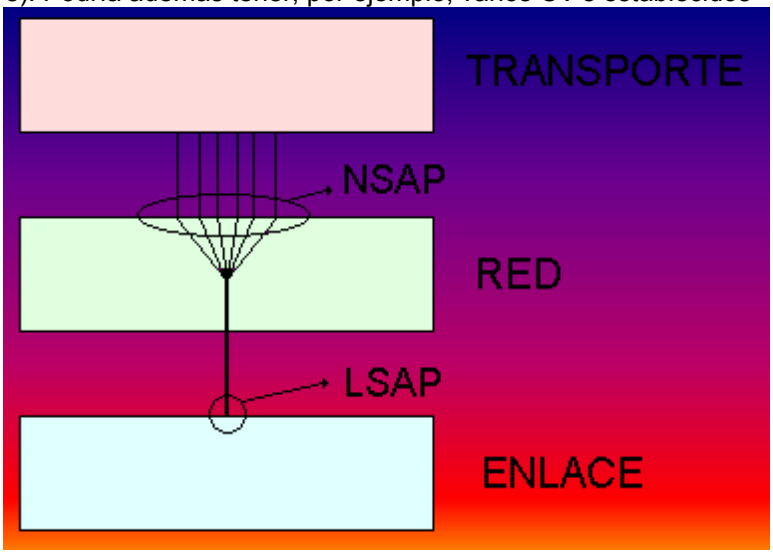


Figura 99

2.4.5.3.3.3 PROTOCOLO

- **Fase de Establecimiento**.-En la figura 100 hemos supuesto que la llamada es aceptada, pero podría ser rechazada. Esta fase sólo tiene lugar para CVC's. Llegados a este punto ambos lados estarán seguros de que la conexión se estableció bien.
- **Fase de Transferencia**.-Como veremos, los datos pueden ser asentidos en el nodo local (caso "a"), o en destino ("b").
- **Fase de Liberación**.-La liberación a su vez puede ser solicitada por uno de los dos lados ("a") o por la propia red ("b").

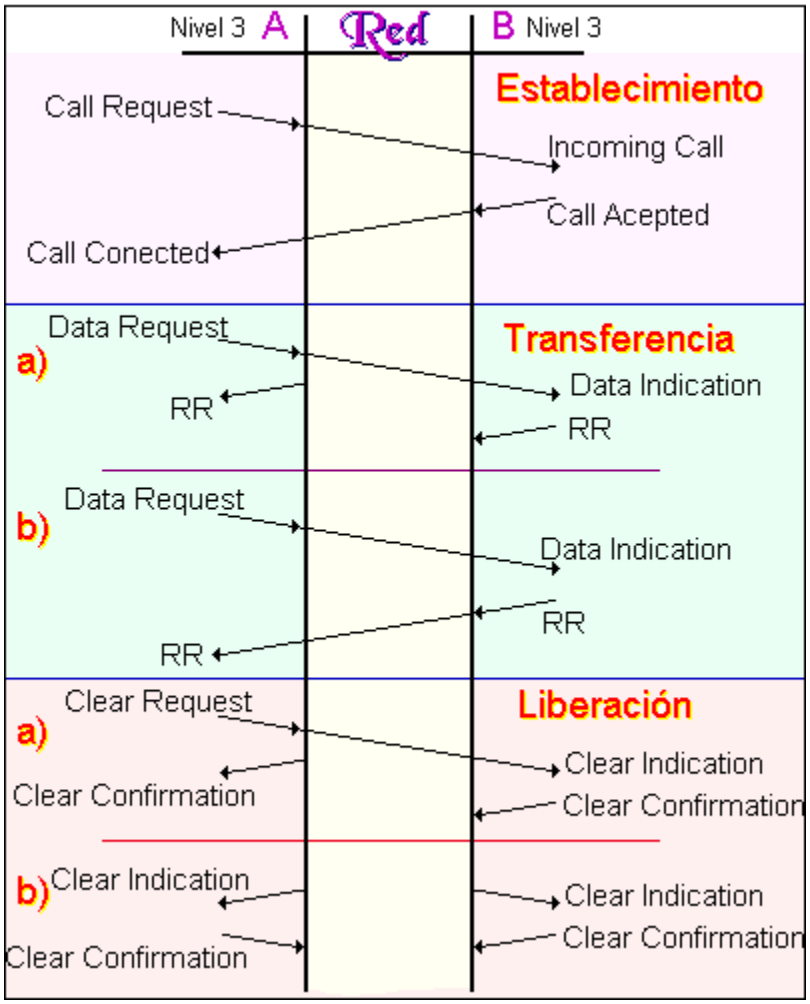


Figura 100 Fases de la Transmisión

Los que dialogan son los dos PLP's. El nivel de enlace sólo sirve de mensajero. Las direcciones a nivel de enlace son distintas de las de nivel de red. Con la dirección de enlace llego al primer nodo. Ahí se desencapsula y se usa la de red para llegar a los demás.
NOTA: A nivel de paquete no tenemos retransmisiones. Sí hay control (detección) de errores, pero no corrección.

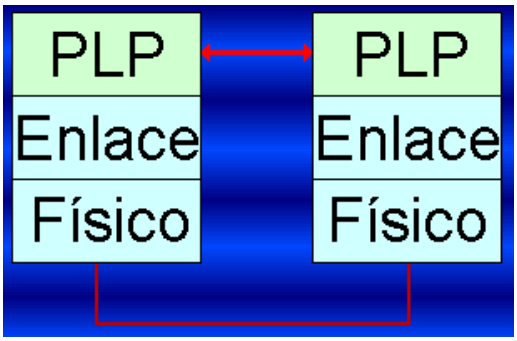


Figura 101 Gráfica esquemática con los niveles OSI

2.4.5.3.3.4 NUMERO DE CANAL LÓGICO (NLC)

Es un número que permite identificar al CV involucrado en una determinada transferencia y que es distinto a cada lado de la comunicación, aunque el CV sea el mismo. El rango de NCL que pueden usarse, es algo a negociar con la empresa que ofrece el servicio. Más NCL, mayor número de CV's establecibles. Un NCL se especifica con 12 bits, lo cual da lugar a que puedan usarse como máximo 4,095 NCL's (el 0 tiene un significado especial).

Utilización.-Los NCL's se escogen por el DTE o por el DCE (la red en el fondo) cuando se necesitan, liberándolos cuando los acaban de usar. Ambos tienen una lista donde marcan los NCL's libres y ocupados (lo que se marca en una lista se refleja inmediatamente en la otra). El DTE empieza a escoger por los NCL's de mayor numeración. El DCE (la red) empieza por los de menor numeración. Podría ocurrir que se junten **en el centro** (los DTE vienen de arriba y los DCE de abajo) y esto desemboca en varias posibilidades:

- Que cuando DTE o DCE vayan a escoger un número, en sus listas figuren todos como ocupados. En este caso, no se aceptarían sus paquetes.
- Que sólo quede un NCL por elegir y los dos lo escojan al mismo tiempo. En este caso la red (DCE) tendría prioridad. La conexión del DTE se contesta con un **clear** desde la red y se rechaza figura 102 a la derecha.

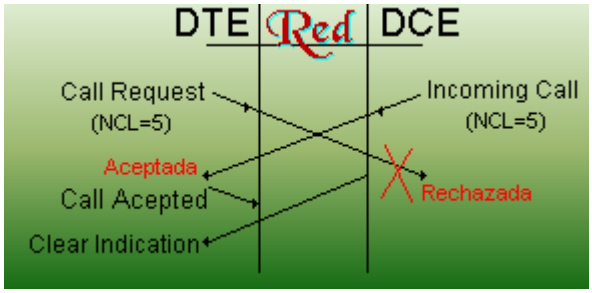
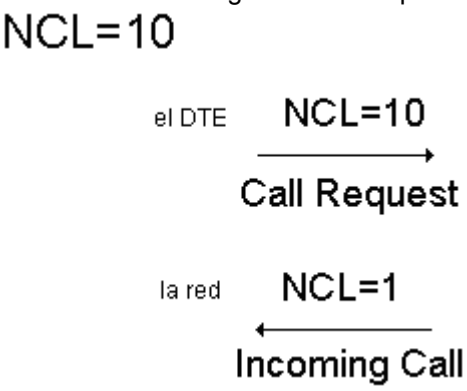


Figura 102 Ejemplos del uso de NCL's.

Comentario a la Figura 102:
En respuesta a un **Call Request** anterior (que el DTE asignó sin problemas al NCL 6 por ejemplo), el DCE trata de asignar el NCL 5 pues lo ve libre. Así el CV de esa conexión tendría asociado el NCL 6 en el DTE y el 5 en el DCE. Al mismo tiempo el DTE ha visto libre el NCL 5 y trata de establecer un nuevo CV asignándoselo Como consecuencia de esto es la operación del DCE (de la red) la que se acepta, rechazándose el Call Request del DTE. Una posible solución para evitar colisiones de este tipo, es dividir por rangos la oferta de NCL's. Por ejemplo asignar una cierta cantidad de números para CV's entrantes, otra para salientes y otros que fuesen bivalentes. Así sólo habría colisión en los bivalentes, pues los entrantes y salientes sólo podrían ser elegidos por DTE y DCE respectivamente.



2.4.5.3.3.4.1 ESTADOS DE LOS CANALES LOGICOS

Los estados de los canales lógicos constituyen la base de la gestión del enlace entre el DTE y el DCE. Mediante los distintos tipos de paquetes, el canal lógico puede tomar uno de los siguientes estados:

Numero del estado.....Descripción del estado.
p1 o d1 o r1.....Nivel de paquetes preparado.
p2..... DTE en espera.
p3..... DCE en espera.
p5..... Colisión de llamadas.
p4..... Transferencia de datos.

p6..... Solicitud de liberación del DTE.
p7..... Indicación de liberación del DCE.
d2..... Solicitud de reinicialización del DTE.
d3..... Indicación de reinicialización del DCE.
r2..... Solicitud de reiniciación del DTE.
r3..... Indicación de reiniciación del DTE.

2.4.5.3.3.5 PDU's EN EL NIVEL DE RED EN X.25

Para el estudio del PLP vamos a ver el formato de sus PDU's, las cuales están alineadas a octetos. El formato de una PDU general del PLP es el mostrado en la figura 103.

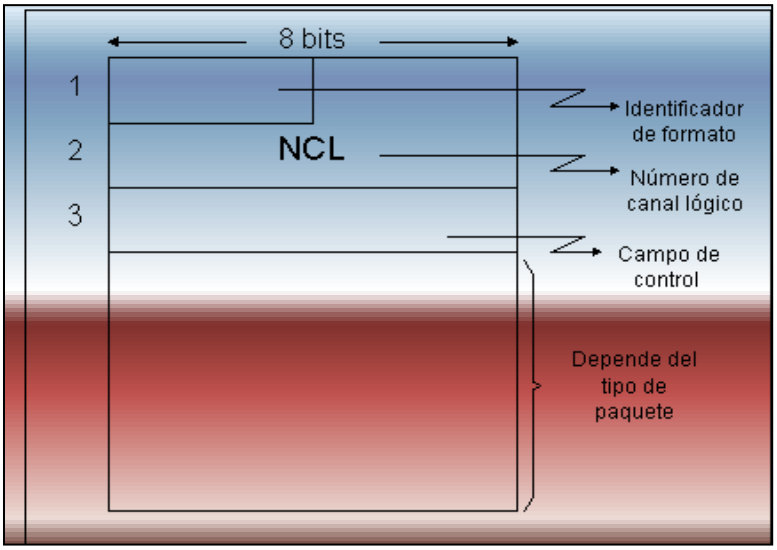


Figura 103

Para profundizar en el estudio de este nivel vamos a ver con más detalles los siguientes paquetes:

- Paquete de petición de llamada y paquete de llamada entrante.
- Paquete de llamada aceptada y paquete de comunicación establecida.
- Paquete de liberación de conexión y paquete de indicación de liberación.
- Paquete de confirmación de liberación.
- Paquete de datos.
- Paquetes de asentimiento y control de flujo.
- Paquete de reinicio.
- Paquete de rearranque.
- Paquete de interrupción

X.25 permite implementar un procedimiento multienlace.

SERVICIO DE RED ORIENTADO A CONEXION (CO)

Todo servicio CO tiene tres fases, y cada una de ellas presenta sus correspondientes funciones

- **Conexión**.-En esta fase se definen las siguientes funciones:
  - **Connect.Request** (Equivale a marcar en telefonía).
  - **Connect.Indication** (Equivale al tono de llamada).
  - **Connent.Response** (Equivale a descolgar).
  - **Connect.Confirm** (Equivale a la percepción del que llama)

Los parámetros que se intercambian en esta fase entre los niveles 3 y 4 son entre otros la dirección y el QoS (permite pedir la calidad que le exigimos a la red para la conexión)

- **Transferencia**.-En esta fase se definen las siguientes funciones:
  Data Request
  Data Indication
  Una para enviar y otra para recibir datos.

Nota: Esto mismo se puede expresar gráficamente como en la figura104

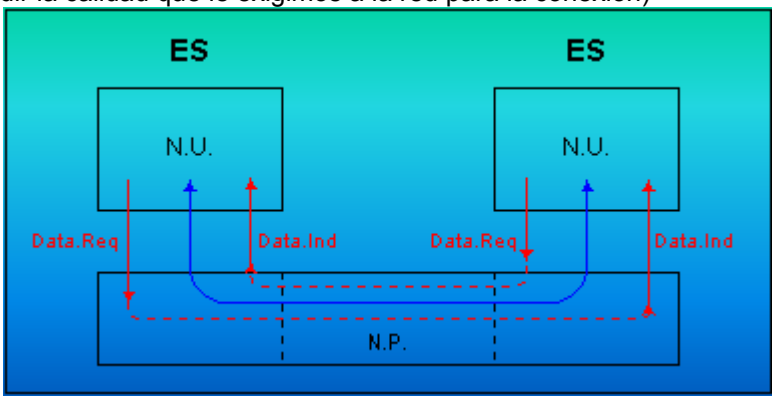


Figura104

O en el tiempo como:

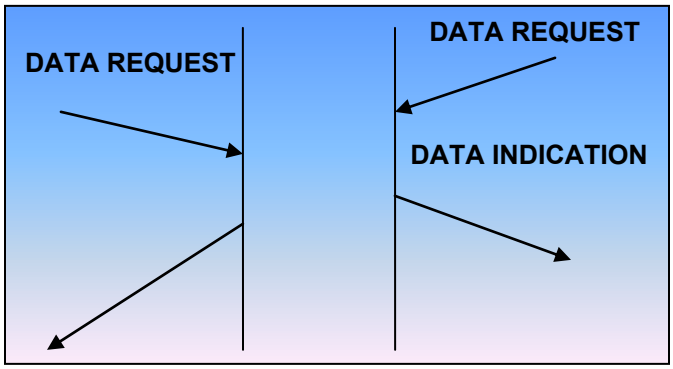


Figura 105

Se observa que en la definición no hay una función que indique que ha pasado con los datos. Por tanto, los servicios CO son servicios no confirmados (en cuanto a la transferencia de datos). En un servicio CO puede no existir limitación ni en la longitud de los datos, ni en el ritmo al que se envían (puede ser un servicio ilimitado) ya que al llegar los paquetes en orden se pueden realizar protocolos sencillos de reconstrucción de la información.

- **Liberación**.-En esta fase de un servicio CO se definen las siguientes funciones:
  - **Disconnect Request**
  - **Disconnect Indication**

  Por la definición, un servicio CO es un servicio no confirmado en cuanto a la liberación de la conexión. También se observa en la definición que la liberación la puede pedir cualquiera de las partes. Un servicio CO es un servicio disruptivo (si lo invocas puede provocar pérdida de información) porque si se libera el circuito la red puede borrar los datos en tránsito. Hay que destacar que esta última característica de los servicios CO, al igual que la de ser limitados en cuanto a la transferencia de datos, no son parte de la definición de un servicio CO sino que dependen de como están implementadas en cada red concreta.

Los niveles de red de las entidades que quieren establecer la comunicación intercambian PDU's (o paquetes) mediante los servicios prestados por el nivel de enlace. Estos paquetes se estructuran en:

- Paquetes para establecimientos de conexiones.
- Paquetes para el intercambio de datos normales.
- Paquetes para el intercambio de datos acelerados.
- Paquetes para el reinicio y rearranque de conexiones.
- Paquetes para la liberación de conexiones.

La recomendación X.121 (se pueden usar otras opcionalmente) específica el formato de las direcciones, figura 106:

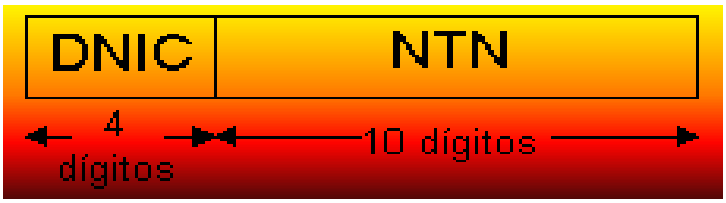


Figura 106 Formato de las direcciones

Según X.121 las direcciones se estructuran en 2 campos:

- **DNIC (Data Network Identifier Code)**.-Identifica a cada red X.25 y distingue al operador público. Es único a nivel mundial. Tiene 4 dígitos decimales.
- **NTN (Network Terminal Number)**.-Número de abonado (hasta 10 dígitos).

Esta estructura obedece a una convención administrativa de la red. Este tipo de dirección posibilita el encaminamiento jerárquico.
Codificación.-La codificación se hace en BCD; concretamente se usa un octeto para cada 2 dígitos. En algunas ocasiones, el número de dígitos es impar lo cual da lugar a medio octeto sobrante y luego veremos que probablemente habrá que usar un relleno (**pading**).
Utilización.-Usar siempre el DNIC, incluso si llamo a mi propia red. No usar el DNIC internamente (sólo NTN) y usar para llamadas externas 0+DNIC+NTN.

El protocolo LAP-B (Link Access Procedure - B) es un protocolo HDLC 2,8, el formato de las tramas se muestra en la figura 107.

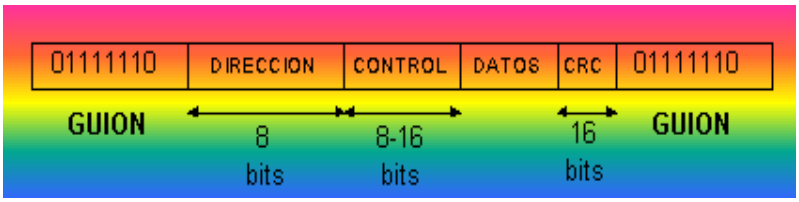


Figura 107 Trama LAP-B

Analizamos más a fondo los tres tipos de tramas que se manejan:

- **Tramas de información**.-El campo de control se muestra en la figura 108:

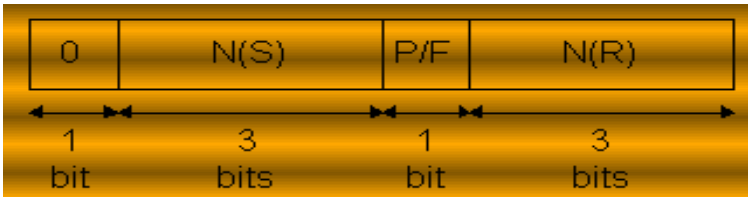


Figura 108 campo de control de una trama de información

0 -Indica que la trama es de información.
P/F -Regula el control de acceso al medio.
N(S) -Número de secuencia en transmisión (caben hasta ocho números diferentes).
N(R) -Número de secuencia en recepción.
N(S) y N(R) se usan para intensificar el flujo entre emisor y receptor, incorporando el método de las ventanas deslizantes. Con N(S) se indica la trama que se envía, y con N(R) se asienten tramas recibidas, es decir, se hace uso del piggybacking: cuando la comunicación es fuertemente bidireccional, en vez de enviar tramas de control conteniendo los asentimientos de recepción, los envió en las tramas de información, indicando la última trama que ha llegado correctamente. Es necesario indicar que existe un formato extendido de tramas de información, con un N(S) de siete bits.

El primer bit es obligatoriamente un '0'. En segundo lugar se coloca el número de secuencia de la trama de información que se envía. A continuación existe un bit

denominado P/F. Es el bit **Poll/Final** de los protocolos HDLC. Por último, aparece un número de secuencia de asentimiento. Se utiliza **piggybacking**, esto significa que se aprovechan las tramas de información para mandar asentamientos. Si una terminal recibe correctamente una trama y él quiere enviar otra, no genera un ACK y después manda su trama sino que incorpora el asentimiento en la propia trama. Por esto, representaremos las tramas de información con una '**I**' seguida de dos números. Con I23, por ejemplo, quien lo manda envía el equivalente a lo que antes representábamos con I2 y ACK3, es decir, envía la trama 2 y advierte de que está esperando la trama 3 del otro interlocutor. En principio por defecto se utiliza numeración modulo 7 (3 bits), así, las tramas irán con números desde el 0 hasta el 7 ambos incluidos. Si el retardo de asentamiento, tiempo que transcurre desde que se envía el último bit de una trama hasta que se recibe su asentamiento, es muy alto, puede interesar aumentar la numeración para poder mandar más tramas en dicho tiempo de asentamiento. Este es el motivo por el que se permite utilizar numeración extendida a módulo 127 (7 bits).

- **Tramas de supervisión**.-El campo de control es como el de la figura 109:

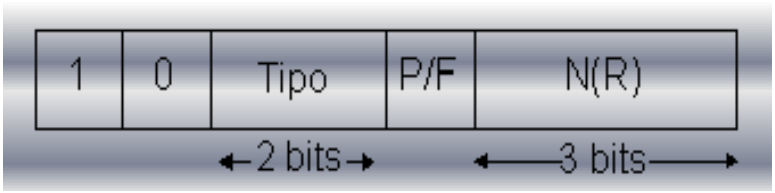


Figura 109 campo de control de una trama de supervisión

Hay cuatro tramas de supervisión:

- RR (receiver ready).
- RNR (receiver not ready).
- REJ.
- SREJ.
- RR y RNR son ACK's positivos, indican que la trama recibida es buena.

REJ y SREJ son asentimientos negativos, indican que la trama fue mal recibida; se usa REJ en el rechazo simple y SREJ en el rechazo selectivo. Además mediante RR y RNR se controla el flujo de la fuente mediante un mecanismo Xon-Xoff: con RNR se indica a la fuente que debe parar la transmisión, y con RR que se puede continuar la transmisión. y en el caso de numeración extendida figura 110.

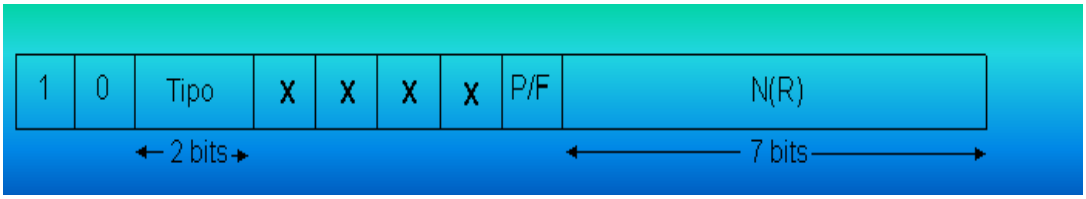


Figura 110 campo de control de una trama de supervisión con numeración extendida

Los tipos son mostrados en la tabla 19:

BITS	TIPO	SIGNIFICADO
00	RR (Receiver Ready)	ACK
01	REJ (Reject)	Informa de que una trama llegó mal
10	RNR (Receiver Not Ready)	Se avisa a la terminal origen que el receptor se desborda. Aún con esto se confirma la última trama recibida. El origen se queda parado hasta recibir un RR.
11	SREJ	Se utiliza en rechazo selectivo. Por tanto, no se usa en X.25.

Tabla 19

- **Tramas no numeradas**. El campo de control es el de la figura 111.

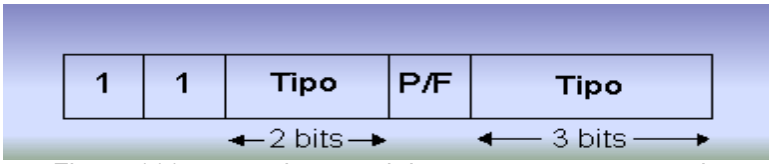


Figura 111 campo de control de una trama no numerada

Algunos tipos utilizados son:

- **SABM (*S*et *A*syncronous *B*alance *M*ode)**.-Sirve para configurar el receptor y el emisor. Se usa para establecimiento de conexión en modo asíncrono balanceado. Un **Connect-Request** del nivel superior produce que el transmisor transmita la trama SABM, la cual al ser recibida genera una señal de Connect-Indication; si la conexión es aceptada mediante la señal **Connect-Response**, el receptor envía la trama UA que indica aceptación de la conexión, la cual producirá al llegar a su destino **Connect-Confirm**.
- **UA (Unnumbered *A*CK)**.-Confirma tramas no numeradas que funcionan en modo parada y espera. Asentimiento no numerado, permite aceptar conexiones y desconexiones.
- **DISC**.-Se utiliza para desconectar.
- **SABME**.-Se configuran emisor y receptor acordando utilizar numeración extendida. Produce el reinicio de una conexión en modo asíncrono balanceado con formato extendido.
- **RESET**.-Ante situaciones irrecuperables se pone todo a cero y se informa al nivel superior de que ha habido un fallo grave. Produce el reinicio de una conexión; se inicializan todas las variables, se liberan los buffers, es como si la conexión empezara de nuevo. Puede ser destructor de información. El envío de esta trama es causada por **errores de protocolo**, es decir, errores ante los cuales los sistemas finales no pueden recuperarse, por ejemplo, la recepción de una trama no definida.

Analicemos un ejemplo completo para fijar todo lo explicado hasta ahora, figura 112. Detengámonos en esta figura para entenderla a fondo. Diferenciamos en este tipo de comunicaciones tres fases:

- **Establecimiento de conexión**.-En esta fase, un sistema final o DTE pide que se abra una comunicación con la trama SABM. En primer lugar, es importante señalar que el receptor será siempre un DCE puesto que trabajamos en el nivel de enlace, es decir, con comunicaciones entre entidades directamente conectadas. Con la trama citada, el DTE consigue informar al DCE de que características tendrá la comunicación que quiere establecer, en este caso por ejemplo, la numeración será la que exista por defecto y no será numeración extendida. Una vez recibida la trama correctamente en el DCE, éste contesta con **UA** para confirmar que la comunicación queda abierta. Hasta aquí, como podemos comprobar en la figura 112, se trabaja en modo parada y espera.

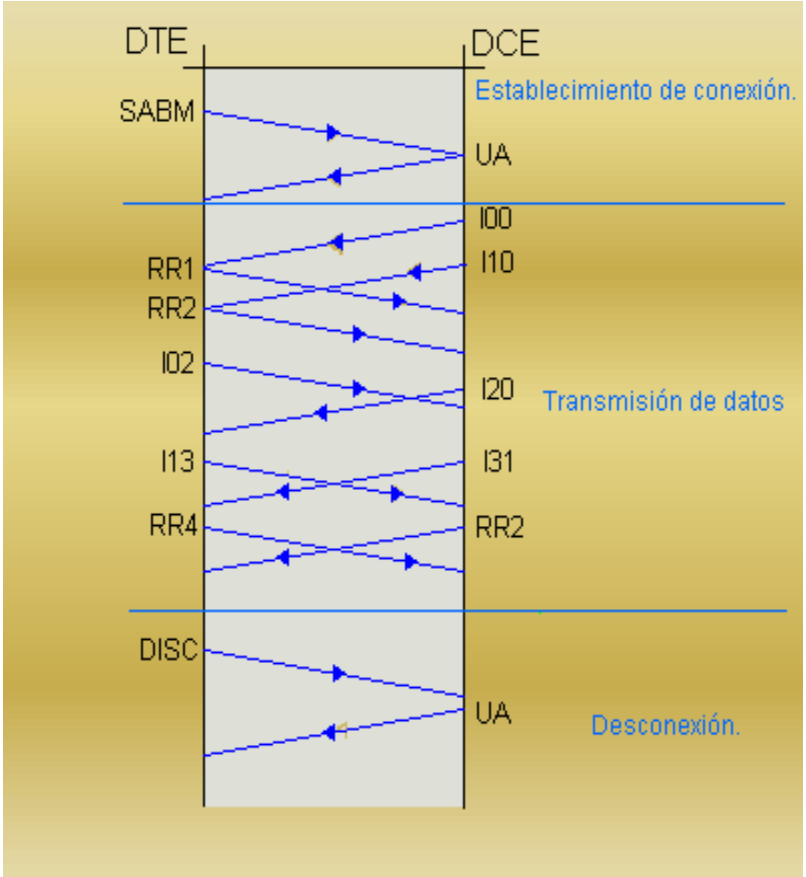


Figura 112 ejemplo de comunicación de LAP-B

- **Fase de transmisión de datos**.-Tras establecer la conexión y algunos de sus parámetros ya se puede pasar a mandar información. En el caso de la figura 112, es el DCE quien envía una trama, la trama I00. Como ya sabemos, esto quiere decir que la trama que se envía es la trama 0 y que el DCE está esperando recibir del DTE la trama 0. Tanto esta trama como la siguiente que manda el DCE, la I01, son confirmadas por el DTE con tramas RR. Como recordamos, no se asiente una trama con su número sino con el número de la trama que a partir de ese momento se espera, es decir, la siguiente a la que se confirma. Esta es la razón por la que I00 se confirma con RR1. La primera trama que envía el DTE es I02, es decir, en este punto él manda la trama 0 y está esperando la 2. Una vez llega ésta al DCE, éste la confirma con I31, esto es, mandando su cuarta trama e indicando que queda a la espera de la trama 1 del DTE. En el proceso ilustrado no figura ningún error pero, de haberlo, todo funcionaría como quedó descrito en ARQ con rechazo simple. Bien porque saltase un **TIMER** o por la recepción de una trama REJ se obligaría a la retransmisión a partir de la trama errónea. El proceso así descrito continuará, si no surge ningún problema irrecuperable, hasta que uno de los interlocutores pida la desconexión.

- **Desconexión**.-Una de las entidades envía la trama DISC que es confirmada con UA. Queda así la comunicación cerrada. Por último, estudiemos algunos parámetros que intervienen en la comunicación y que son modificables y configurables en función de las condiciones de la red:
  - **T1 o Plazo de Retransmisión**.-Es el tiempo que se espera desde la transmisión de una trama hasta su retransmisión por falta de ACK. Es el objeto del TIMER.
  - **T2 o Retardo Máximo antes de Asentimiento**.-Pueden no asentirse las tramas inmediatamente según llegan. Puede esperarse un tiempo menor que este T2 por si llegan más tramas que puedan ser asentidas todas juntas.

- **T3 o Plazo de Inactividad**.-Si transcurre un tiempo sin que se transmita o reciba nada se emite un RR asintiendo la última trama que hubiese llegado. Es necesario testear el enlace para comprobar un posible fallo grave como la caída de un nodo.
- **N1 o Longitud Máxima de la Trama.**
- **N2 o Número Máximo de Retransmisiones de una Trama**.-Si después de N2 retransmisiones de una trama, ésta no es asentida se resetea el enlace o se desconecta informando al nivel superior.
- **K o Tamaño de Ventana.**

En X.25 se especifican dos niveles y una interfaz figura 113.

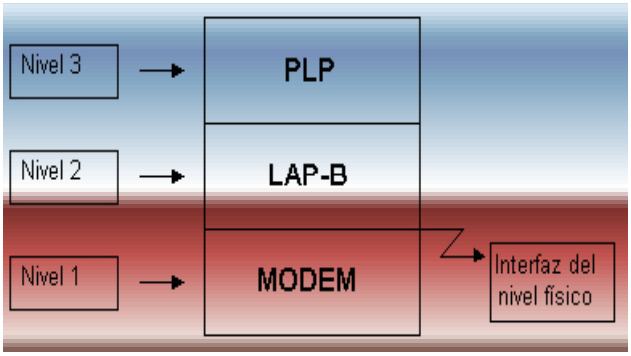


Figura 113

La interfaz del nivel físico separa el DTE del DCE. El DTE va desde el nivel 2 hacia arriba y es propiedad del usuario. El DCE incluye el módem y todo lo demás de la red; su propietario es el operador de red.

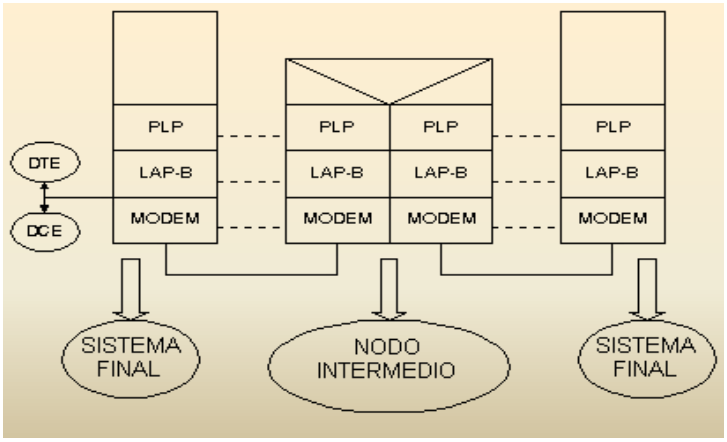


Figura 114

2.4.5.4 FORMATO DEL PAQUETE

En un paquete de datos, la longitud por omisión del campo de datos de usuario es de 128 octetos, aunque X.25 ofrece opciones para distintas longitudes. Otros tamaños autorizados son: 16, 32, 64, 256, 512, 1,024, 2,048 y 4,096 octetos. Los dos últimos valores fueron añadidos en la revisión de 1984. Si el campo de datos de un paquete supera la longitud máxima permitida el DTE receptor liberará la llamada virtual generando un paquete de reinicialización. Todo paquete que atraviesa la interfaz DTE/DCE con la red debe incluir al menos tres octetos, los de la cabecera del paquete, aunque esta puede incluir también otros octetos adicionales. Los 4 primeros bits del primer octeto contienen el número de grupo del canal lógico. Los 4 últimos bits del primer octeto contienen el identificador general de formato. Los bits 5 y 6 del identificador general de formato (SS) sirven para indicar el tipo de secuenciamiento empleado en las sesiones de paquetes. X.25 admite dos modalidades de secuenciamiento: módulo 8 (con números entre 0 y 7) y módulo 128 (con números entre 0 y 127). El bit **D**, séptimo bit del identificador general de formato sólo se utiliza en determinados paquetes. El octavo bit es el bit **O**, y sólo se emplea para paquetes de datos destinado al usuario final. Sirve para establecer dos niveles de datos de usuario dentro de la red.

El segundo octeto de la cabecera del paquete contiene el número de canal lógico (LCN). Este campo de 8 bits, en combinación con el número de grupo del canal lógico, proporciona los doce bits que constituyen la identificación completa del canal lógico; por tanto, son 4,095 los canales lógicos posibles. El LCN 0 está reservado para las funciones de control (paquetes de diagnóstico y de reinicialización). Las redes utilizan estos dos campos de diversas formas. En algunas se emplean combinados, mientras que en otras se consideran de forma independiente. Los números de canal lógico sirven para identificar el DTE frente al nodo de paquetes (DTCE), y viceversa. Estos números pueden asignarse a circuitos virtuales permanentes, llamadas entrantes y salientes, llamadas entrantes y por último llamadas salientes. Durante el comienzo del proceso de comunicación, es posible que el DTE y el DCE utilicen el mismo LCN. Así por ejemplo, una solicitud de llamada generada por un DTE podría emplear el mismo número de canal lógico que una llamada conectada correspondiente a un DCE. Para reducir al mínimo esta posibilidad, la red comienza a buscar un número a partir del extremo inferior, mientras que el DTE busca su número empezando por arriba. Si la llamada saliente (solicitud de llamada) de un DTE tiene el mismo LCN que una llamada entrante (llamada conectada) procedente del DCE de la red, X.25 liberará la llamada entrante y procesará la solicitud de llamada. Cuando el paquete no es de datos, el tercer octeto de la cabecera de paquete X.25 es el del identificador de tipo de paquete, mientras que cuando es de datos ese octeto es el de secuenciamiento.

En los paquetes de establecimiento de llamada se incluyen también las direcciones de los DTE y las longitudes de estas direcciones. El convenio de direccionamiento utilizado podría ser por ejemplo, el estándar X.121. Los campos de direccionamiento pueden estar contenidos entre el cuarto y el decimonoveno octeto del paquete de solicitud de llamada. En los paquetes de establecimiento de llamadas, estos campos de direccionamiento sirven para identificar las estaciones interlocutoras: la que llama y la que contesta. A partir de este momento, la red utilizará los números de canal lógico asociados para identificar la sesión entre los dos DTE. Existen también otros campos de facilidad que pueden emplearse cuando los DTE deseen aprovechar algunas de las opciones del estándar X.25. Por último el paquete puede transportar datos de llamada del propio usuario. El espacio máximo para datos de usuario que admiten los paquetes de solicitud de llamada es de 16 octetos. Este campo es útil para transportar ciertas informaciones dirigidas al DTE receptor, como por ejemplo palabras de acceso, información de tarificación.

También utiliza estos datos el protocolo X.29. Para determinadas opciones como la llamada rápida, está permitido incluir hasta 128 octetos de usuario. La cabecera del paquete se modifica con el fin de facilitar el movimiento de datos de usuario por la red. El tercer octeto de la cabecera, normalmente reservado para el identificador de tipo de paquete, se descompone en dos campos independientes:

Bits	Descripción o valor.
1	0.
2-4	Secuencia de envío del paquete [P(S)].
5	Bit de más datos (el bit M).
6-8	Secuencia de recepción de paquetes [P(R)].

Las misiones de estos campos son las siguientes: si el primer bit vale 0, indica que se trata de un paquete de datos. El número de secuencia de envío [P(S)] tiene asignados tres bits. Otro bit lleva a cabo la función de bit **M**. Por último los tres bits restantes se asignan al número de secuencia de recepción [P(R)]. Los números de secuencia de envío y de recepción sirven para coordinar y asentir las transmisiones que tienen lugar entre DTE y DCE. A medida que un paquete atraviesa la red de un nodo a otro, es posible que los números de secuencia cambien durante el recorrido por los centros de conmutación. Pese a ello, el DTE o DCE receptor tiene que saber que número de recepción ha de enviar al dispositivo emisor. El empleo de P(R) y P(S) en el nivel de red exige que el P(R) sea una unidad mayor que el P(S) del paquete de datos.

2.4.5.4.1 EL BIT D

La facilidad "bit D" se añadió en la versión de 1980 de la norma X.25. Sirve para especificar una de las siguientes funciones: cuando este bit vale 0, el valor de P(R) indica que es la red la que asiente los paquetes; cuando el bit D vale 1, la confirmación de los paquetes se realiza de extremo a extremo, es decir, es el otro DTE el que asiente los datos enviados por el DTE emisor. Cuando se utiliza el bit D con valor 1, X.25 asume una de las funciones del nivel de transporte: la contabilización de extremo a extremo.

2.4.5.4.2 EL BIT M

El bit M (más datos) indica que existe una cadena de paquetes relacionados atravesando la red. Ello permite que tanto la red como los DTE identifiquen los bloques de datos originales cuando la red los ha subdividido en paquetes más pequeños. Así por ejemplo, un bloque de información relativo a una base de datos debe presentarse al DTE receptor en un determinado orden.

2.4.5.4.3 PAQUETES A Y B

La combinación de los bit M y D establece dos categorías dentro del estándar X.25 que se designan como paquetes A y paquetes B. Gracias a ello los DTE o DCE pueden combinar el secuenciamiento de dos o más paquetes y la red puede también combinar paquetes. En X.25, una secuencia de paquetes completa se define como un único paquete B y todos los paquetes contiguos tipo A que lo precedan (si es que hay alguno). Un paquete de categoría B sirve para cerrar una secuencia de paquetes relacionados con el tipo A. Por contra los paquetes A representan la transmisión en curso, han de contener datos, y deben llevar el bit M a 1 y el bit D a 0. Sólo los paquetes tipo B pueden tener el bit D a 1 para realizar confirmaciones de extremo a extremo. La red puede agrupar una serie de paquetes A y el paquete B subsiguiente dentro de un sólo paquete, pero los paquetes B han de mantener las entidades independientes en paquetes independientes. La combinación de paquetes puede resultar útil cuando se empleen paquetes de distintas longitudes a través de una ruta de la red, o cuando las subredes de un sistema de redes interconectadas empleen distintos tamaños de paquete. De este modo es posible manejar los paquetes a nivel lógico como un todo. En este caso, puede usarse el bit M para señalar al DTE receptor que los paquetes que llegan están relacionados y siguen una determinada secuencia. Uno de los objetivos de los bits M y D es la combinación de paquetes. Por ejemplo, si el campo de datos del DTE receptor es más largo que el del DTE emisor, la red puede combinar los paquetes dentro de una secuencia completa.

2.4.5.4.4 EL BIT Q

Este bit es opcional, y puede usarse para distinguir entre datos de usuario e informaciones de control.

2.4.5.4.5 ESTABLECIMIENTO DE CONEXIONES

Se definen 4 tipos de paquetes para el establecimiento:
Petición de llamada.
Llamada entrante.

2.4.5.4.5.1 COMUNICACIÓN ESTABLECIDA

La conexión se establece por iniciativa del de nivel superior. El nivel 4 de la estación local va a dialogar con el nivel 4 de la estación remota (diálogo extremo a extremo). Para ello hay que tener una conexión a nivel 3 (que es el que proporciona el servicio extremo a extremo).

El nivel 4 de la estación local manda una primitiva de comunicaciones al nivel 3, éste construye un paquete que se usa para solicitar conexión a la red. Este paquete es el de **petición de llamada**. Esta PDU se envía a la red. Para ello se solicita al nivel de enlace que sea transmitida. Puesto que el nivel de enlace es orientado a conexión, la conexión a nivel de enlace se establece cuando el sistema arranca. El nivel de enlace consigue que la SDU que le había mandado el nivel de red llegue al nivel de enlace del nodo remoto. Ahí se construye otro paquete, el **paquete de llamada entrante**. Este paquete se entrega al nivel 3 del DCE remoto. El nivel 3 del nodo remoto detecta que se le pide una conexión y pregunta al nivel 4 mediante una primitiva, y es el nivel 4 quien rechaza o acepta la conexión. Si el nivel 4 decide aceptar la conexión se lo comunica al nivel 3 mediante otra primitiva. El nivel 3 genera entonces otro paquete, el de **llamada aceptada**. El nivel 3 se lo pasa al nivel 2, éste lo convierte en bits y se lo pasa al nivel físico, quien lo convierte en señal se transmite, y llega al nivel 3 del nodo remoto donde se destruye, la red hace llegar al nivel 3 del nodo local la información, donde se genera el paquete de comunicación establecida y este paquete llega al nivel 3 del DTE local y mediante una primitiva llega al nivel superior informándole de que la comunicación está establecida. El nivel 4 de la estación remota, a partir de que acepta la conexión pasa a la fase de transmisión de datos. El nivel 4 de la estación local no considera que la conexión se ha establecido con éxito hasta que le llega la última primitiva de conexión establecida.

2.4.5.4.5.2 PAQUETE DE PETICIÓN DE LLAMADA, LLAMADA ENTRANTE

Los paquetes de petición de llamada y llamada entrante tienen el mismo formato, diferenciándose únicamente en el sentido en que se transmite el paquete: DTE-DCE el primer caso y DCE-DTE en el segundo, figura 115.

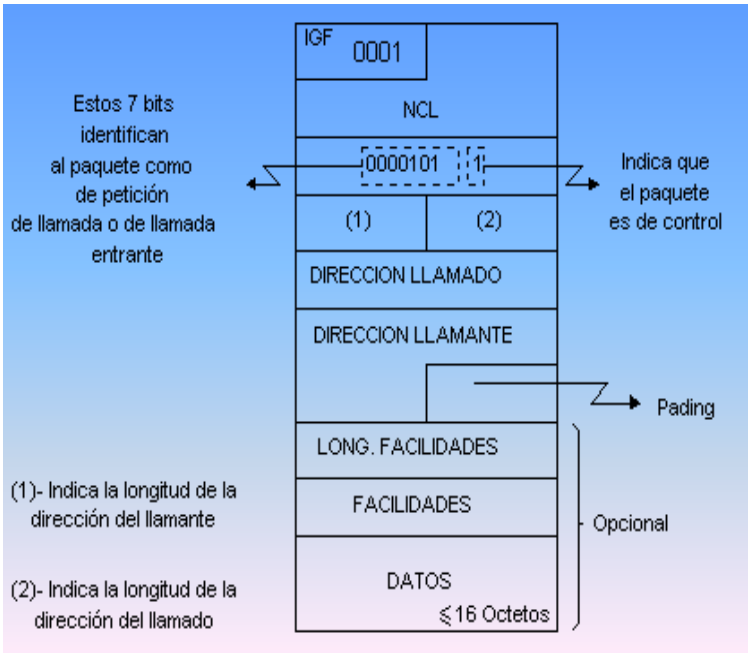


Figura 115 formato general de petición de llamada o llamada entrante

- **El IGF**.-Es el índice general de formato. Su longitud es de 4 bits.
- **El NCL**.-Es el Número de Canal Lógico que es un identificador de multiplexión (posibilidad de cursar varias conexiones de nivel superior sobre una sola conexión de nivel inferior).
- **Los campos (1) y (2)** indican la longitud de la dirección del llamante y del llamado respectivamente. Las longitudes se codifican con cuatro bits que indican el número total de dígitos de las direcciones en X.25. Los puntos de acceso al servicio se identifican mediante el plan de numeración que asigna direcciones únicas a los usuarios de la red. Las direcciones se codifican en los dos campos de direcciones. Se obliga a que el campo de direcciones esté alineado a octeto. Si las direcciones de llamante y llamado no tienen ambas un número impar de dígitos o un número par, puede sobrar algún semiocteto. Los campos de direcciones son de longitud variable.

- **Pading** se usa precisamente para solventar este problema de semioctetos sobrantes. Es un relleno de 4 ceros que se pone para que no sobre nada.
- **Campo de longitud de facilidades**.-Indica la longitud del campo de facilidades. Es obligatorio ya que indica si el siguiente campo está presente o no.
- **Campo de facilidades**.-Las facilidades son servicios suplementarios al servicio básico (por ejemplo especificación de uso de un tamaño de paquetes de datos superiores al tamaño por defecto 128 octetos, o de un tamaño de ventana diferente a 2, etc.).

Estos paquetes contienen datos de usuario del nivel superior, los cuales no llevan delante un campo de longitud ya que acaban donde acaba la trama. Este campo transporta una SDU que ha sido trasmitida por el nivel superior al inmediatamente inferior. Esto contradice que el servicio sea orientado a conexión, porque permite que antes de que se establezca la conexión las entidades de nivel superior intercambien datos. La longitud de este campo, como se ve en la figura 115, es menor o igual que 16 octetos. Sin embargo, si se usa la facilidad de selección rápida **(fast select)** pasa a ser menor o igual que 128 octetos. Estos datos, si el tamaño es de 16 octetos, se usan para:
Proporcionar un mecanismo de control de acceso, ya que con la dirección del llamante sólo se identifica al PTR, no a los usuarios (autentificación). Es decir, se usa para intercambiar una palabra de paso, para que así el usuario tenga información adicional para aceptar o rechazar la conexión.
Enviar la PDU de establecimiento de conexión del nivel superior. En el caso de que el tamaño del campo de datos sea de 128 octetos se usa, además de para las dos anteriores para enviar datos en modo no orientado a conexión.

2.4.5.4.5.3 PAQUETE DE LLAMADA ACEPTADA Y DE COMUNICACIÓN ESTABLECIDA

El paquete de llamada aceptada va del DTE al DCE y el de comunicación establecida del DCE al DTE. El formato es el mismo para los dos, figura 116.

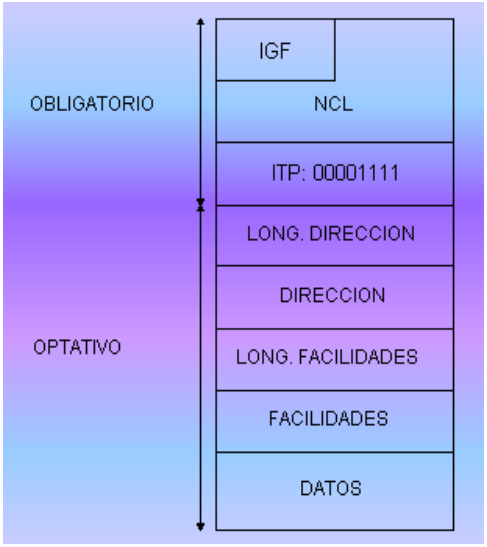


Figura 116 formato general de llamada aceptada o comunicación establecida

- **El campo de control (ITP)**.-Nos permite saber si el paquete es de llamada aceptada o de comunicación establecida. Sólo son imprescindibles los tres primeros octetos. La parte opcional está presente cuando hay alguna facilidad que justifique su presencia (si ponemos los campos opcionales de facilidades o datos, tengo que poner también los de longitud y direcciones, aunque puedo dejarlos a cero). Las facilidades que justifican esta parte son:
  Selección rápida (fast select).-Permite un campo de datos de hasta 128 octetos. Esto permite la presencia de datos en los paquetes que se usan para aceptar o rechazar la llamada. Por tanto, si una estación nada más recibir una Petición de Llamada manda una

PDU de desconexión, consigue una transferencia de datos sin haberse establecido la conexión. Tanto estos paquetes como los de petición de llamada y los de llamada entrante, así como los de liberación de conexión y de indicación de liberación admiten la facilidad de selección rápida. X.25 facilita esta opción ya que hay aplicaciones que funcionan mejor en modo datagrama (servicio no orientado a conexión).

2.4.5.4.5.4 INTERCAMBIO DE DATOS

Una vez que hemos establecido la conexión ya estamos preparados para el intercambio de datos. Los paquetes que se usan en este caso son:

- Paquetes de datos.
- Paquetes RR.
- Paquetes RNR.

Estos dos últimos paquetes son paquetes de confirmación o también llamados paquetes de supervisión (asentimiento) que se usan para control de flujo.

2.4.5.4.5.5 PAQUETE DE DATOS

El paquete de datos en la recomendación X.25 presenta formato de la figura 117.

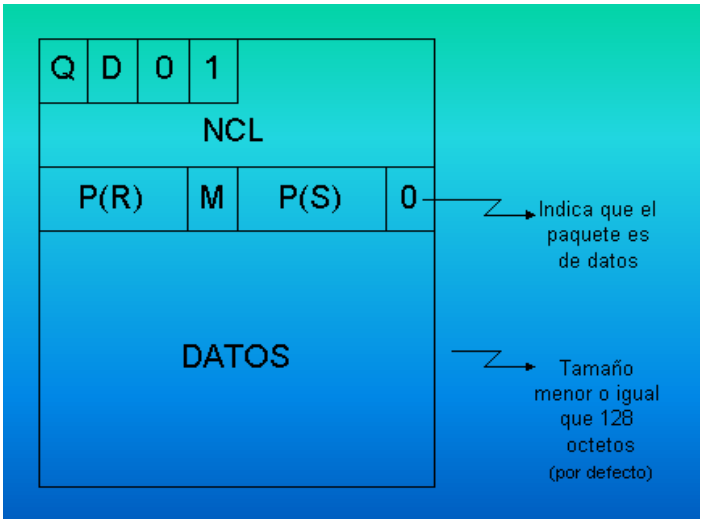


Figura 117 formato general de un paquete de datos

Esto es el formato normal. Existe además un formato extendido cuyo aspecto es el de la figura 118. Este formato usa dos octetos para llevar la información de control. Se sabe en que formato estamos por los bits 6 y 5 del primer octeto del paquete. Si estos bits son 10 el formato es extendido y si son 01 el formato es normal. En una conexión todos los paquetes de datos tienen el mismo formato. El formato extendido en general se usa poco.

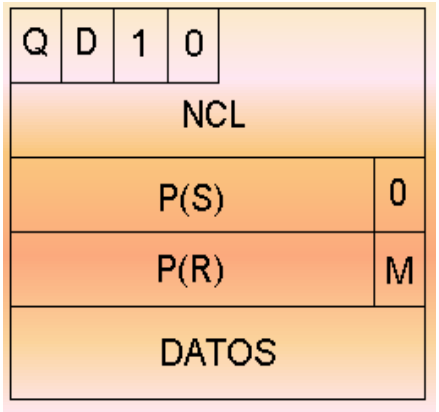


Figura 118 formato general de un paquete de datos extendido

Campo de datos.-En este campo van los datos del usuario. Consiste en una secuencia de octetos (al menos uno, el paquete de datos no puede ir vacío). Hay un número máximo de octetos por

paquete: 128 octetos. Esta longitud máxima es la longitud por defecto. Al igual que la ventana, se puede solicitar un aumento del tamaño del paquete, pero esto también implica mayor ocupación de la red y mayor precio.

El campo de control.-Está divido en subcampos. Estos subcampos no pueden tener valores arbitrarios. De los 8 bits que componen el campo de control se usan algunos para distinguir unos paquetes de otros y otros para llevar información de control. Se usa un sólo bit para identificar al paquete de datos, que es un 0 en el primer bit (el de más a la derecha). El resto de los paquetes tienen un 1 en esta posición. Los otros subcampos son:
P(R): Número de secuencia de recepción. Es también un asentimiento (piggybacking)
P(S): Número de secuencia de transmisión.
Los números de secuencia (P(R) *y* P(S) o también N(R) y N(S)) y la ventana se utilizan exclusivamente para control de flujo y detección de errores. Un número de secuencia es un identificador secuencial cíclico que se asigna a las PDU's transmitidas (P(S)) en una conexión dada. Este número de secuencia se va incrementando con cada PDU que se envía. El número de secuencia se utiliza generalmente para:

- Realizar control de errores.
- Realizar control de flujo.

En X.25 esto se realiza a nivel de enlace. A nivel de red los números de secuencia sólo se utilizan para control de flujo. Esto se realiza en combinación con el mecanismo de ventana.
El paquete de datos en formato extendido tiene números de secuencia más grandes, que permiten ventanas más grandes. El tamaño de la ventana por defecto en X.25 es 2. Se puede solicitar un aumento de ventana, pero será más caro, ya que se utilizan más recursos de la red. Este incremento viene limitado por el número de secuencia.

El bit M.-Se utiliza para implementar la función de segmentación y reensamblado, que consiste en cursar datos de una SDU utilizando varias PDU's (entregándose la SDU íntegramente en destino). En origen se segmenta la SDU y en destino se reensambla. La segmentación y el reensamblado se hacen a nivel de red no de enlace.
Si M=1 faltan más paquetes por llegar de la SDU que se está transmitiendo.
Si M=0 no faltan más paquetes por llegar de la SDU que se está transmitiendo.

Campo NCL.-Nos va a permitir distinguir los datos de las distintas conexiones que podemos establecer en X.25. El paquete de datos no necesita campo para la dirección de destino, ya que el servicio es orientado a conexión y cuando se establece una conexión hay una asociación lógica entre los niveles de red de los dos extremos. El campo NCL aparece para poder usar multiplexión (cursar varias conexiones de nivel superior sobre una única conexión de nivel inferior). En X.25 se permite que sobre la única conexión que nos ofrece el nivel de enlace se puedan establecer tantas conexiones como desee el nivel de red. Estas conexiones puede que tengan el mismo destino o un destino distinto (podemos tener tantas conexiones en paralelo como queramos). El NCL es un identificador de multiplexión, que es un número que va en el campo de control y que en principio no tiene ninguna estructura y que nos permite saber qué datos pertenecen a cada conexión. Por tanto es obligatorio que aparezca. La longitud de este campo es de 12 bits, por lo que el número máximo de conexiones que podemos establecer es 2^{12}. El NCL se asigna dinámicamente (a cada conexión se le asigna dinámicamente un valor para el NCL). La asignación se realiza en la fase de establecimiento de conexión. Las entidades que se conectan usan un procedimiento para negociar un número para el identificador. La entidad que pide la llamada selecciona un NCL que esté libre (hay tablas de conexión en los sistemas que tienen registradas las conexiones establecidas).

El paquete de petición de llamada se envía a través del nivel de enlace al nodo local, que lo recibe a nivel de red. El NCL que le propone la estación que pide la llamada lo incluye en sus tablas como una conexión ocupada. Esta información llega hasta el nodo local del abonado remoto. El nivel de red del nodo remoto de la red genera el paquete de llamada entrante. El NCL que genera es distinto al usado en el origen. Para asignar el NCL se usa el mismo procedimiento que en origen, por lo que el NCL que esté libre para ese usuario lo añade a la tabla, lo codifica en el paquete de llamada entrante y lo entrega al abonado, que apunta en sus tablas que tenemos un

nuevo NCL correspondiente a una conexión remota. Si este procedimiento tiene éxito cuando se mande el paquete de llamada aceptada, éste irá con el mismo NCL que el de llamada entrante. Por eso en el paquete de llamada aceptada la dirección de destino es opcional, puede ser suficiente con el NCL. El usar la dirección de destino puede resultar ambiguo, pero el uso del NCL nunca es ambiguo. Los NCL's están limitados por contratación. Aunque desde el punto de vista técnico pueden haber hasta 2^{12}, por motivos comerciales se limita los NCL's que pueden estar útiles. Se limitan para que el operador dimensione la red. Se paga por cada NCL que contratemos. El límite a la cantidad de recursos de red que puede usar el usuario es la capacidad del canal. Se establecen rangos en todos los posibles valores de NCL.

El bit 0.-Está reservado para procedimientos de control. Los números 1 a X están reservados para los circuitos virtuales permanentes. Luego hay otros reservados para las llamadas entrantes salientes o ambas, que se determinan por contratación. Hay dos modalidades de conexión en X.25:
CVP: circuitos virtuales permanentes.
CVC: circuitos virtuales conmutados.
Los CVP no se establecen ni se liberan usando los paquetes de petición y liberación de llamada, sino por contratación. Se preconfiguran los nodos de tal forma que, por contratación, el circuito está permanentemente establecido.
Los CVC son los que para establecerse y liberarse necesitan del intercambio de paquetes de establecimiento y liberación.

El bit Q.-No afecta al comportamiento de X.25. La entidad de nivel de red simplemente informa al usuario del nivel superior de su estado a 0 ó a 1. El bit Q, a nivel X.25, se envía de forma transparente. Se puede utilizar para que los protocolos de nivel superior marquen a sus paquetes de control (Q=1) o datos (Q=0). En destino se procesarán de distinta forma y tendrán un tratamiento preferente a los paquetes de datos.

El bit D.-Se utiliza para controlar el tipo de asentimiento (también llamado **acuse de recibo**)
D=0 Asentimientos locales (sin acuse de recibo).
D=1 Asentimientos remotos (con acuse de recibo).

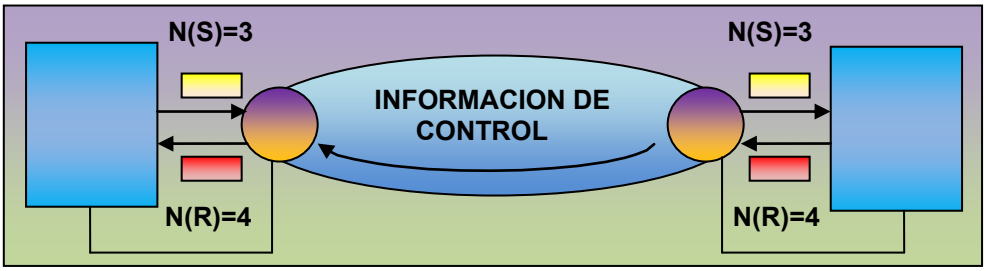


Figura 119

El paquete que contiene N(R) =4 (asentimiento) se puede mandar cuando llega el paquete al nodo local o cuando llega el paquete al abonado remoto y se produce información de control. Si se manda cuando el paquete llega al nodo local tiene la ventaja de la rapidez. Si se manda cuando el paquete ha sido asentido en destino tenemos la ventaja de estar seguros de que el receptor ha recibido los datos. La manera en que el usuario solicita confirmación de entrega es mediante:

- **Parámetro de la primitiva de Datos**.-Para solicitar confirmación de entrega.
- **Primitiva específica**.-La que se da al usuario para confirmar.

La configuración se realiza mediante una primitiva específica en X.25. Este servicio se implementa usando el bit D:
D=1: solicita confirmación de entrega, por lo que la red asiente los paquetes sólo después de que se hallan asentido en destino.

D=0: no solicita confirmación de entrega. Los asentamientos se hacen desde el nodo local.
El inconveniente de tener D=1 es que la ventana sirve para el control de flujo. Podemos transmitir hasta que se acabe la ventana sin que nos llegue asentamiento. Si el tiempo de asentamiento es pequeño hay envío continuo, por lo que la ventana no limita la transmisión. Si el tiempo de asentamiento es elevado puede que se termine la ventana, por lo que el circuito virtual del emisor no puede transmitir. Al usar el bit D el tiempo de asentimiento es más grande. Esto es indeseable. Queremos envío continuo. Si queremos acuse de recibo este problema debe tolerarse.

2.4.5.4.5.6 PAQUETE DE SUPERVISIÓN

Existen dos paquetes de supervisión:

- RR.
- RNR.

Hay un tercero que es opcional (REJ).
La función de estos paquetes es:

- Realizar control de flujo XON/XOFF.
- Realizar asentimientos explícitos.

El formato de los paquetes RR y RNR es el mismo, diferenciándose entre ellos solamente en un bit como se ve en la figura 120

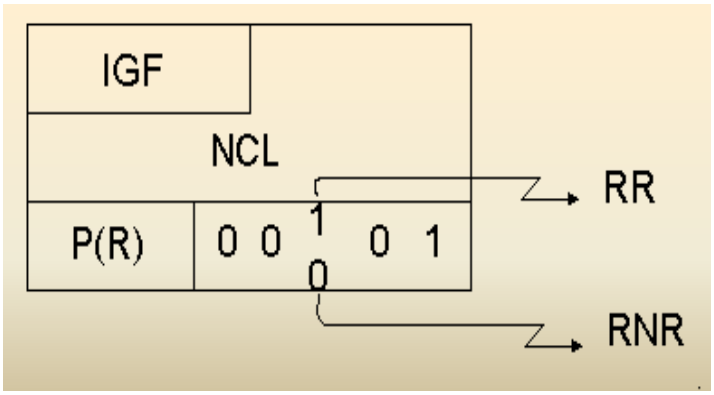
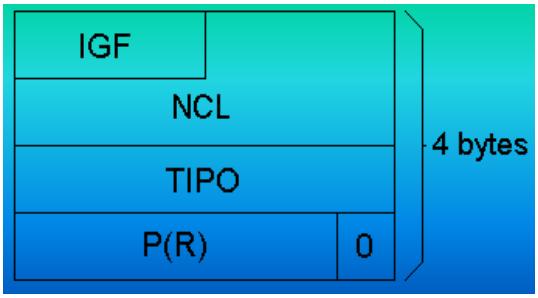


Figura 120 formato general de un paquete de supervisión



P(R).-Son 3 bits que indican el número de secuencia que se asiente (indica cual es el siguiente que espera recibir) Los paquetes RR y RNR varían ligeramente en el formato extendido, figura 121.

Figura 121 formato general extendido de RR y RNR

Los asentimientos explícitos se usarán cuando no disponemos de datos para enviar al receptor, puesto que no es posible enviar paquetes de datos vacíos para representar asentimiento. La diferencia entre RR y RNR para su uso en control de flujo XON/XOFF (para el emisor o le deja transmitir) es:

- Si envío RR el emisor puede recibir.
- Si envío RNR la entidad que lo emite informa de que no está preparada.

Desde el punto de vista del receptor del paquete:

- Si se recibe RNR para de transmitir (sólo en el canal lógico por el que se recibe el paquete).
- Si se recibe RR puede seguir transmitiendo

NOTA: Existe una opción adicional en X.25, que prácticamente no se usa y que incluye rechazos con retransmisiones (REJ se consigue con el campo de tipo a 01001)

2.4.5.4.5.7 INTERCAMBIO DE DATOS ACELERADOS

El servicio de datos acelerados o datos fuera de banda consiste en datos asociados a una conexión pero que no guardan la secuencia ni el control de flujo de los datos normales. El objetivo es que lleguen lo más rápidamente posible (son enviables incluso cuando la transmisión está parada). En X.25 este servicio se implementa mediante el paquete de interrupción. Hay dos paquetes de interrupción:

- uno enviado por parte del DTE.
- otro enviado por parte del DCE.

En cuanto a formato estos paquetes son iguales. Sólo se diferencian en el sentido de la transmisión. Tanto la interrupción por DCE como por DTE presentan en la figura 122.

.

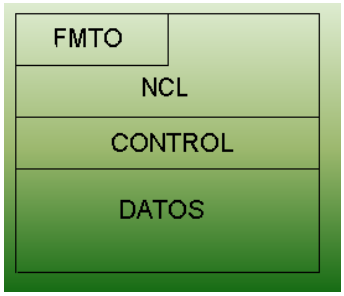


Figura 122 formato general del paquete de interrupción y protocolo de transmisión

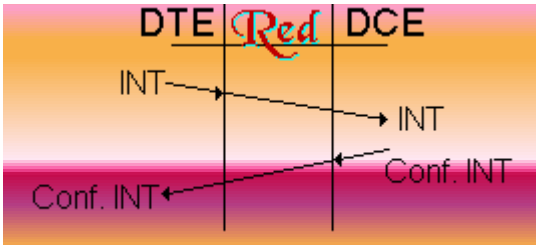


Figura 123

Funciona en parada y espera.-Hasta que no llega un **Conf.INT**, no puedo enviar otro INT.
El campo datos.-Es variable. Históricamente el tamaño de los datos era de un octeto. Las versiones más modernas permiten hasta 32 octetos (en cualquier caso, es una cantidad pequeña, pues ya estaría enviando más de lo que se debe).

El servicio de datos acelerados se usa para control de flujo de la entidad de nivel superior, por lo que no afecta al flujo de datos normales. Es como si tuviéramos 2 flujos de transmisión perfectamente distinguibles. X.25 es un protocolo para teleproceso, por lo que tiene conectada una terminal remota. En el caso de que la terminal se cuelgue, existe un carácter de interrupción para interrumpir el proceso. Este carácter se envía en el paquete de interrupción. Hay dos paquetes más asociados a éste:

- Confirmación de interrupción por parte del DTE.
- Confirmación de interrupción por parte del DCE.

Estos paquetes se utilizan porque el servicio de interrupción es un servicio confirmado.

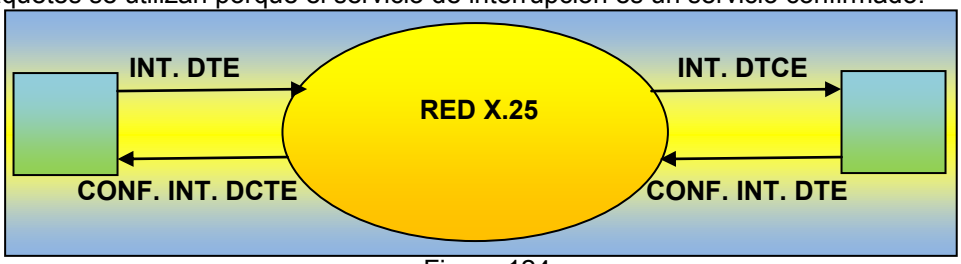


Figura 124

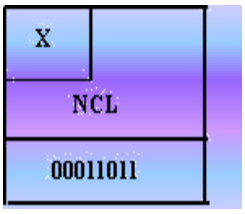


Figura 125

El formato de estos paquetes es el mostrado en la figura 125. Existe una restricción, hay que esperar confirmación antes de enviar otra interrupción. Es decir, sólo puede haber un paquete de interrupción pendiente de confirmación en cada canal lógico. El efecto práctico de esta restricción es que el volumen de datos que podemos enviar con formato de interrupción es pequeño.

2.4.5.4.6 REINICIO Y REARRANQUE DE CONEXIONES

2.4.5.4.6.1 REINICIO

El servicio de reinicio puede realizarse a iniciativa del proveedor o a iniciativa del usuario. Este servicio consiste en situar la conexión en el estado inicial, por lo que los temporizadores asociados a la conexión se paran, los números de secuencia asociados a la conexión se ponen al valor inicial y los buffers asociados a la conexión se vacían. El resultado final es que la conexión vuelve al estado inicial. El servicio de reinicio potencialmente destruye datos, por lo que se contradice que X.25 sea fiable. Por ello este procedimiento es indeseable. Pero este servicio es necesario cuando: Se producen errores no recuperables por otro procedimiento. Estos errores son:

- Caída de un nodo de tránsito, por lo que se pierde la información de estado asociada a esa conexión. En este caso la propia red ejecuta el procedimiento de reinicio.
- Fallo detectado por el nivel de red (errores de protocolo), por ejemplo recibir un paquete de datos vacío, de mayor longitud que la permitida.

Este servicio se implementa mediante el intercambio de paquetes de reinicio. Es un servicio confirmado. Se usan 4 paquetes:

- Petición de reinicio (del DTE al DCE).
- Indicación de reinicio (del DCE al DTE).
- Confirmación de reinicio por DTE (del DTE al DCE).
- Confirmación de reinicio por DCE (del DCE al DTE).

Cuando un DTE envía petición de reinicio espera a recibir confirmación de reinicio por parte del DCE, y entonces considera la conexión reestablecida. Cuando es la red o el abonado remoto se envía un paquete de indicación de reinicio y se espera recibir confirmación de reinicio por parte de DTE y entonces considera la conexión reestablecida. En realidad es el nivel de red el que se reinicia. El reinicio se notifica también al nivel superior. El nivel de red manda la primitiva **reset indication** al nivel superior, ya que el reinicio destruye los datos y el nivel superior considera que el servicio es fiable y no recupera errores. La red debe avisar al nivel superior. Aún así el nivel superior debe estar preparado para tomar una medida correctiva. Los paquetes de petición e indicación de reinicio tienen el mismo formato, como se ve en la figura 126.

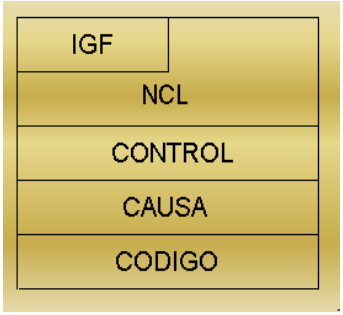
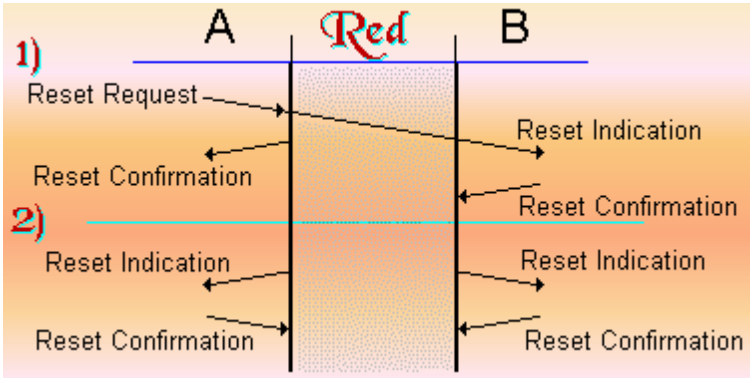


Figura 126 formato general de un paquete de petición de reinicio y esquema del protocolo reset.



El contenido del campo de control es 00011011. El contenido de los campos causa y código viene especificado en la recomendación (están tabulados). Estos campos son opcionales. Los paquetes de confirmación de reinicio por DTE y DCE tienen el siguiente formato de la figura 128.

Figura 127

El campo de control tiene el siguiente contenido: 00011111. La única diferencia entre ellos es el lugar donde se generan, figura 128.

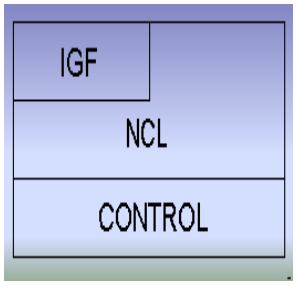


Figura 128 Formato general de un paquete de confirmación de reinicio.

Una situación excepcional es que los dos interlocutores soliciten reinicio a la vez. En este caso el servicio se reestablece cuando confirma DTE.

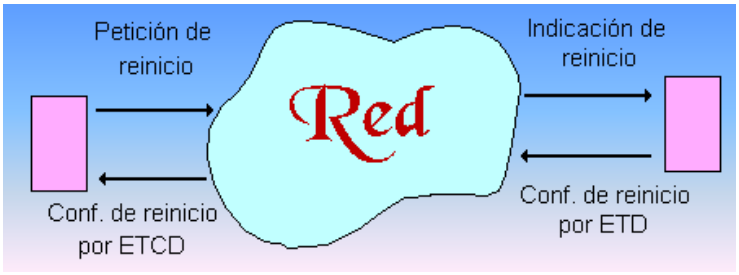


Figura 129 gráfica de generación de paquetes de reinicio

2.4.5.4.6.2 REARRANQUE

Es un procedimiento de recuperación frente a errores particularmente graves que afectan a toda la interfaz entre el usuario y la red (por ejemplo se cae el equipo de usuario o el nodo local). Usa para su implementación 4 paquetes:

- Petición de rearranque.
- Indicación de rearranque.
- Confirmación de rearranque por parte del DTE.
- Confirmación de rearranque por parte de DCE.

Estos paquetes tienen la particularidad de que se cursan para el NCL=0. La razón es que el procedimiento de rearranque no sólo afecta a una conexión sino a todas las de la interfaz usuario-red. El procedimiento de rearranque por tanto es local a una interfaz. Se usa cuando se inicializa el sistema o cuando se detecta un fallo irrecuperable por otros medios, por ejemplo, datos que se reciben por un NCL que no está definido. Al inicializarse se ejecuta el procedimiento de rearranque para sincronizar el sistema con la red y que estén en el mismo estado inicial. Este estado inicial consiste en que no halla ningún circuito conmutado y que los circuitos virtuales estén en el estado inicial permanentes. Si el procedimiento de rearranque es iniciado por el DTE, éste genera una PDU de petición de rearranque que es cursada por el NCL 0 hasta el nodo local y éste le contesta mediante un paquete de confirmación de rearranque. Al producirse el rearranque hay que reconfigurar todos los elementos de la conexión. Las acciones que se toman son:
Reinicio de la conexión a nivel de enlace (previa). Esto se hace antes de enviar el paquete de petición de rearranque mediante una primitiva que manda el nivel de red al de enlace. Por tanto, llevamos la conexión a nivel de enlace al estado inicial.
Una vez hecho el reinicio se envía el paquete (o se recibe si es el otro extremo). Se recibe el paquete de rearranque, se notifica al nivel superior el reinicio de todos y cada uno de los circuitos virtuales permanentes de la red y hay indicación de liberación a todos y cada uno de los circuitos virtuales conmutados.

Se entiende que en los CVC's la conexión ha sido liberada y en los CVP's la conexión ha sido reiniciada (se encuentra en el estado inicial). Esto se hace mediante primitivas. El formato de los paquetes de petición e indicación de rearranque (o reinicialización) es el mostrado en la figura 130.

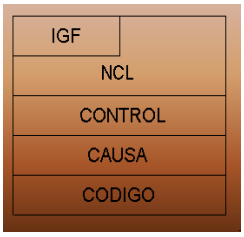
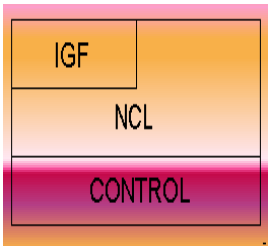


Figura 130 formato general del paquete de rearranque



Se envía por el canal lógico 0, que es el que se reserva para señalización. Los efectos de **Restart** son:

- Todos los CV permanentes se reinician.
- Todos los CV conmutados se desconectan.

Los paquetes de confirmación de rearranque por parte del DTE y DCE son también iguales a los de confirmación de Reset, figura 131.

Figura 131 formato general de confirmación de rearranque

2.4.5.4.7 LIBERACIÓN DE CONEXIONES

Se usan 4 paquetes:

- Petición de liberación (de DTE a DCE).
- Indicación de liberación (de DCE a DTE).
- Confirmación de liberación por parte del DTE (de DTE a DCE).
- Confirmación de liberación por parte del DCE (de DCE a DTE).

2.4.5.4.7.1 PETICION/IDICACION DE LIBERACIÓN

El paquete de petición de liberación de conexión va del DTE al DCE y el de indicación de liberación del DCE al DTE. Por lo demás ambos paquetes tienen el mismo formato:
Causa.-Es un byte que indica por que se ha liberado la comunicación (si ha sido el DTE, la red, etc.).
Diagnóstico.-Es un byte que no hace sino refinar la causa. Es opcional en el de petición de liberación si los siguientes campos no existen. En el paquete de indicación es obligatorio si la parte opcional está presente, de lo contrario la decodificación del paquete sería ambigua.
La parte optativa se envía en base a las reglas del protocolo.-No cuando el usuario lo desee, sino cuando lo exige el protocolo. Es decir, si hay una facilidad que lo solicite, como por ejemplo selección rápida, que permite que los paquetes de petición de liberación puedan llevar datos y por tanto se puedan intercambiar datos. El campo de datos puede tener hasta 128 octetos. Si la respuesta a un paquete de llamada entrante es uno de petición de liberación se rechaza la conexión.

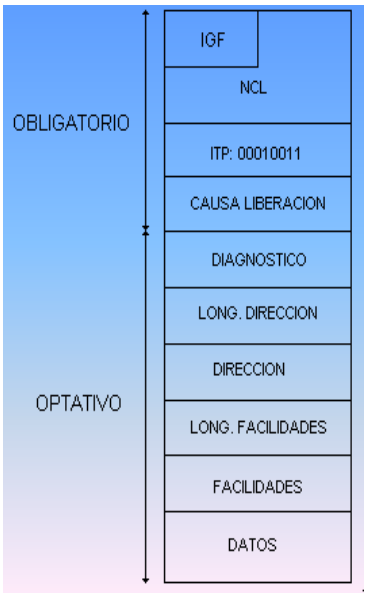
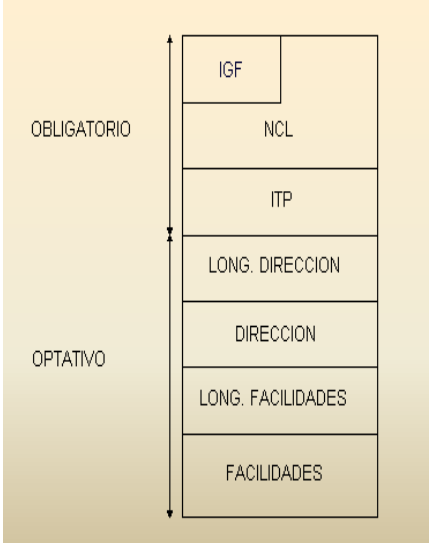


Figura 132 formato general de liberación de conexión e indicación de liberación

2.4.5.4.7.2 CONFIRMACION DE LIBERACIÓN POR PARTE DEL DTE/DCE

No hay campo de datos en este caso, ya que cuando se envía este paquete se cierra la conexión. Su formato es el de la figura 133. La parte optativa sólo está presente si una facilidad requiere su presencia. Hay dos formas de realizar la liberación de las conexiones:

- **Liberación abrupta**.-Liberación unilateral por parte de una de las entidades que participan en la conexión, por lo que hay una potencial pérdida de datos entrantes.
- **Liberación ordenada**.-Ambas estaciones, y las estaciones de red deben estar de acuerdo para realizar la liberación, por lo que no hay pérdida de datos entrantes.



En X.25 se usa liberación abrupta. Cualquiera de las dos estaciones puede decidir el final de la conexión en cualquier momento unilateralmente. Procedimiento de liberación:
El nivel 4 de la estación que desea la liberación pasa al nivel 3 la primitiva **disconection request**. El nivel 3 genera la PDU de petición de liberación. El nivel 3 se la pasa al nivel 2 mediante la primitiva **data request**. El nivel 2 construye la trama en la que mete la SDU que le ha pasado el nivel 3. La trama se pasa al nivel 1 convertida en binario y del nivel 1 se pasa al medio físico convertida en señal. De aquí llega al DCE. Se pasa del medio físico al nivel 1 de éste al nivel 2 y aquí se decodifica y se pasa al nivel 3 mediante la primitiva **data indication**. Mediante señalización interna de red se indica que se quiere liberar la conexión y mediante primitivas se realiza el proceso inverso.

Figura 133 Formato general de confirmación de liberación.

En el momento en el que el nodo local recibe la petición de liberación puede generar la PDU de confirmación de liberación, que es entregada al nivel 2 mediante **data request**. No se necesita confirmación del abonado remoto. La liberación es abrupta. Aún así la red notifica al abonado remoto que se libera la conexión. El nivel 3 del nodo remoto genera una PDU de indicación de liberación que llega al nivel 3 del abonado remoto, que notifica al nivel superior una primitiva de **disconection indication**. El nivel 3 puede enviar espontáneamente una confirmación de liberación, aunque el nivel superior manda una primitiva de **disconection response**. Después de pedir la petición de liberación no se pueden mandar datos al nivel superior, ya que éste considera liberada la conexión y sólo espera la confirmación de liberación. La primitiva de disconection response no es obligatorio que sea respondida por el nivel 3 del DCE ya que se entiende que la conexión ha sido liberada. La confirmación a nivel de protocolo es necesaria puesto que la estación local tiene que estar segura que el nodo local ha recibido la petición de liberación, para poder liberar el NCL de esa conexión y poder usarlo para otra. La desconexión puede suceder espontáneamente por parte de la red. La red manda una PDU a cada usuario de indicación de liberación. La red lo realiza en casos de errores irrecuperables. Causa habitual de liberación espontánea es un error en un nodo local de abonado no recuperable por otros medios. Aunque hay pérdida de datos, el servicio es fiable puesto que avisa que pueden haberse perdido datos. Un mecanismo para confirmar que no se han perdido datos es que las estaciones de nivel superior, de mutuo acuerdo, soliciten acuse de recibo y hagan uso de paquetes de confirmación de entrega. La diferencia entre liberación y rearranque es que la liberación sólo afecta a un canal lógico y el rearranque afecta a todos los de una misma interfaz usuario-red.

2.4.5.5 PROCEDIMIENTO MULTIENLACE

En X.25 se puede hacer uso de la división de conexiones de la siguiente manera, figura 134:
El **ML-P**: **Micro Link Protocol**. Es el encargado de hacer el multienlace.
Funcionamiento del ML-P.

Los bits R y C se utilizan para indicar el tipo de PDU.
R=1 (reset): el que transmite la PDU solicita un establecimiento o reinicio de la conexión
C=1: para confirmar (aceptar) el reset o el establecimiento de la conexión. Se utiliza para responder a un paquete con R=1, (R=1 sería equivalente a lo que en LAP-B era SABM o RST y C=1 sería equivalente a lo que en LAP-B era UA)
Transmisión.- ML-P debe repartir la carga entre las líneas que tiene por debajo. Reparte entre las que estén dispuestas a recibir. Además debe asignar números de secuencia (12bits).
Recepción.-ML-P debe resecuenciar, ya que el retardo es variable entre las distintas líneas.

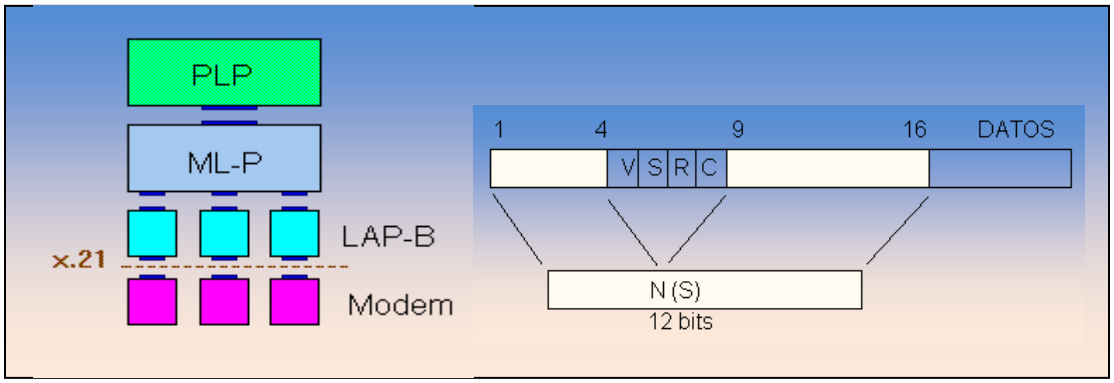


Figura 134

2.4.5.6 NORMAS AUXILIARES DE X.25

Las siguientes recomendaciones auxiliares pueden considerarse parte de la norma X.25:

- X.1 Clases de servicio del usuario.
- X.2 Facilidades del usuario.
- X.10 Categorías de acceso.
- X.92 Conexiones de referencia para paquetes que transmiten datos.
- X.96 Señales de llamada en curso.
- X.121 Plan internacional de numeración.
- X.213 Servicios de red

2.4.5.7 PRINCIPIOS DE CONTROL DE FLUJO

X.25 permite al DTE o al DCE limitar la velocidad de aceptación de paquetes. Esta característica es muy útil cuando se desea controlar si una estación recibe demasiado tráfico. El control de flujo puede establecerse de manera independiente para cada dirección y se basa en las autorizaciones de cada una de las estaciones. El control de flujo se lleva a cabo mediante diversos paquetes de control X.25, además de los números de secuencia del nivel de paquete. El procedimiento de interrupción permite que un DTE envíe a otro un paquete de datos sin número de secuencia, sin necesidad de seguir los procedimientos normales de control de flujo establecidos por X.25. El procedimiento de interrupción es útil en aquellas situaciones en las que una aplicación necesite transmitir datos en condiciones poco habituales. Así por ejemplo, un mensaje de alta prioridad puede enviarse como paquete de interrupción, para garantizar que el DTE receptor acepta los datos. Un paquete de interrupción puede contener datos de usuario (un máximo de 32 octetos). El empleo de estas interrupciones afecta a los paquetes normales que circulan por el circuito virtual, ya sea conmutado o permanente. Una vez enviado un paquete de interrupción es preciso esperar la llegada de una confirmación de la interrupción antes de enviar a través del canal lógico un nuevo paquete de interrupción. Los paquetes de Receptor Preparado (RR) y de Receptor no Preparado (RNR) se usan de forma parecida a sus comandos homónimos del protocolo HDLC y del subconjunto LAP-B. Desempeñan una importante tarea de controlar el flujo iniciado por los dispositivos de usuario.

Ambos paquetes incluyen un número de secuencia de recepción en el campo correspondiente, para indicar cual es el siguiente número de secuencia que espera el DTE receptor. El paquete RR sirve para indicar al DTE/DCE emisor que puede empezar a enviar paquetes de datos, y también utiliza el número de secuencia de recepción para acusar recibo de todos los paquetes transmitidos con anterioridad. Al igual que el comando de respuesta RR de HDLC, el paquete RR puede servir simplemente para acusar recibo de los paquetes que han llegado cuando el receptor no tiene ningún paquete específico que enviar al emisor. El paquete RNR sirve para pedir al emisor que deje de enviar paquetes. También existe un campo de secuencia de recepción con el cual se asientan todos los paquetes recibidos con anterioridad. El RNR suele usarse cuando durante un

cierto periodo de tiempo la estación es incapaz de recibir tráfico. Conviene señalar que si un DTE concreto genera un RNR, lo más probable es que la red genere otro RNR para el DTE asociado, con el fin de evitar que se genere en la red un tráfico excesivo. La capacidad de almacenamiento y espera en cola en los nodos de conmutación de paquetes de la red no es ilimitada. Por eso un RNR a veces conduce al estrangulamiento de ambos extremos de la sesión DTE/DCE.

Estos dos paquetes proporcionan a X.25 un sistema de control de flujo que va más allá que el que ofrece el nivel de enlace LAP-B. Así pues, se dispone de control de flujo y control de ventanas a dos niveles: en el nivel de enlace para LAP-B y en el nivel de red para X.25. Sin embargo, el nivel de enlace no ofrece un control de flujo eficaz para los DTE's; por el contrario, en el nivel de red, X.25 emplea los RR y RNR con números específicos del canal lógico, para llevar a cabo las operaciones de control de flujo. Cualquier nodo que tenga asignado un número de canal lógico puede efectuar este control de flujo. En algunas redes, se asigna un bloque de números de canal lógico a la computadora central y este se encarga de gestionar los NLC de sus terminales y programas de aplicación. El paquete de rechazo (REJ) sirve para rechazar de forma específica un paquete recibido. Cuando se utiliza, la estación pide que se retransmitan los paquetes, a partir del número incluido en el campo de recepción de paquetes.

Los paquetes de reinicialización (reset) sirven para reinicializar un circuito virtual permanente o conmutado. El procedimiento de reinicialización elimina en ambas direcciones, todos los paquetes de datos y de interrupción que pudieran estar en la red. Estos paquetes pueden ser necesarios también cuando aparecen determinados problemas, como es la perdida de paquetes, su duplicación, o la perdida de secuencia de los mismos. La reinicialización sólo se utiliza en modo de transferencia de información y puede ser ordenada por el DTE (solicitud de reinicialización) o por la propia red (indicación de reinicialización). El procedimiento de reiniciación (restart) sirve para inicializar o reinicializar la interfaz del nivel de paquetes entre el DTE y el DCE. Puede afectar hasta 4,095 canales lógicos de un puerto físico. Este procedimiento libera todas las llamadas virtuales y reinicializa todos los circuitos virtuales permanentes de la interfaz. La reiniciación puede presentarse como consecuencia de algún problema serio, como es la caída de la red. Todos los paquetes pendientes se pierden, y deberán ser recuperados por algún protocolo de nivel superior. En ocasiones, la red generara una reiniciación al arrancar o reinicializar el sistema para garantizar que todas las sesiones empiecen desde 0. Cuando un DTE haya enviado una señal de reiniciación, la red habrá de enviar una reiniciación a cada uno de los DTE que tengan establecida una sesión de circuito virtual con el DTE que genero la reiniciación. Los paquetes de reiniciación pueden incluir también códigos que indiquen el motivo de tal evento.

Dentro de la red de paquetes pueden perderse algunos paquetes de usuario. Ello puede suceder también en una red X.25. Los paquetes de liberación, reiniciación y reinicialización pueden provocar que la red ignore los paquetes aún no cursados. Una situación así no es demasiado infrecuente ya que en muchos casos estos paquetes de control llegan a su destino antes de que lo hayan hecho todos los paquetes de usuario. Los paquetes de control no están sometidos al retardo inherente a los procedimientos de control de flujo que afectan a los paquetes de usuario. Por tanto, los protocolos de nivel superior están obligados a tener en cuenta estos paquetes perdidos. Dentro de la red X.25, el paquete de liberación (clear) desempeña diversas funciones, aunque la principal es el cierre de una sesión entre dos DTE. Otra de sus misiones consiste en indicar que no puede llevarse a buen término una solicitud de llamada. Si el DTE remoto rechaza la llamada enviara a su nodo de red una solicitud de liberación. Este paquete será transportado a través de la red al nodo de red de origen, el cual entregara a su DTE una indicación de liberación. El cuarto octeto del paquete contiene un código que indica el motivo de la liberación.

2.4.5.8 FACILIDADES DE X.25

La versión X.25 de 1984 incluye varias facilidades adicionales. Algunas de estas funciones no son obligatorias para poder considerar una red como compatible X.25, aunque son bastante útiles y algunas en concreto pueden calificarse como esenciales para una red. Las facilidades se invocan mediante instrucciones concretas dentro del paquete de solicitud de llamada. Su clasificación es:

- Facilidades internacionales.
- Facilidades de DTE especificadas por CCITT.
- Facilidades ofrecidas por la red pública de datos de origen.
- Facilidades ofrecidas por la red pública de datos de destino.

Notificación de la facilidad en línea.-Esta facilidad permite al DTE, en cualquier momento, solicitar facilidades u obtener los parámetros de las facilidades tal y como los entiende el DCE. Para el dialogo entre el DTE y el DCE se emplean los paquetes de notificación. Estos mismos paquetes indican si puede gestionarse el valor de la facilidad.
Numeración de paquetes extendida.-Esta facilidad proporciona el esquema de numeración de secuencias módulo 128. En su ausencia lo que se emplea es el módulo 7. El 1984 se consideró importante añadir esta facilidad para hacer frente a los grandes retardos de propagación que aparecen en la comunicación vía satélite o en los enlaces por radio con unidades marítimas.
Modificación del bit D.-Esta facilidad está pensada para usarse con equipos DTE desarrollados con anterioridad a la introducción del procedimiento del bit D. Permite trabajar con asentimiento de extremo a extremo.
Retransmisión de paquetes.-Un DTE puede solicitar al DCE la retransmisión de uno o varios paquetes de datos. Para ello el DTE especifica, dentro de un paquete de rechazo, el número de canal lógico y un valor de P(R). El DCE deberá retransmitir todos los paquetes comprendidos entre el número P(R) y el siguiente que tuviera que enviar por primera vez. Esta facilidad es similar a la técnica de rechazo no selectivo que utilizan los protocolos de línea en el segundo nivel del modelo OSI.
Obstrucción de las llamadas entrantes.-Obstrucción de las llamadas salientes. Estas facilidades impiden que el DCE presente llamadas entrantes al DTE, o que el DCE presente llamadas salientes del DTE.
Canal lógico unidireccional entrante, Canal lógico unidireccional saliente.-Estas facilidades sólo permiten al canal lógico aceptar en el primer caso o enviar llamadas en el segundo pero no ambas cosas. Su función es similar a las facilidades de obstrucción salvo en que ahora la restricción afecta sólo a canales individuales.
Tamaño de paquetes por omisión no estándar.-Permite seleccionar el tamaño de paquetes que la red admitirá por omisión. Para gestionar el tamaño de los paquetes pueden emplearse paquetes de notificación.
Tamaño de ventana por omisión estándar.-Permite ampliar el tamaño de las ventanas por encima del valor por defecto dos para todas las llamadas.
Asignación de clases de velocidad de transmisión por defecto.-Esta facilidad permite seleccionar una de las siguientes velocidades de transmisión (en bits por segundo): 75, 150, 300, 600, 1,200, 2,400, 4,800, 9,600, 19,200 y 48,000. Pueden gestionarse también otros valores.
Negociación de los parámetros de control de flujo.-Esta facilidad permite variar el tamaño de una ventana de una llamada a otra. A veces un DTE sugiere el tamaño de la ventana durante el establecimiento de la llamada. En algunas redes estos parámetros deben ser los mismos para ambos DTE.
Negociación de la clase de velocidad de transmisión.-Permite modificar la velocidad de transmisión de una llamada a otra.
Grupo cerrado de usuarios (CUG).-Conjunto de funciones que permite a los usuarios formar grupos de DTE de acceso restringido. Esta facilidad proporciona a la red pública un nuevo grado de seguridad y privacidad. Incluye diversas opciones como el acceso en un sólo sentido entrante o saliente. Por lo general, la estación que llama especifica el grupo cerrado de usuarios que desea mediante los campos de facilidad incluidos en el paquete de solicitud de llamada. Si la estación solicitada no es miembro de ese grupo la red rechaza la llamada. Grupo cerrado de usuarios bilateral. Esta facilidad es similar a la anterior, pero permite establecer restricciones de acceso entre pares de DTE.
Selección rápida, aceptación rápida de la selección, cobro revertido, aceptación del cobro revertido.-Estas facilidades permiten cargar el costo de la llamada al DTE receptor. Pueden usarse con llamadas virtuales y con selecciones rápidas.

Prevención de cobros locales.-Esta facilidad autoriza al DCE a rechazar las llamadas que tenga que pagar su DTE. Por ejemplo, un DTE puede no estar autorizado a aceptar los cobros revertidos de ningún DTE que llame.
Identificación del usuario de la red.-Esta facilidad permite que el DTE que llama entregue a su DCE la información de tarificación, seguridad o gestión, llamada por llamada. Si no es válida esta información la llamada no se cursa.
Información de tarificación.-Esta facilidad permite que el DCE informe a su DTE sobre las condiciones de tarificación de la sesión de paquetes en curso.
Selección de compañía.-Permite que el DTE que llama escoja una o varias compañías telefónicas para gestionar su sesión de paquetes.
Grupo local.-Esta facilidad se encarga de distribuir las llamadas que lleguen entre un grupo preestablecido de interfaces DTE/DCE. Esta mejora de la versión 1984 permite a los usuarios seleccionar múltiples puertos de una computadora o procesador frontal, o escoger entre varios de estos sistemas dentro de un mismo nodo de usuario. Se trata de una posibilidad muy útil en aquellas organizaciones equipadas con grandes sistemas informáticos que necesiten flexibilidad para asignar tareas a los distintos recursos.
Redireccionamiento de la llamada.-Esta facilidad, también fruto de la revisión de 1984, redirige la llamada cuando el DTE de destino está averiado, comunica, o cuando ha solicitado expresamente que se reoriente la llamada. Permite orientar las comunicaciones entrantes hacia algún DTE de apoyo, que se encargará de solucionar los posibles problemas y de mantener al usuario final aislado de los fallos. El redireccionamiento de llamadas permite también redirigir la llamada a distintas zonas de un país o continente por cuestiones relacionadas con los usos horarios.
Notificación del cambio en la dirección de la llamada.-En caso de que se haya producido la redirección de una llamada, esta facilidad explica al DTE que llama por que la dirección de destino de la llamada conectada o del paquete indicador de liberación es distinta de la dirección del paquete de petición de llamada del DTE.
Notificación de redireccionamiento de llamada.-Cuando se produce un redireccionamiento de llamada, esta facilidad informa del hecho al DTE alternativo, indicándole además por que ha cambiado la dirección del DTE original.
Indicación y selección del retardo de tránsito.-Esta última facilidad permite al DTE seleccionar un determinado tiempo de tránsito por la red de paquetes. Esta función puede ser de gran utilidad para el usuario final, pues le confiere un cierto control sobre la velocidad de respuesta de la red.

2.4.5.9 OTROS ESTANDARES Y NIVELES

2.4.5.9.1 EL PAD (ENSAMBLADO/DESENSAMBLADO DE PAQUETES)

PAD es un servicio que se ofrece al usuario para permitirle conectarse con una red de paquetes. Tras el primer borrador de la norma X.25, aparecido en 1976, los comités de normalización editaron en 1977 una nueva recomendación en la que aparecían tres especificaciones relativas a las interfaces para terminales asíncronos: X.3, X.28 y X.29. Estas recomendaciones se verían reforzadas más adelante con la revisión de 1984. La idea del PAD es ofrecer una conversión de protocolos entre un DTE y una red pública o privada, junto con otra conversión complementaria en un extremo receptor de la red. Se trata de conseguir un servicio transparente para los DTE de usuario. La norma X.3 y sus normas accesorias X.28 y X.29 sólo están pensadas para dispositivos asíncronos, pero muchos fabricantes ofrecen otros servicios tipo PAD capaces de aceptar protocolos como BSC o SDLC. Estas opciones no asíncronas del esquema PAD se encuentran dentro de la filosofía de X.3, X.28 y X.29. Los estándares PAD permiten diversas configuraciones. La norma X.29 sirve para establecer comunicaciones entre un PAD y un DTE X.25, o entre dos PAD. La versión X.3 de 1984 proporciona una serie de 22 parámetros, que son utilizados por el PAD para identificar y atender a cada una de las terminales con las que se comunica. Cuando se establece una conexión con el PAD desde un DTE. El usuario puede también alterar estos parámetros una vez iniciada su sesión con el PAD. Cada uno de estos 22 parámetros consta de un número de referencia y de una serie de valores. Ejemplos de parámetros:
Parámetro 3 = 0 Ordena al PAD que envíe sólo paquetes llenos

Parámetro 3 = 2 Ordena al PAD que envíe el paquete una vez que la terminal entregue un carácter de retorno de carro.
Parámetro 6 = 1 Una terminal de usuario desea recibir las señales de servicio del PAD. Es útil para localizar averías.
Parámetro 7 = 1 Cuando reciba de la terminal un carácter de interrupción (break), el PAD enviará un paquete de interrupción al DTE receptor.

El paquete PAD tiene un formato similar al del paquete X.25 convencional. Necesita una cabecera de tres octetos, seguida de un campo de control de un octeto y por último los números y valores correspondientes al PAD. Estas son las funciones que desempeñan los distintos estados:

- Activo: el DTE y el DCE intercambian un 1 por la interfaz.
- Solicitud de servicio: se autoriza al PAD para detectar la velocidad de transmisión de los datos y el código que utiliza el DTE, y para seleccionar el perfil inicial.
- DTE en espera: la interfaz queda en estado de espera.
- Preparado para dar servicio: se entra en este estado una vez que el PAD ha transmitido su señal de identificación.
- PAD en espera: el PAD queda a la espera de señales de control o de datos.
- Comando del PAD: a este estado se llega desde diferentes estados de espera. Permite transmitir comandos al PAD.
- Conexión en curso: en este estado se entra cuando el PAD inicia una conexión con la red.
- Señales de servicio: autoriza todas las señales de servicio de este estado.
- Transferencia de datos: permite la transferencia de datos a través de la interfaz.

En espera de un comando: en este estado se entra cuando el DTE debe recibir a un comando o dato del PAD.

2.4.5.9.2 X.28

En este estándar se definen los procedimientos de control de flujo entre la terminal del usuario y el PAD. Una vez recibida una conexión inicial desde el DTE de usuario, el PAD establece el enlace y proporciona los servicios propios de la norma X.28. El DTE de usuario entrega al PAD diversos comandos X.28, y el PAD solicita de X.25 una llamada virtual con el DTE remoto. A partir de entonces, el PAD será responsable de transmitir los paquetes adecuados de solicitud de llamada X.25. Existen los siguientes procedimientos:

- Establecimiento de trayectoria.
- Inicialización del servicio.
- Intercambio de datos.
- Intercambio de información de control.

Con X.28, cuando un PAD recibe un comando procedente de una terminal, está obligado a devolver una respuesta. También pueden definirse dos perfiles para atender al DTE de usuario. Con el perfil transparente, el PAD que atiende el servicio es transparente para ambos DTE, es decir, que los dos DTE's **piensan** que existe una conexión virtual entre ellos. En esta situación, el DTE remoto debe encargarse de algunas funciones PAD, como es la comprobación de errores. El perfil simple, por el contrario, atiende las solicitudes del usuario mediante las opciones que proporciona la norma X.3 y las funciones de parámetros. La versión 1984 de X.3 ofrece al usuario una gran flexibilidad porque le permite ajustar las características adicionales de cada modelo de terminal. Para ello emplea el comando **PROF PAD**. EL comando PROF proporciona a los fabricantes una mayor versatilidad, al permitirles configurar cada PAD de modo que sirvan de interfaces para otros protocolos, como los controles de enlace BSC y SDLC. Un ejemplo de comandos y señales de servicio X.28 sería el siguiente: SET 3:0,6:1. Esto significa que asignar el valor 0 al parámetro 3 y el valor 1 al parámetro 6.

2.4.5.9.3 X.29

Este estándar indica al PAD y a la estación remota como deben intercambiar funciones de control dentro de una llamada X.25. X.29 permite que el intercambio de información tenga lugar en

cualquier momento, ya sea en la fase de transporte de datos o en cualquier otra etapa de la llamada virtual. La secuencia del bit **Q** gobierna algunas de las funciones de X.29. El bit Q (bit cualificador de datos) lo utiliza el DTE remoto para distinguir los paquetes de información de usuario (Q=0) y paquetes que contienen información esencial del PAD (Q=1). X.29 resulta especialmente útil cuando una computadora central necesita modificar los parámetros de funcionamiento X.3 de las terminales conectadas a él. Para reconfigurar sus estaciones de trabajo, la computadora central puede enviar un paquete de control X.29 a un PAD, con el bit Q puesto a 1. En X.29 están definidos siete mensajes de control, llamados mensajes del PAD. En concreto:

- Establecer (set): modifica un valor X.3.
- Leer (read): lee un valor X.3.
- Establecer y leer: modifica un valor X.3 y pide confirmación del hecho al PAD.
- Indicación de parámetros: se devuelve en respuesta a los comandos anteriores.
- Invitación a liberar la llamada: permite al DTE remoto liberar la llamada X.25; el PAD por su parte, libera la terminal local.
- Indicación de interrupción (break): el PAD indica que la terminal ha transmitido una señal de interrupción (break).
- Error: respuesta a un mensaje inválido del PAD.

III.-INICIO DE LA EVOLUCION TECNOLOGICA

3.1 EVOLUCION DE LOS MEDIOS

3.2 ISDN (INTEGREAD SERVICES DIGITAL NETWORK)

3.2.1 INTRODUCCION

El término **Servicios Integrados** se refiere a la posibilidad de comunicar a través de ella cualquier tipo de información voz, imágenes, videos, textos, diseños, documentos, música de alta calidad, o ficheros de datos de cualquier tipo, con simples llamadas telefónicas. La ISDN es compatible a nivel internacional (EURO ISDN) y las comunicaciones de voz lo son también con la telefonía analógica clásica. Además, la ISDN se ha definido mediante un conjunto de normas de validez internacional, lo que permitió que las terminales y aplicaciones desarrolladas en un país, puedan ser utilizadas directamente por cualquier otro. Inicialmente, la ISDN coexistirá con las redes convencionales de telefonía y datos, pero progresivamente se convertirá en una Única y Universal Red de Telecomunicaciones. Hasta hoy se han solventado las necesidades de comunicación, con la RTC, Red Conmutada de Telefónica, y con líneas Punto a Punto tanto analógicas como digitales, éstas últimas considerablemente más caras. La idea básica a tener en cuenta cuando se habla de la ISDN es que cualquier tipo de información (voz, datos, imágenes, etc.), una vez codificada digitalmente puede ser tratado de idéntica manera, con la única diferencia de las velocidades requeridas. Una ISDN es integrada porque utiliza la misma infraestructura para muchos servicios que tradicionalmente requerían interfaces distintas (télex, voz, conmutación de circuitos, conmutación de paquetes); es digital porque se basa en la transmisión digital, utiliza canales de 64Kbps (G.732); y es una red porque proporciona transmisión y conmutación. La digitalización de la red telefónica analógica ha dado lugar a la Red Digital Integrada (RDI), en la que lo único que no es digital son las líneas de acceso de los abonados (bucle de abonado). El CCITT define la ISDN de la siguiente forma: "Una red que procede por evolución de una Red Digital Integrada (RDI) telefónica y que facilita conexiones digitales extremo a extremo para soportar una amplia gama de servicios, tanto de voz como de otros tipos, y a la que los usuarios tienen acceso a través de un conjunto limitado de interfaces normalizadas de usuario multiservicio". Y también (Recomendación I.120): "Un elemento clave de la integración de servicios para una ISDN es proporcionar un abanico de servicios utilizando un conjunto limitado de tipos de conexión y disposiciones de interfaz usuario-red de propósito general".

Es decir, la ISDN se presenta como la bandera de las redes RDI, aunque su oferta es diferente:

- Audio de 7kHz de ancho de banda, en vez de los 3.1kHz de la red telefónica.
- Canales digitales de 64kbps de velocidad en vez de las que se alcanzan utilizando módems que difícilmente llegan a los 40kbps.
- Mayor funcionalidad y servicios gracias al canal común de señalización.

Un único y estandarizado método de acceso que da paso a toda una red de área extensa, con posibilidad de transferir información tanto en modo circuito como en modo paquete, figura 135.

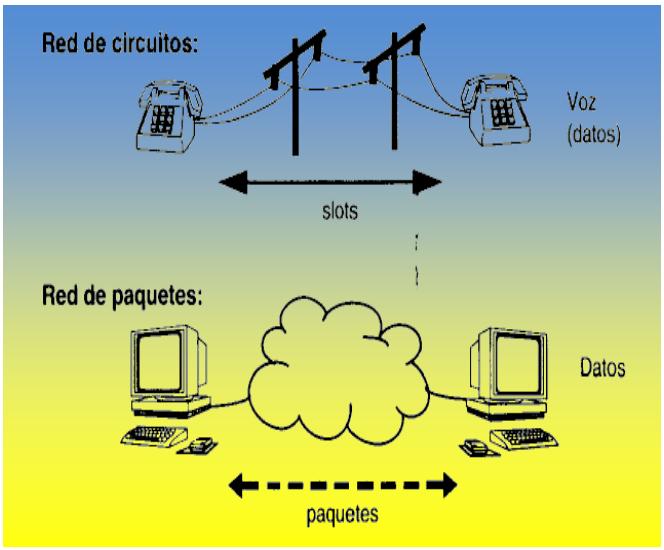


Figura 135 La ISDN integra redes de circuitos y redes de paquetes permitiendo el soporte eficiente de voz, datos e imágenes en baja definición.

La ISDN presenta al usuario una serie de interfaces normalizadas para la conexión a la Red. de esta forma se pretende normalizar todas las conexiones a la Red mediante los Accesos de Usuario. Una Central Pública se considera ISDN cuando cumple los requisitos enumerados a continuación:

- Tanto la matriz de conmutación de circuitos como el sistema de transmisión entre centrales debe ser digital, Centrales RDI.
- La señalización requerida para ISDN entre Centrales Públicas se basa en el Sistema de Señalización por Canal Común nº 7 del CCITT. (SSCC 7). Un sistema basado en intercambio de información mediante mensajes entre Centrales.
- La central debe estar dotada de señalización **PUSI (Parte Usuario Servicio Integrado)**, que se encarga de dar servicio a los diferentes Accesos de Usuario de la ISDN de forma especializada. Además de contar con la señalización **PUT (Parte Usuario Telefónico)**, encargada de atender las comunicaciones de voz, ancho de banda 3.1KHz.
- Debe disponer de capacidades de conmutación de paquetes, mediante el **MP (Manejador de paquetes)** o **ECP's (Elementos de Conmutación de Paquetes)**, de forma que los paquetes de información del usuario puedan progresar en la Red. Esta característica no está disponible aún en algunas tecnologías de forma que en algunos Accesos no podrá habilitarse.

La central ISDN permite la conexión con otras Redes de Comunicación de Clientes, de forma que puedan prestarse, aparte de los servicios ISDN, aquellos servicios que utilizan los Clientes en la actualidad. Por este motivo se definen una serie de Integraciones con otras redes: Integración ISDN-RTB. La integración con la Red Telefónica Básica está asegurada, ya que las Centrales ISDN son una evolución de las Centrales RDI que poseen señalización PUT (Parte de Usuario Telefónico) por su propia definición. Así pues esta integración es total para todas las tecnologías sin excepción.

Gracias al tipo de señalización elegido, conmutación de paquetes, el establecimiento de una conexión ISDN se efectúa a más velocidad, lo que permite un ahorro considerable de tiempo en el establecimiento de la comunicación. Es también una ventaja añadida la posibilidad de enviar pequeños mensajes en la "llamada" para indicar situaciones especiales, envío de textos como: "Llámame en 30 minutos", permiten al Usuario Llamado la posibilidad de devolver la llamada. La aparición de elementos como el número de origen de la llamada, el número destino, etc., mejoran los servicios de la Red en beneficio del Usuario. Ver la figura 136, ejemplo de un mensaje de señalización.

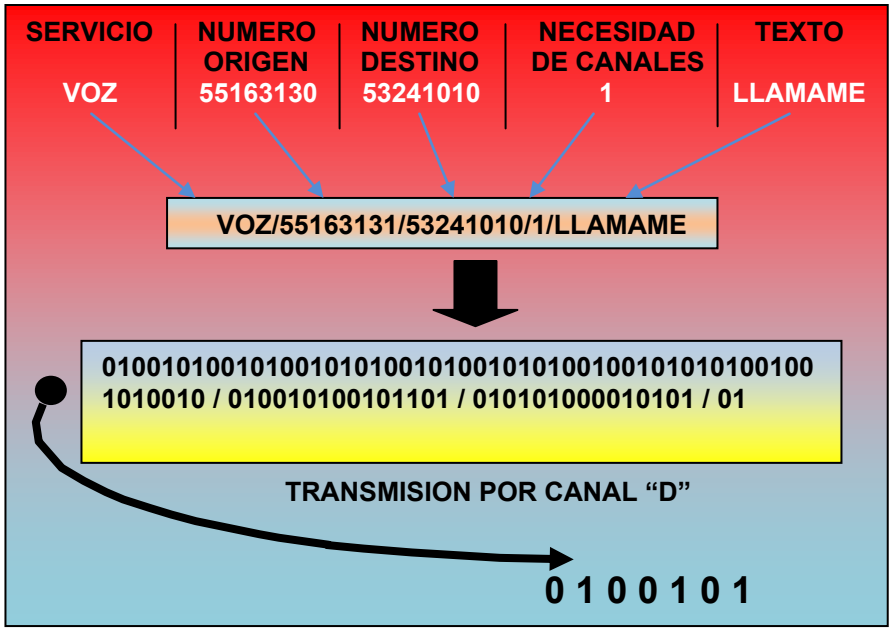


Figura 136. Paquete de señalización

Para permitir la interconexión de las terminales actuales, que no soportan de forma nativa protocolos ISDN, se han diseñado los denominados **Adaptadores de Terminal** (**TA**). Los TA

garantizan de esta forma la conexión de la mayoría de recursos de comunicaciones existentes sin necesidad de cambios notables.

3.2.2 VENTAJAS

Es evidente que la posibilidad de acceder a la gran variedad de servicios que la ISDN ofrece desde un único y universal punto de acceso, es la ventaja principal de la red. Pero como además existen ventajas globales que todos y cada unos de los usuarios de la ISDN pueden disfrutar:

- **Calidad de servicios**.-Excepcional 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 ISDN no está limitado por la naturaleza de la información ni por la fuente generadora.
- **Simplicidad y seguridad**.-Acceso único. Identificación de abonados.
- **Posibilidad de Utilización**.-Innumerables servicios y facilidades. Integración de voz, datos, texto e imagen. Terminales multiservicio. Integración de redes. Oportunidad para el desarrollo de nuevas aplicaciones.
- **Economía**.-Transferencia de grandes volúmenes de información con bajo costo. Solución única a las diversas necesidades. Ahorro de costos.

3.2.3 SERVICIOS DE UNA RED ISDN

Se pueden estructurar en tres categorías:

- **Servicios Básicos o portadores.-**Permiten acceder (a través de una interfaz normalizada) a la red básica y transferir información entre usuarios. Existen dos modalidades, Servicios Portadores en Modo Circuito y Servicios Portadores en Modo Paquete.
    - **Servicios portadores en modo circuito.-**Proporciona un circuito dedicado de principio a fin, a velocidades de 64Kbps o superiores. Es utilizado por aquellas aplicaciones que requieren una conexión en tiempo real, por ejemplo una conversación telefónica. Es un servicio sin restricciones, por lo que los usuarios pueden implementar sobre él cualquier protocolo. Se definen tres servicios en función del tratamiento de la señal digital:
        1) **Servicio portador a 64kbps sin restricciones**.-Se define como el servicio portador que puede emplear uno o varios canales a 64Kbps, sin ninguna estructura predefinida, de forma que la Central es transparente a la información del usuario. Por extensión del servicio que puede prestar se denomina también servicio portador de Datos.
        2) **Servicio portador para conversación**.-Se define como el servicio portador que mediante la utilización de un canal a 64Kbps permite la comunicación de voz extremo a extremo. Está estructurado según la codificación de una señal digitalizada de ancho de banda 4KHz. Es el servicio de Voz de la ISDN.
        3) **Servicio portador a 3.1KHz**.-Se define como el servicio portador que emplea un canal de 64Kbps para intercambio de información con un ancho de banda de 3.1KHz, desde 300Hz a 3,400Hz. Necesita de un Adaptador de Terminales. Las señales analógicas pueden generarse en un Fax de Grupo 2, en un módem, en un teléfono analógico, etc.
    - **Servicios portadores en modo paquete.**-Proporciona una conexión lógica entre los usuarios. Permite la explotación del canal D para comunicaciones en modo paquete con otros usuarios de la Red. Es utilizable por aquellas aplicaciones insensibles al retardo, como por ejemplo, una transmisión de ficheros.
        1) **Servicio portador en modo paquete virtual**.-Se define como el servicio portador en modo paquete que emplea procedimientos de llamada para el establecimiento de la conexión en modo paquete. Su velocidad binaria es de 9,600bps, aunque en algunos casos puede llegar a velocidades similares a la del canal D.

2) **Servicio portador en modo paquete permanente**.-Se define así al servicio de conmutación de paquetes exento de las fases de establecimiento de llamada, de esta forma la conexión se efectúa entre dos estaciones de conmutación de paquetes de forma permanente y la transferencia de información efectiva supera al servicio anterior, si bien no puede elegirse el destinatario de la información. Aunque la velocidad binaria de transferencia de datos es igual a la del caso anterior, la ausencia de elementos de control de la comunicación permite enviar más información con menos paquetes.

- **Teleservicios o Servicios de Valor Añadido**.-Utilizan los servicios portadores e implementan niveles superiores de comunicación. Pueden ser ofertados tanto por la compañía telefónica como por terceras empresas. Los Teleservicios de transmisión de datos y videotelefonía pueden emplearse con combinaciones de canales B, mediante el empleo de H0 o H12 o de la asociación de dos canales B, comunicación a 128Kbps. Existe la posibilidad de que aparezcan nuevos Teleservicios, aunque harán uso de uno de los servicios portadores, los más comunes son:
  - **Telefonía (con 3.1Khz)**.-Servicio similar al ofrecido por la RTB. Permite la comunicación de señales vocales con ancho de banda de 300 a 3,400Hz. Interfuncionamiento con la RTB.
  - **Telefonía a 7Khz**.-Servicio de telefonía mejorada, similar a las comunicaciones microfónicas, emplea un ancho de banda de 7KHz para comunicaciones vocales.
  - **Facsímil grupo 2/3**.-Permite la conexión de datos mediante digitalización de señales analógicas para servicio de fax. Puede emplearse para conexiones de fax con los equipos conectados a la RTB.
  - **Facsímil grupo 4**.-Servicio de fax definido para ISDN, que permite la conexión de Facsímil de alta calidad sin interfuncionamiento con la RTB.
  - **Teletex**.-Necesita de Adaptadores de Terminales para su conexión a la ISDN.
  - **Videotex**.-Servicio similar al ofrecido por la RTB, así pues puede permitir la interconexión con la RTB, siempre que se emplee un Equipo Terminal RTB a través de un Adaptador de Terminales.
  - **Videotelefonía**.-Permite la transmisión de imágenes junto con voz en una conexión ISDN extremo a extremo, no es compatible con la RTB.
  - **Transmisión de datos**.-Permite la conexión de canales B de forma transparente, sin interferir la información de Usuario. No existe interfuncionamiento con la RTB.
  - **Modo mixto**.-Permite el envío de información combinada, imágenes y texto a través de la ISDN. No es compatible con la RTB.
- **Servicios Suplementarios**.-Proporcionan a los usuarios información que ya tiene la red, razón por la que no se consideran de valor añadido. Entre los muchos servicios de esta categoría se encuentra la identificación de la llamada entrante, la multiconferencia, la redirección de llamadas, la información de tarificación, etc. Los servicios Suplementarios se enumeran a continuación:
  - **Grupo Cerrado de Usuarios**.-Permite formar grupos de acceso restringido, tanto para llamadas entrantes como salientes.
  - **Identificación del usuario llamante**.-Permite al usuario llamado la presentación del número de la persona que ha realizado la llamada.
  - **Restricción de identificación de usuario llamante**.-Permite al usuario que efectúa la llamada restringir su identificación hacia el usuario llamado.
  - **Identificación de usuario conectado**.-Permite al usuario llamante conocer la identidad del usuario con el que se ha establecido la llamada, caso de desvíos.
  - **Restricción de Identificación de usuario conectado**.-Permite al usuario llamado impedir la identificación de la conexión hacia el usuario llamante.
  - **Indicación de llamada en espera**.-Informa al usuario de la presencia de una llamada cuando tiene los dos canales B ocupados.
  - **Múltiples números por acceso**.-Permite dotar al acceso de varios números, en el caso de Acceso Básico, 8 por acceso.

- **Selección directa a extensiones**.-Permite la selección de un usuario conectado a través de una central de forma directa, mediante marcación.
- **Subdireccionamiento**.-Muestra una capacidad adicional para el encaminamiento de una llamada en un acceso, sin consumir recursos de numeración.
- **Portabilidad de terminales**.-Este servicio suspende una llamada establecida durante un máximo de 3 minutos, desconectando físicamente la terminal de la comunicación. La comunicación así suspendida puede recuperarse desde cualquier otra terminal en el mismo acceso
- **Línea directa sin marcación**.-Establece la marcación directa, llamada a un número previamente almacenado sin más que descolgar el microteléfono.
- **Desvío de llamadas**.-Reencamina una llamada entrante a otro destino predefinido.
- **Información de tarificación**.-Permite conocer el costo de la llamada, existen dos modalidades: durante la comunicación y al final de la comunicación.
- **Información Usuario a Usuario nivel 1**.-Permite el intercambio de información entre usuarios en la fase de establecimiento de la llamada.
- **Información Usuario a Usuario nivel 3**.-Es una ampliación del servicio anterior, permitiendo mensajes de mayor longitud en la misma fase de establecimiento de la llamada.
- **Presentación de la identificación de la línea llamante (CLIP, calling line identification presentation).-**Este servicio permite recibir en el llamado la identidad del número llamante. Este servicio no es necesario contratarlo ya que se da por defecto.
- **Restricción de la identificación de la línea llamante (CLIR, calling line identification restriction).-**Este servicio permite que en todas las llamadas generadas no aparezca la identidad del llamado. Este servicio necesita ser contratado. En general los teléfonos ISDN permiten llamada a llamada evitar que se envíe al llamado el número del llamante, mediante la señalización adecuada
- **Presentación de la identificación de la línea conectada (COLP, connected line identification presentation).**-Este servicio permite en las llamadas salientes tener conocimiento del número al cual se ha conectado la llamada. Debido a que puede existir uno o más desvíos de llamadas, el número llamado puede no coincidir con el número conectado. Este servicio no es necesario contratarlo pues se da por defecto.
- **Restricción de la identificación de la línea conectada (COLR, connected line identification restriction).-**Este servicio, que es necesario contratar, tiene por finalidad que en ninguna llamada entrante aparezca la información del número conectado. Dependiendo de la terminal o teléfono ISDN que se utilice esta funcionalidad puede ser realizada llamada a llamada sin necesidad de contratar el servicio.
- **Subdireccionamiento (SUB, sub-addressing).-**El subdireccionamiento permite a un acceso ISDN disponer de una capacidad adicional de direccionamiento. La contratación del servicio permite que esta información llegue al acceso. Todos los accesos independientemente de que hayan contratado el servicio o no tienen la capacidad de generarla. El subdireccionamiento sólo funciona en llamadas dentro de la ISDN. El número máximo de dígitos que se pueden enviar es veinte, la red se comporta de manera transparente a esta información.
- **Número múltiple de abonado (MSN, multiple subscriber number).-**Este servicio permite disponer de más de un número de abonado para un determinado acceso. La utilidad de este servicio se encuentra en dos casos generales:
    1) Poder discriminar, desde RTC u otra red que no disponga señalización ISDN, de servicios a través de distintos números: voz, fax, datos, etc..
    2) Simplemente discriminar entre distintas terminales
- **Marcación directa de extensiones (DDI, direct-dialling-in).-**Este servicio permite seleccionar directamente una terminal que está conectada a través de una central a la ISDN.

- **Llamada en espera (CW, call waiting)**.-Este servicio permite que en el caso de que los dos canales B de un acceso básico estén ocupados recibir notificación de una tercera llamada. Es importante indicar que no es un simple aviso sino que la llamada está presente en la interfaz y caso de liberar o retener alguno de los canales B se podrá completar la llamada.
- **Línea directa sin marcación**.-La contratación de este servicio permite el establecimiento de llamadas sin necesidad de marcación. El destino ha de ser previamente definido por el abonado y puede ser modificado cuantas veces se desee. Puede realizarse de dos maneras distintas:
    1) Línea directa sin marcación con establecimiento inmediato.-En este caso la llamada se establece inmediatamente cuando el teléfono se descuelga sin introducir número
    2) Línea directa sin marcación con establecimiento diferido.-En este caso la llamada se establece cuando después de descolgar ha transcurrido un determinado tiempo.
- **Información de tarificación (AOC, advice of charge).-**Este servicio permite recibir información del importe de la llamada. Este servicio puede ser contratado para suministrar la información durante la llamada y al finalizar o bien solamente al finalizar.
- **Portabilidad de terminal (TP, terminal portability).-**Este servicio suplementario permite sobre una llamada establecida suspenderla para posteriormente continuarla en otra ubicación (roseta) o bien en otra terminal. Para ello el usuario puede dar una clave que le será pedida posteriormente para la recuperación de la llamada. Este servicio suplementario no es necesario contratarlo ya que su implementación forma parte de la señalización ISDN.
- **Desvío incondicional de llamadas (CFU, call forwarding unconditional).-**Con el desvío incondicional de llamadas un abonado establece que todas las llamadas dirigidas a un determinado número sean desviadas al número que previamente ha determinado. Caso de ser el número único en el acceso todas las llamadas serán redirigidas.
- **Señalización Usuario a usuario (UUS, user-to-user signalling)**.-Permite a dos usuarios ISDN establecer un flujo de información entre ellos sobre el canal D. El bit rate disponible es algo menor que el bit rate del canal D (16kbps o 64kbps).
- **Grupo cerrado de usuarios (CUG, closed user group).-**Permite asociar varios números de ISDN formando grupos de tal manera que se establezcan determinadas reglas en cuanto a los derechos de llamadas entrantes o salientes del grupo.
- **Identificación de llamada maliciosa (MCID, malicious call identification).-** Permite al abonado que ha solicitado este servicio que a través de cierta señalización quede identificado en la central el origen de una determinada llamada en curso o en fase de finalización.
- **Salto**.-Este servicio permite la agrupación de varios accesos básicos a efectos de reparto de tráfico dirigido a un determinado número que se denomina número de salto. Los accesos mantienen sus números normales y se le añade un número por el cual recibirán las llamadas dirigidas al grupo.
- **ISPBX**.-Esta funcionalidad a diferencia del grupo de salto hace que un conjunto de accesos básicos pierdan su entidad individual y pasen a ser tratados de forma colectiva. Es decir cuando la central entrega una llamada a un grupo ISPBX lo hace por cualquier acceso básico independientemente del número del llamado. Un grupo ISPBX tiene un número de cabecera y puede tener una numeración adicional que sería selección directa de extensiones. Por todo lo dicho se entiende que este servicio es para un determinado tipo de equipos de abonado que en el caso más corriente sería una central. A diferencia de otros servicios este impone que el nivel 2 trabaje exclusivamente modo punto a punto (IET = 0).

3.2.4 CANALES RDSI

- **Canal B**.-Es el canal básico del usuario, transporta la información entre usuarios (datos digitales, voz digital codificada PCM, etc.) generalmente a 64Kbps. En un canal B se pueden establecer cuatro tipos de conexiones.
  - **Circuito conmutado**.-El usuario realiza una llamada y se establece una conexión de circuito conmutado con otro usuario de la red. El establecimiento de la llamada no tiene lugar en el canal B, sino en el canal D.
  - **Paquetes conmutados**.-El usuario se conecta a un nodo de conmutación de paquetes, intercambiando los datos con los demás usuarios vía X.25.
  - **Modo de trama**.-El usuario se conecta a un nodo de retransmisión de tramas y los datos se intercambian con otros usuarios vía LAP-F.
  - **Semipermanente**.-Es una conexión con otro usuario establecida anteriormente, y que no requiere un protocolo de establecimiento de llamada.
- **Canal D**.-Transporta la información de señalización entre el usuario y la red, que sirve para controlar las llamadas de circuitos conmutados asociadas a los canales B. Dependiendo de la configuración pueden tener una velocidad de 16 o 64Kbps.
- **Canal H***:* Usados para información de usuario a alta velocidad. Tienen por tanto la misma funcionalidad que los canales B, de hecho son agrupaciones de canales B con lo que conseguimos velocidades múltiplos de 64 Kbps: 384Kbps (H0), 1,536Kbps (H11) y 1,920Kbps (H12).

Ya hemos dicho que el acceso a los servicios de la red se consigue a través del canal D (canal de señalización), mientras que los datos se transportan a través de los canales B. Todos ellos son digitales, **full-dúplex** e independientes entre sí. Estos tipos de canales se agrupan en estructuras de transmisión que se ofrecen como paquetes al usuario. Podemos distinguir dos tipos de estructuras.

- **Estructura de canal básico (Acceso básico)***:* consiste en dos canales B de 64Kbps y un canal D de 16Kbps. Es una configuración para entornos con bajo volumen de tráfico, y que puede satisfacer las necesidades de la mayoría de usuarios individuales, viviendas y pequeñas oficinas.
- **Estructura de canal primario (Acceso primario)***:* Destinado a entornos con alto volumen de tráfico, como oficinas con PBX digitales, LAN o bases de datos. En Europa proporciona 30 canales B de 64Kbps y un canal D de 64Kbps consiguiendo una capacidad de 2,048Mbps. En EEUU proporciona 23 canales B de 64Kbps y un canal D de 64Kbps para una velocidad de 1,544Mbps, figura 137.

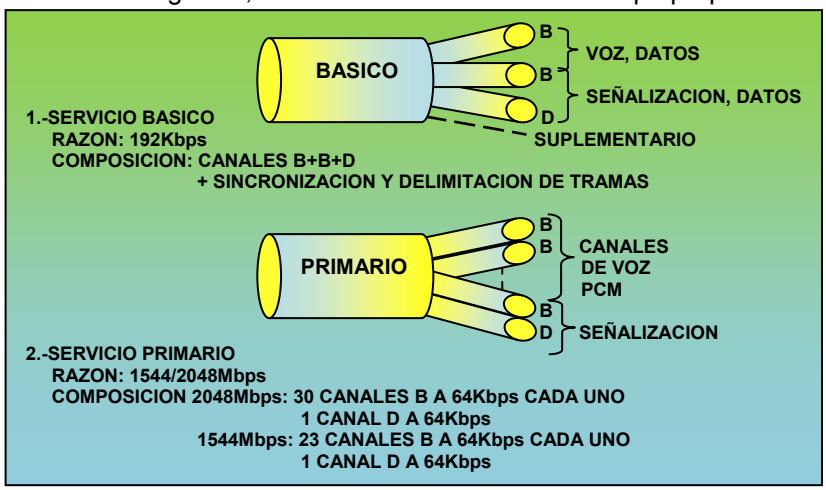


Figura 137

Para usuarios con menos requerimientos, se pueden usar menos canales B, proporcionando accesos no estandarizados (D, B+D, 6B+D, etc.).
También existen estructuras que incluyen canales H.

- **Estructura del canal H0 con interfaz de velocidad primaria**.-Admite canales H0 a 384Kbps. Para 1,544Mbps se usan las estructuras 3H0+D y 4H, mientras que para 2,048Mbps se usa la estructura 5H0+D.
- **Estructura del canal H1 con interfaz de velocidad primaria**.-La estructura del canal H11 consiste en un canal H11 a 1,536Kbps. La estructura del canal H12 consiste en un canal H12 a 1,920Kbps y un canal D a 64Kbps.
- **Estructuras con interfaz de velocidad primaria para mezcla de canales B y H0**.-Consta de uno o ningún canal D más una combinación de canales B y H0 (3H0+5B+D, 3H0+6B, etc.).

Cuando en una estructura no hay ningún canal D, se supone que otro canal D en otra interfaz primaria, en la misma posición de abonado, proporcionará cualquier señalización necesaria.

3.2.5 GRUPOS FUNCIONALES Y PUNTOS REFERENCIA

La configuración de referencia del acceso usuario-red está basado en dos elementos:

- Grupos funcionales o los modelos de las terminales.
- Puntos de referencia o interfaces de comunicación de las terminales.

3.2.5.1 Grupos funcionales

Se llaman grupos porque no intentan describir una terminal específica, sino un conjunto genérico de equipos con sus funciones y responsabilidades:

- **Terminación de Red 1 (NT1)**.-Localizado en casa del abonado es el responsable de ejecutar funciones de bajo nivel. Presenta el final de la conexión física que monitoriza el acceso a la red.
- **Terminación de Red 2 (NT2)**.-Equipo de usuario que realiza las funciones de adaptación a los distintos medios físicos, así como de la señalización y multiplexión del tráfico. Por ejemplo, una central PBX.
- **Equipo Terminal 1 (TE1)**.-Son periféricos que integran de forma nativa los protocolos ISDN y pueden conectarse directamente a la interfaz *S* y *T*. Por ejemplo, un teléfono digital o una tarjeta adaptadora para PC.
- **Equipos Terminales 2 (TE2)**.-Son aquellos periféricos que utilizan las actuales interfaces y protocolos no nativos de ISDN. Precisan de un TA para poder acceder a la red. Por ejemplo, un teléfono analógico tradicional.
- **Terminación de línea (LT)**.-Su función es simétrica a la del NT1 pero localizado al lado de la central.
- **Adaptador de Terminal (TA)**.-Permiten la conexión de los ET1 a la SDNI actuando como conversor de protocolos **V.24** o **X.21** en la señalización ISDN.

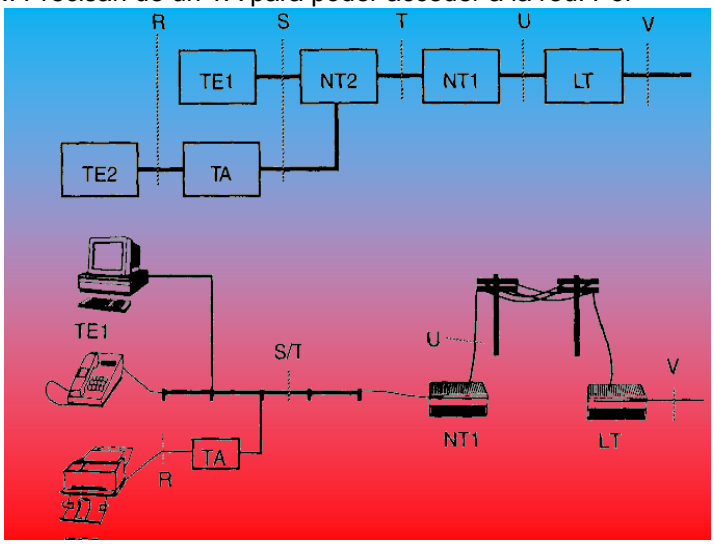


Figura 138 Modelo genérico de configuración ISDN y su implementación en un acceso básico con bus pasivo.

3.2.5.2 PUNTOS DE REFERENCIA

Son las interfaces de comunicación entre los grupos funcionales. Están definidos:

- **R**.-Son todos los protocolos no nativos de ISDN, como **V.24** o **X.21** Precisan adaptadores de terminal para conectarse.
- **S (Subscriber)**.-es el punto de acceso universal a la red para las terminales con ISDN nativo. Puede coincidir o incluir al punto T.
- **T (Interfaz entre NT1 y NT2)**.-Separa el bucle de abonado de la instalación propia del usuario.
- **U**.-Representa las características de transmisión en la línea, de forma que especifica el formato de la trama en la misma, los códigos posibles, niveles de señal, las perturbaciones permitidas (atenuación, ruido). Brinda al TR1 la posibilidad sincronización, la activación, y sirve de transporte al Acceso.
- **V (Interfaz dentro de la central)**.-Pertenece a la implementación propia de la compañía operadora.

La configuración de referencia, ver figura 139, está definida por Agrupaciones funcionales, equipos con una función concreta, y puntos de referencia o interfaces, puntos concretos en los que la ISDN presenta características de transmisión o conmutación determinadas.

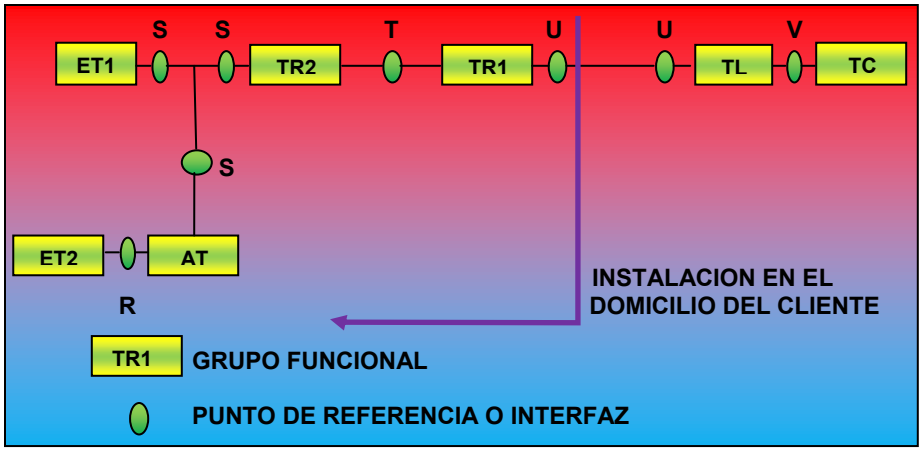


Figura 139 Configuración de Referencia.

3.2.6 PROTOCOLOS DE SEÑALIZACION

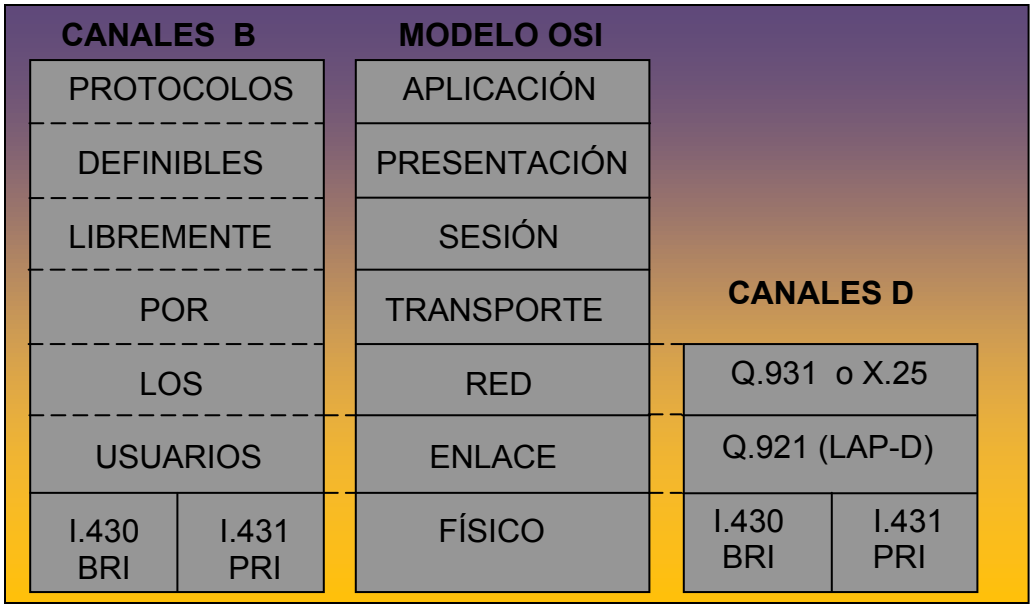


Figura 140 los canales B accesibles son auténticos circuitos que conectan los usuarios finales y proporcionan un inmejorable nivel de transparencia cuyas limitaciones son únicamente las del nivel físico.

En ISDN, el canal D tiene implementados los niveles 1, 2 y 3 del modelo OSI, mientras que los canales B sólo tienen implementado el nivel 1, lo que permite a los usuarios utilizar sus propios protocolos desde el nivel 2 hasta el 7

Protocolos en el canal D.-Los tres niveles definidos en el canal D son:

- **Nivel 1**.-Basado en la recomendación I.430, describe la conexión física entre el Equipo Terminal (TE) y el Terminal de Red (NT2). Define las características eléctricas, el tipo de conector, codificación de línea y **framming**. La conexión física es síncrona, serie y **full-dúplex**. Los canales B y D son multiplexados en el tiempo sobre la misma línea física en un mismo **frame**, desde el NT1 en casa del abonado y la central telefónica.
- **Nivel 2**.-Basado en la recomendación Q.421, describe los procedimientos que aseguran la comunicación libre de errores sobre el enlace físico y define la conexión lógica entre el usuario y la red. El protocolo también proporciona las reglas para la conexión de múltiples terminales sobre una misma línea física (multipunto). El protocolo de nivel 2 es LAP-D, una extensión del LAP-B del **X.25**, que mejora la capacidad de direccionamiento.
- **Nivel 3**.-Basado en la recomendación Q.931, define la interfaz y los mensajes de señalización entre el usuario y la red. El protocolo implementado a este nivel determina las rutas tomadas a través de la red para conectar a los usuarios entre sí. También puede utilizarse el protocolo **X.25** como nivel 3, aunque no está implementado en todas las redes.

Protocolos en el canal B.-Los niveles definidos son:

- **Nivel 1**.-Tiene exactamente la misma especificación I.430 que el canal D ya que comparten la misma línea física donde ambos canales son multiplexados.
- **Nivel 2-7**.-No está definido ninguno de estos niveles, lo que permite al usuario utilizar los protocolos que prefiera.

El canal de señalización utilizado en ISDN es conocido por ***SS7*** y es un aspecto muy significativo de la arquitectura de la red. Hasta la aparición de ISDN, las redes transportaban los datos y la señalización por el mismo medio. En ISDN, como ya hemos comentado, la señalización es transportada por los canales D, que son independientes de los canales B utilizados para transportar los datos. El término independiente no ha de tomarse en un sentido lógico, sino también físico, puesto que los canales D utilizan una propia subred con sus propios enlaces, protocolos y formatos. Se puede afirmar por tanto que ISDN está formada por dos redes separadas pero complementarias.

- Una red utilizada para transportar la información entre usuarios (canales B y H).
- Una red de señalización inteligente.

Los canales B y H al quedar liberados de la señalización, pueden ofrecer un servicio portador puro, de alta calidad y sin limitaciones de protocolos. Por otra parte, los canales D, además de gestionar la conexión y controlar los circuitos, proporcionan los servicios complementarios, incluso pueden llegar a constituir una red de paquetes X.25. Esta arquitectura segregada aporta una serie de ventajas:

- El tiempo de establecimiento de la conexión entre usuarios finales es menor.
- Es más fácil el control de la llamada durante su establecimiento y después, lográndose mayor rapidez, flexibilidad y seguridad.
- La interconexión de las bases de datos de la red de señalización permite introducir nuevos servicios, extendiendo la red de señalización para la administración de la red, monitorización y gestión.
- Al ser un estándar mundial de señalización, se simplifica la interconexión de redes y facilita el acceso a bases de datos remotas.

Se ha visto que una de las de las ventajas de la ISDN es la digitalización que se traduce en un medio muy fiable de transportar información. La segunda gran ventaja es la señalización: La señalización está estructurada en dos capas (niveles), el primero es el de enlace, es el nivel 2 y se encarga de que ante determinados errores en línea siempre posibles, la información se retransmita: El nivel 2 de la señalización ISDN usuario-red se denomina LAP-D está basado en el nivel 2 de la X.25 y se ha mejorado y adaptado a la ISDN. En primer lugar se ha hecho multiterminal ya que así lo requiere la ISDN, permitiendo hasta 64 terminales de asignación fija de **IET (identificador de equipo terminal)** y 63 de asignación automática, que es el funcionamiento

normal de las terminales. La señalización así mismo es punto a punto o en difusión, de esta manera la red ofrece una llamada entrante a todas las terminales conectadas al bus. El nivel 3 o de red es el que transporta realmente la señalización y es el que repercute directamente en los eventos que el usuario ve. Cuando una terminal (dirigido por un humano o no) debe establecer una comunicación genera un mensaje de **SETUP** establecimiento en el cual se indica con que número se quiere conectar, que capacidad de portadora necesita (voz, audio 3.1, digital sin restricciones etc.). La red a continuación a través de mensajes irá informando a la terminal del progreso de la llamada con información codificada (causas).

3.3 FDDI

3.3.1 INTRODUCCION

La **FDDI (Fiber Distributed Data Interface, Interfaz de Datos Distribuidos por Fibra)**, es una interfaz de red en configuración simple o doble anillo, uno transmitiendo en el sentido de las agujas del reloj (anillo principal) y el otro en dirección contraria (anillo de respaldo o backup) con paso de testigo, que puede ser implementada con fibra óptica, cable de par trenzado apantallado (STP-Shielded Twisted Pair), o cable de par trenzado sin apantallar (UTP-Unshielded Twisted Pair). La tecnología FDDI permite la transmisión de los datos a 100Mbps, sobre distancias de hasta 200Km o 100Km si el anillo es doble, la distancia entre nodos sucesivos no puede sobrepasar los 2Km, soportando hasta 1,000 estaciones conectadas, según la norma ANSI X3T9.5, con un esquema tolerante a fallos, flexible y escalable. Esta norma fue definida, originalmente, en 1982, para redes de hasta 7 nodos y 1Km. de longitud, denominada como **LDDI (Locally Distributed Data Interface)**. Sin embargo, en 1986 fue modificada y publicada como borrador de la norma actual, e inmediatamente aprobada, apareciendo los primeros productos comerciales en 1990.

El tráfico de cada anillo viaja en direcciones opuestas. Físicamente, los anillos están compuestos por dos o más conexiones punto a punto entre estaciones adyacentes. Los dos anillos de la FDDI se conocen con el nombre de primario y secundario. El anillo primario se usa para la transmisión de datos, mientras que el anillo secundario se usa generalmente como respaldo. Se distinguen en una red FDDI dos tipos de estaciones: las estaciones **Clase B**, o estaciones de una conexión **(SAS, Single Attach Station)**, se conectan a un anillo, mientras que las de **Clase A**, o estaciones de doble conexión **(DAS, Dual Attach Station)**, se conectan a ambos anillos. Si se produce un corte en los anillos las estaciones DAS más próximas a cada lado o del corte entre sí ambos anillos, con lo que se crea un anillo de mayor longitud que permite mantener conectados todos los hosts. En el caso de producirse un segundo corte en otro punto del anillo se crean dos anillos aislados, cada uno de los cuales puede seguir funcionando, figura 141.

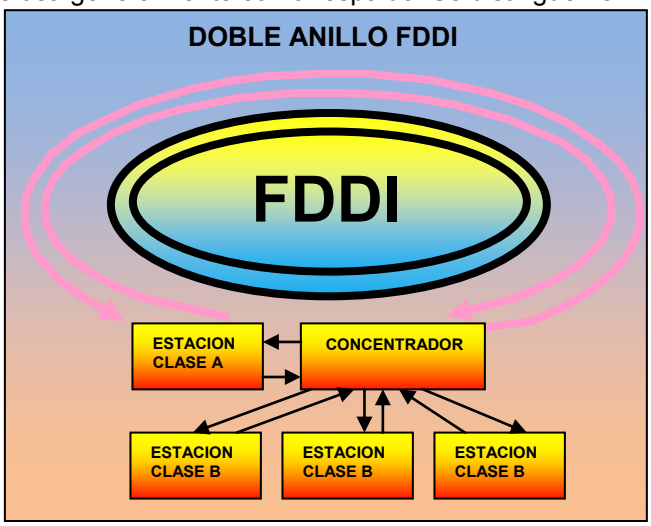


Figura 141

Las SAS se conectan al anillo primario a través de un concentrador que suministra conexiones para varias SAS. El concentrador garantiza que si se produce una falla o interrupción en el suministro de alimentación en algún SAS determinado, el anillo no se interrumpa. Esto es particularmente útil cuando se conectan al anillo PC's que se encienden y se apagan con frecuencia. Las redes FDDI utilizan un mecanismo de transmisión de tokens similar al de las redes Token Ring, pero además, acepta la asignación en tiempo real del ancho de banda de la red, mediante la definición de dos tipos de tráfico:

- **Tráfico Síncrono**.-Puede consumir una porción del ancho de banda total de 100Mbps de una red FDDI, mientras que el tráfico asíncrono puede consumir el resto.
- **Tráfico Asíncrono**.-Se asigna utilizando un esquema de prioridad de ocho niveles. A cada estación se asigna un nivel de prioridad asíncrono.

El ancho de banda síncrono se asigna a las estaciones que requieren una capacidad de transmisión continua. Esto resulta útil para transmitir información de voz y video. El ancho de banda restante se utiliza para las transmisiones asíncronas. FDDI también permite diálogos extendidos, en los cuales las estaciones pueden usar temporalmente todo el ancho de banda asíncrono.

El mecanismo de prioridad de FDDI puede bloquear las estaciones que no pueden usar el ancho de banda síncrono y que tienen una prioridad asíncrona demasiado baja. En cuanto a la codificación, FDDI no usa el sistema de Manchester, sino que implementa un esquema de codificación denominado **4B/5B**, en el que se usan 5 bits para codificar 4. Por lo tanto, dieciséis combinaciones son datos, mientras que las otras son para control. Con este sistema se gana ancho de banda con respecto a la codificación Manchester diferencial, pero se pierde capacidad de sincronización entre las estaciones, lo que debe ser compensado con unos preámbulos de tramas relativamente grandes y una elevada calidad en la construcción de los relojes de las estaciones. Es posible enviar tramas de más de 4Kbytes si se dan todas estas condiciones sin que emisor y receptor pierdan la sincronía de datos. Debido a la longitud potencial del amillo, una estación puede generar una nueva trama inmediatamente después de transmitir otra, en vez de esperar su vuelta, por lo que puede darse el caso de que en el anillo haya varias tramas a la vez. Las fuentes de señales de los transceptores de la FDDI son LED's o láser. Los primeros se suelen usar para tendidos entre máquinas, mientras que los segundos se usan para tendidos primarios de backbone. Las tramas de FDDI son similares a las de la red IEEE 802.5, pero también puede aceptar tramas síncronas procedentes de una red de transmisión ISDN conmutada o de una modulación PCM. Cada una de estas tramas síncronas se compone de una cabecera, de un campo de datos para los circuitos no conmutados (16 bytes) y de otro para los circuitos conmutados (hasta 96 bytes). Esto quiere decir que, si se utilizan los 96 bytes posibles en cada trama síncrona a razón de 1 byte por cada canal PCM, se podrían mantener 96 canales PCM abiertos, todos ellos transmitiendo datos simultáneamente en esa trama, por ejemplo, soportando 96 conversaciones telefónicas a la vez. Por ello, FDDI es una red muy apropiada para la transmisión de voz y datos, perfectamente adaptable para aplicaciones en tiempo real, que requieren transmisiones sin retardos significativos y con una cadencia de transmisión continúa.

3.3.2 TECNOLOGIA

El estándar FDDI especifica una troncal de fibra óptica multimodo, que permite transportar datos a altas velocidades con un esquema de conmutación de paquetes y paso de testigo en intervalos limitados. Se define como estación a cualquier equipo, concentrador, bridge, brouter, HUB, router, work station, conectado a la red FDDI. En cada **oportunidad de acceso** a la red, por parte de una estación, se transmite una o varias tramas FDDI, de longitud variable hasta un máximo de 4,500 bytes. La longitud máxima de 4,500 bytes es determinada por la codificación 4B/5B, con una frecuencia de reloj de 125MHz, siendo por tanto la eficiencia del 80%. En la estructura FDDI, se distinguen 4 subcapas básicas, cada una con funciones totalmente separadas:

- **PMD (Physical Media Dependent, Dependencia del Medio Físico)**.-Especifica las señales ópticas y formas de onda a circular por el cableado, incluyendo las especificaciones del mismo, así como las de los conectores. Así, es la responsable de definir la distancia máxima de 2Km. Entre estaciones FDDI y el tipo de cable multimodo con un mínimo de 500MHz y LED's transmisores de 1,300 nanómetros (nm). Estas especificaciones se cumplen en los cables de 62.5/125 micras (mm) y por la mayoría de los cables de 50/125mm. La atenuación máxima admitida en el anillo FDDI es de 11 decibeles (dB) de extremo a extremo, típicamente referenciada a 2.5dB por Km. ANSI aprobó la subcapa PMD en 1988, y se corresponde con la mitad inferior de la capa 1 (capa de enlace físico) en el modelo OSI. Existe también una especificación de fibra monomodo

("single-mode", SMF-PMD, 9mm), empleando detectores/transmisores láser para distancias de hasta 60Km. entre estaciones.

- **PHY (Physical Layer Protocol, Protocolo de la Capa Física)**.-Se encarga de la codificación y decodificación de las señales así como de la sincronización, mediante el esquema 4B/5B, que proporciona una eficacia del 80%, a una velocidad de señalización de 125MHz, con paquetes de un máximo de 4,500 bytes, proporciona la sincronización distribuida. Fue aprobada por ANSI en 1988 y se corresponde con la mitad superior de la capa 1 en el modelo OSI.
- **MAC (Media Access Control, Control de Acceso al Medio)**.-Su función es la programación y transferencia de datos hacia y desde el anillo FDDI, así como la estructuración de los paquetes, reconocimiento de direcciones de estaciones, transmisión del testigo, y generación y verificación de secuencias de control de tramas **(FCS o Frame Check Sequences)**. Se corresponde con la mitad inferior de la capa 2 del modelo OSI (capa de enlace de datos) y fue aprobada por ANSI en 1986.
- **SMT (Station Management, Gestión de Estaciones)**. Se encarga de la configuración inicial del anillo FDDI, y monitorización y recuperación de errores. Incluye los servicios y funciones basados en tramas, así como la gestión de conexión **(CMT o Connection Management)**, y la gestión del anillo **(RMT o Ring Management)**. Se solapa con las otras 3 subcapas FDDI, y por tanto fue la de más complicada aprobación por parte de ANSI, que se realizó en 1993.

En los últimos meses han quedado definidas normas que permiten el uso de cableados de cobre en lugar de fibra, con la ventaja de su menor costo, e incluso del aprovechamiento de instalaciones ya existentes, con codificación MLT3. Es lo que se ha denominado **TPDDI (Twisted Pair Distributed Data Interface)**, e incluso CDDI **(Copper Distributed Data Interface)**. Se emplean cables IBM tipo 1 (Token Ring) y conectores DB-9 para STP, mientras que para UTP se utiliza cable de categoría 5 (Data Grade) y conectores RJ-45 (los mismos que para Ethernet 10BASET). En ambos casos, la distancia máxima es de 100 metros. Anteriormente, se había intentado emplear cableado de par trenzado tipo 1 (IBM STP), también con conectores DB-9, pero con codificación NRZI. Aunque no ha sido estandarizado por ANSI, 11 fabricantes emplean esta configuración, denominada SDDI-STP. Por ello, algunos fabricantes han echo sus productos TPDDI compatibles con CDDI.

3.3.3 NIVELES DEL MODELO OSI

La especificación de FDDI abarca los niveles físico y de enlace del modelo OSI y, a su vez, establece dos subniveles dentro de la capa física y otras dos dentro de la capa de enlace. El nivel físico está dividido en un subnivel dependiente del medio (PMD) y un protocolo del nivel físico (PHY). El primero de ellos define las características del medio de transmisión, incluyendo los enlaces de fibra óptica, niveles de potencia, tasas de error, componentes ópticos y conectores. El protocolo del nivel físico, a su vez, define los algoritmos de codificación y decodificación, la temporización de las señales, así como otras funciones. El nivel de enlace queda dividido en un subnivel de control de acceso al medio (MAC) y un subnivel de control del enlace lógico (LLC). LLC está definido por el estándar IEEE 802.2 independientemente de FDDI, utilizándose este último en múltiples protocolos de enlace. El MAC define la forma en la que se accede al medio, incluyendo la especificación del formato de las tramas, la manipulación del testigo (token), el direccionamiento, los algoritmos para calcular los valores **CRC (Cyclic Redundancy Check)** y los mecanismos de recuperación de errores. De forma adicional, FDDI define la capa de la estación de gestión (SMT) donde se especifica la configuración de la estación FDDI, la configuración y las características del control del anillo, que incluye la inserción y extracción de estaciones, inicialización, aislamiento a los fallos y recuperación, programación y recopilación de estadísticas. A continuación en la figura 142 se muestran los niveles físico y de enlace de FDDI:

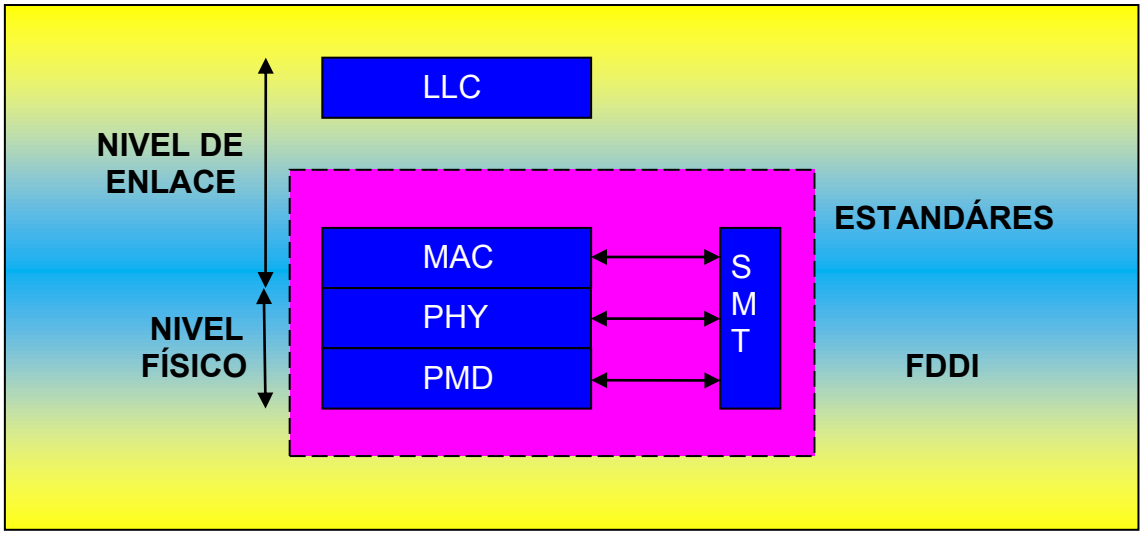


Figura 142

FDDI tiene cuatro componentes claves; el control de acceso al medio (MAC), la capa física (PHY), la capa dependiente del medio físico (PMD), y la capa de manejo de estación (SMT). FDDI es un protocolo de la capa de enlace, que significa que los protocolos de las capas más altas operan independientemente del protocolo FDDI. Las aplicaciones van usando los protocolos desde las capas más altas hasta la capa de control de enlace lógico, en el mismo sentido que lo pueden hacer en Ethernet o Token Ring. Pero debido a que FDDI usa un protocolo de capa física distinto al de Ethernet o Token Ring, el tráfico debe ser puenteado o enrutado fuera del anillo FDDI. FDDI también permite paquetes de mayor longitud que las redes de baja velocidad; por esta razón, las conexiones entre una FDDI y LAN's Ethernet o Token Ring requieren de fragmentación o reensamblado de tramas. La capa física maneja la codificación y descodificación de paquetes de datos en flujos de símbolos. También maneja la sincronización del reloj en el anillo FDDI. La capa PMD maneja la transmisión analógica en banda base entre los nodos del medio físico. El estándar PMD incluye TP-PMD para par trenzado de cobre y Fiber-PMD para cable de fibra óptica. TP-PMD, es un estándar nuevo de ANSI, que reemplaza al preestándar previamente usado para ejecutar tráfico en FDDI sobre cables de cobre. El estándar TP-PMD esta basado en el esquema de codificación MLT-3, anteriormente se usaba el esquema NRZ, menos fiable. Las interfaces TP-PMD proporcionan una transmisión fiable sobre distancias de hasta 100m. La capa MAC define el direccionamiento, planificación, y enrutado de datos. También se comunica con los protocolos de las capas más altas, tales como TCP/IP, SNA, IPX, DECnet, DEC LAT, y Appletalk. La capa MAC de FDDI acepta mensajes **(PDU's-Protocol Data Units)** de hasta 9,000 símbolos procedentes de los protocolos de las capas superiores, añadiéndolos a la cabecera MAC, y luego pasándolos en paquetes de hasta 4,500 bytes a la capa física, figura 143.

Figura 143 Formato del a) Token FDDI b) trama FDDI

La estructura de un frame y token FDDI es muy similar a la de Token Ring. El protocolo MAC de FDDI es también muy parecido al de Token Ring. La diferencia más notable es que en FDDI siempre funciona con el principio de Early Token Release. Existe también un token-holding timer que establece el tiempo máximo que una estación puede transmitir de una vez. Este parámetro

tiene importantes consecuencias en el rendimiento de la red. El valor por defecto de 4ms es adecuado en la mayoría de las situaciones, excepto en las redes muy grandes (más de 20Km) en que es conveniente aumentarlo. La normalización define el contenido de este formato en términos de símbolos, donde cada símbolo corresponde con 4 bits de datos. Se usan símbolos debido a que, en la capa física, los datos se codifican en grupos de cuatro bits. Sin embargo, las entidades MAC deben tratar bits individuales, de modo que la discusión que sigue se refiere a veces a símbolos de cuatro bits y otras veces a bits individuales

La filosofía que persigue FDDI es atender primero el tráfico síncrono y después el tráfico asíncrono. Para ello, cada estación tiene varios temporizadores:

- **Token Rotation Time (TRT)**.-Tiempo transcurrido desde que llegó el último testigo.
- **Token Hold Time (THT)**.-Tiempo máximo que una estación puede poseer el testigo.
- Todas las estaciones tienen un parámetro fijo, el **Target Token Rotation Time (TTRT)**, que fija el tiempo que tarda el testigo en dar una vuelta al anillo, y cada una tiene un parámetro propio, **Syncronous Time (ST o Ci)**. Este parámetro fija el tiempo máximo que una estación está transmitiendo tráfico síncrono.
- **Tiempo de Transmisión Valido (TVX)** y **Tiempo de Rotación del Token (TR)**. Los siguientes elementos de cálculo de tiempos son tomados del estándar FDDI. **Dmax=** 1,617 ms (por defecto) = Latencia máxima del anillo. Donde Dmax es la latencia máxima (por ejemplo: retraso de circulación) del delimitador de comienzo para viajar alrededor del anillo expresado en tiempo. Consiste en el retraso total del cable del anillo más el tiempo total de latencia de todas las estaciones. Puede acomodarse en una gran variedad de topologías. Por ejemplo: considerando sólo los retrasos de los componentes del camino en un camino de 200Km, el retraso de SD en esta distancia es 1,017ms, asumiendo una velocidad de propagación aproximada de 5,085ns/Km. El limite de la longitud del camino de 200Km permite una longitud total del cableado del anillo de 100Km, el cual acomoda la longitud del camino de ida y vuelta que existe entre las conexiones de tipo clase B tanto como la longitud total del cable para los caminos formados por las conexiones de clase A, plegado sobre ellos mismo durante tiempos cuando son configurados en forma de cadena. Si restamos del total de latencia máxima del anillo (1,617ms), el valor del retraso del camino (1,017ms), nos quedan 0,600ns. Y si luego asumimos que el número total de conexiones físicas sean 1,000 y dividimos este valor entre 0.600ms, nos quedaría una latencia por estación del 600ns, ó 15 símbolos por conexión física. Otros valores dados en la referencia son :
  Mmax= 1,000 (por defecto) = Máximo número de entidades MAC
  Imax = 25ms = Tiempo máximo de inserción de estación física.
  Amax = 1ms = Tiempo máximo de adquisición de la señal.
  Tiempo Token = 0.00088ms = Longitud del Token (6+16 símbolos).
  Lmax =0.0035ms = Máximo tiempo para transmitir la trama setup.
  Fmax = La longitud máxima de la trama es 9,000 símbolos más 16 símbolos de preámbulos.
  Petición FR = 0.00256ms = Longitud de petición de trama. La petición FR es el tiempo requerido para transmitir una trama de petición y los 16 símbolos de preámbulo.

El mecanismo que se sigue es el siguiente:
1) Cuando llega el testigo, comprobamos que ha llegado a tiempo. Para ello, vemos si TRT > 0. Si es cierto, la estación captura el testigo. Si es falso, la estación lo deja pasar a la siguiente estación. En cualquier caso, TRT se reinicializa a TTRT.
2) Una vez que la estación posee el testigo, el valor de TRT se carga en THT. Se comienzan a transmitir tramas síncronas.
3) THT llega a cero. En ese caso, se termina el turno de la estación, y se pasa el testigo a la siguiente.
4) Antes de que THT llegue a 0 se acaban las tramas síncronas que tenía la estación preparada para transmitir. Se transmiten ahora todas aquellas tramas asíncronas de que se dispongan, hasta que THT llegue a cero.
5) Si acabamos también las tramas asíncronas, pasamos el testigo.

Se plantea un problema cuando se acaba el THT mientras se está transmitiendo una trama. Este fenómeno se llama **over run.** El intervalo máximo entre dos testigos en una estación ronda 2*TTRT. SMT se encarga del manejo del anillo FDDI. Las funciones proporcionadas por SMT incluyen la identificación de vecinos, detección de fallos y reconfiguración, inserción y eliminación de nodos en el anillo, y la monitorización estadística del tráfico. Otro camino relativo a este problema es usar concentradores para construir redes. Los concentradores son dispositivos con múltiples puertos donde los nodos FDDI son conectados. La función de los concentradores FDDI es similar a los hubs de Ethernet o las unidades de múltiple acceso **(MAU's)** de Token Ring. Los nodos son conectados al concentrador, el cual aísla los fallos cuando ocurre en estas estaciones finales. Con un concentrador, los nodos pueden ser activados o desactivados. Los concentradores hacen a las redes FDDI más fiables y también proporcionan funciones de manejo SNMP. Por esta razón, muchas de las redes FDDI actuales están construidas con concentradores.

3.3.4 TRAMA FDDI

Las tramas en la tecnología FDDI poseen una estructura particular. Cada trama se compone de los siguientes campos, ver la figura 143:

- **Preámbulo**.-Sincroniza la trama con el reloj de cada estación. La estación que originó la trama usa un campo de 16 símbolos libres (64 bits); estaciones sucesivas pueden cambiar la longitud del campo de acuerdo con los requisitos de temporización. El símbolo libre es un patrón completo de no datos. La forma real de un símbolo de no datos depende de la codificación de la señal en el medio.
- **Delimitador de comienzo (SD, Starting Delimiter)**.-Indica el comienzo de la trama. Se codifica como JK, donde tanto J como K son símbolos de no datos.
- **Control de trama (FC, Frame Control)**.-Tiene el formato de CLFFZZZZ, donde C indica si la trama es síncrona o asíncrona; L indica el uso de direcciones de 16 a 48 bits; FF indica si es una trama LLC, de control MAC o reservada. Para una trama de control, los restantes 4 bits indican el tipo de trama de control.
- **Dirección de destino (DA)**.Especifica la estación o estaciones a las que va dirigida la trama. Puede ser una única dirección física, una dirección de grupo multidestino o una dirección de difusión. El anillo puede contener una mezcla de longitudes de dirección de 48 bits.
- **Dirección origen (SA)**.-Especifica la estación que envió la trama.
- **Información**.-Contiene datos LLC o información relacionada con una función de control.
- **Secuencia de comprobación de trama (FCS)**.-Comprobación de redundancia cíclica de 32 bits referente a los campos FC, DA, SA y de información.
- **Delimitador de fin (ED)**.-Contiene un símbolo de no datos (T) y marca el final de la trama sin contar el campo FS.
- **Estado de trama (FS)**.-Contiene los indicadores de detección de error (E), dirección reconocida (A) y trama copiada (C). Cada indicador se representa mediante un símbolo, que es **R** para **reinicio** o **falso**, y **S** para **activo** o **verdadero**. Una trama de testigo consta de los siguientes campos:
    - **Preámbulo**.-Como antes.
    - **Delimitador de comienzo**.-Como antes.
    - **Control de trama (FC)**.-Presenta el formato de bits 10000000 ó 11000000 para indicar que se trata de un testigo.

3.3.5 GESTION DE FALLOS

Para los problemas relacionados con el manejo de testigos, FDDI especifica técnicas generales de gestión de fallos. Todas las estaciones de la red son responsables de la monitorización del protocolo de paso de testigo y de la inicialización del anillo si se producen condiciones no válidas. Una condición no válida incluye un período largo de inactividad del anillo (lo que indica un testigo perdido), o un período largo de transmisión de datos sin un testigo (lo que significa un paquete de datos persistente). Cuando una estación detecta cualquiera de estas condiciones, comienza la

inicialización del anillo con el procedimiento de **reclamación del testigo**. La estación emite un flujo continuo de paquetes de datos de control, denominados **paquetes de reclamación**. Cada paquete de datos contiene un valor de TTRT sugerido. Si una estación que envía paquetes de reclamación recibe uno de otra estación, compara sus valores de TTRT. Si su propio TTRT es menor, continua transmitiendo los paquetes de reclamación. Si el valor de la otra estación es menor, transmite los paquetes de dicha estación. Si los valores son iguales, se usa la dirección de la estación para determinar que estación tiene precedencia. Eventualmente, el paquete de reclamación que tiene el menor valor de TTRT pasa por otras estaciones y vuelve a la estación transmisora. En este momento, la estación transmisora se reconoce como la ganadora del proceso de reclamación del testigo. Entonces comienza la inicialización real del anillo. La ganadora del proceso de reclamación del testigo transmite un testigo que contiene su valor de TTRT. Las demás estaciones reconocen que ahora el anillo se ha inicializado ya que, anteriormente, han recibido los paquetes de reclamación en lugar de los testigos. Cada estación salva el valor TTRT, realiza el proceso de inicialización y pasa el testigo a la siguiente estación. No se transmite ningún paquete de datos hasta que el testigo ha pasado una vez por el anillo. Cuando se produce un fallo importante, tal como una ruptura del anillo, se usa un **proceso faro**. Cuando una estación que ha estado transmitiendo paquetes de reclamación reconoce que ha transcurrido un periodo específico sin resolución del proceso de reclamación del testigo, inicia el proceso faro transmitiendo un flujo continuo de paquetes faro. Si una estación recibe de otra un paquete faro, detiene la transmisión de sus paquetes faro y pasa los que ha recibido. Los paquetes faro de la estación inmediatamente siguiente a la ruptura se propagaran, eventualmente, a través de la red, permitiendo la reconfiguración de la misma. Si una estación recibe sus propios paquetes faro, supone que el anillo se ha restablecido e inicia el proceso de reclamación del testigo.

3.4 SONET

3.4.1 INTRODUCCION

SONET **(Synchronous Optical NETwork)** originalmente propuesto por Bellcore **(Bell Comunication Research)**, normalizada por ANSI; define un estándar para señales ópticas, una estructura de trama para el multiplexado de tráfico digital y un tráfico de operaciones. Sonet se ideo para proporcionar una especificación que aproveche las ventajas que proporciona la transmisión digital de alta velocidad a través de fibra óptica. En sus orígenes, a mediados de los años 80's, SONET se refería solamente a la interconexión de las redes telefónicas de las compañías de teléfonos estadounidenses. Los canales de voz numéricos se iban integrando progresivamente, por multiplexación temporal, a canales más grandes, en una jerarquía de niveles basada en una codificación a 51.84Mbps, en la que todos los elementos estaban perfectamente sincronizados. Entonces se estandarizaron ocho niveles de multiplexación SONET que se designaron con la abreviatura **STS (Synchronous Transport Signal)**. Cuando el soporte de transmisión es una fibra óptica, hay una correspondencia bit a bit entre los canales eléctricos STS y los canales ópticos, medidos éstos con la abreviatura **OC (Optical Carrier)**. Desde entonces, la capacidad de los canales ópticos ha seguido creciendo, lo que se refleja en la tabla 20:

Afluente eléctrico	*Canal óptico*	Caudal (Mbps)
STS-1	OC-1	51.84
STS-3	OC-3	155.52
STS-9	OC-9	466.56
STS-12	OC-12	622.08
STS-18	OC-18	933.12
STS-24	OC-24	1,244.16
STS-36	OC-36	1,866.24
STS-48	OC-48	2,488.32
	OC-96	4,976.64
	OC-192	9,953.28

Tabla 20

SONET persigue los siguientes propósitos:

- Compatibilidad en los equipos construidos para manejo de fibra óptica.
- Redes Síncronas.
- Manejo avanzado de **OAM&P *(*Operations, Administration, Maintenance, and Provisioning*)***.
- Eficiencia a la hora de extraer/agregar tramas ***(*ADM, Add/Drop Multiplexing).**
- Estándares para manejo de anillos.
- Manejo de transporte de nuevos servicios como **(ATM, Asynchronous Transfer Mode)**.

3.4.2 CARACTERISTICAS

Es un sistema síncrono con multiplexación por división en el tiempo (TDM). Se transmite una trama cada 125ms, haya o no datos útiles que transmite (8,000 tramas por segundo). Hay distintos tipos de canales estandarizados para distintas velocidades cada una con un tamaño de trama diferente. Así, en STS-1 (51.84Mbps) las tramas son de 810 bytes.

3.4.2.1 RED DE ELEMENTOS SONET

SONET se despliega típicamente encima de la fibra óptica en un modo de dual-anillo, como mostrado en el cuadro siguiente:

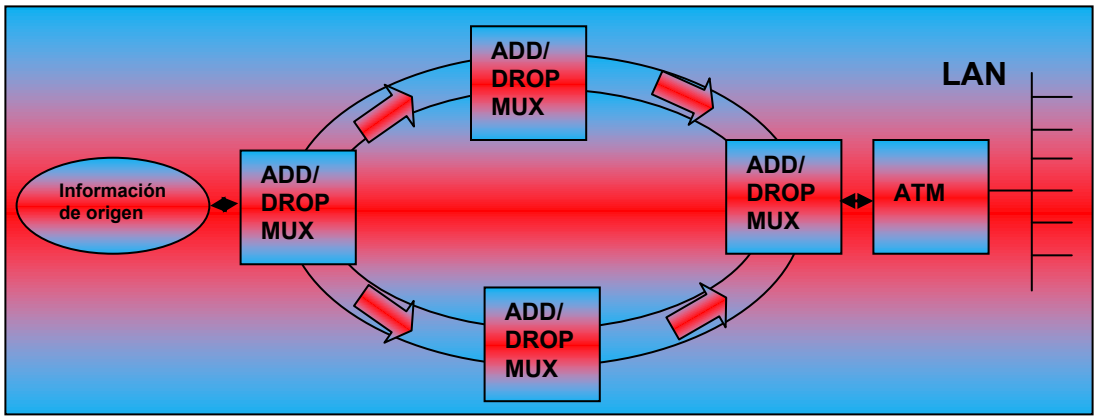


Figura 144 Sonet Network Using Dual-Ring

Los Multiplexores de Add/Drop (ADM) la inserción y quita payload del usuario originado de las fuentes de información, como un interruptor de ATM, en los marcos de SONET que circulan en el anillo. Los anillos duales habilitan tolerancia de la falta ejecutando el cambio del anillo del funcionamiento al anillo alternado de protección cuando un fracaso ocurre. El sistema de SONET despliega los tipos siguientes de elementos de la red, figura 145.

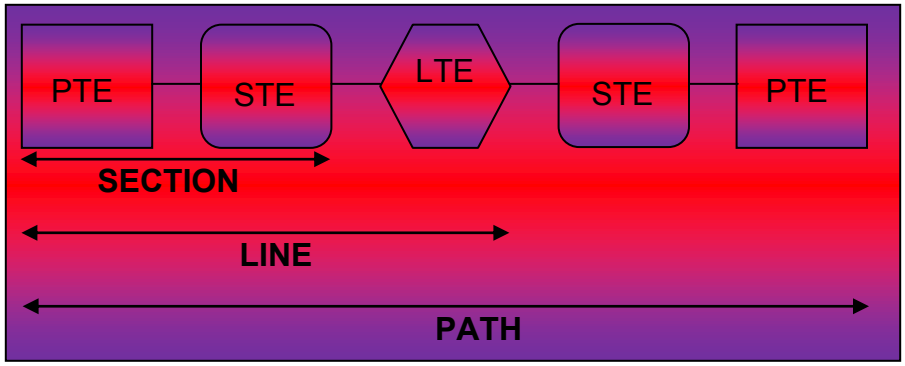


Figura 145 Sonet Network Elements

- **Camino Terminando Equipo (PTE)**.-Es el STS camino terminando equipo es un elemento de red que multiplex/demultiplex la STS carga útil. El puede producir, acceso, modificar o terminar el camino por encimas de la cabeza, o poder realizar algunas combinaciones de estas combinaciones, por ejemplo. un STS camino terminando equipo reúne 281,554Mbps DS1 señales e insertan camino por encima de la cabeza a desde un 51.84Mbps STS-1 señal.
- **Línea terminando Equipo (LTE)**.-Línea terminando equipo es el elemento de red que produce o termina señal de línea, el puede producir acceso, modificar o terminar la línea por encima de la cabeza, o poder combinar algunas combinaciones de estas acciones.
- **Sección Terminando Equipo (STE)**.-Sección terminando equipo son dos elementos próximos de la red de SONET. Puede ser un elemento terminado de red o un regenerador. El puede producir, acceso, modificar o terminar la sección por encima de la cabeza o poder realizar una combinación de las acciones.

3.4.3 ESTRUCTURA DEL MARCO SONET STS-1

El cauce de SONET básico es un Transporte **Signal-1 Síncrono (STS-1)** que consiste en marcos que tienen 810 bytes organizados en 9 filas a través de 90 columnas. A 8,000 marcos por segundo, esto da una proporción del cauce de 51.840Mbps. El STS-1 marco se muestra en la figura 146:

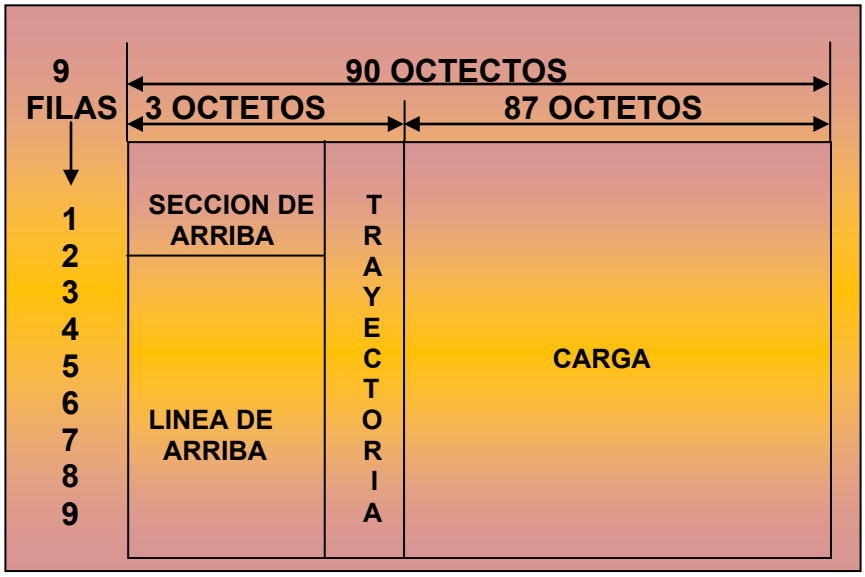


Figura 146 Sonet STS-1 Estructura de la Trama.

El arriba para SONET gerente linee y el equipo de la sección consume 3 de las 90 columnas, dejando 87 columnas para el payload. El payload, llamó el **Sobre de Payload Síncrono (SPE)**, incluye el camino sobre la cabeza de 1 columna. Esto deja 86 columnas para el payload del usuario que proporciona datos del usuario a una tasa de 86 x 9 x 8 x 8000 = 49.536Mbps.
Indicadores Payload.-Aunque SONET proporciona una estructura del marco síncrono no reprime el Payload para ocurrir a las posiciones específicas en el marco de SONET. En cambio, permite el payload del usuario a **Flotador** dentro de y por Sonet los limites idean, usando campo en lo bytes arriba del Sonet, apuntar al principio del payload del usuario idean una perspectiva del usuario Sonet proporcionando a su vez la capa física bytes-síncronos.
Jerarquía de multiplexores Sonet.-Los datos tasa más alto que STS-1 son obtenidos multiplexando los STS-1 signos múltiples. Por ejemplo, puede un byte entrelazarse tres STS-1 signos para formar un STS-3 signo que opera a 155.52Mbps. Otra forma de multiplexar es encadenar el arriba y bytes del payload de múltiplo STS-1 signos. Por ejemplo, un STS-3c marco contiene 9 columnas arriba (para la sección y camino sobre la cabeza) y 261 columnas para el SPE. La proporción operando es el mismo a 155.52Mbps. La SONET multiplexing jerarquía se muestra en la tabla 21:

Electrical Signal	Optical Signal	Gross Rate (Mbps)	User Rate (Mbps)
STS-1	OC-1	51.84	49.536
STS-3	OC-3	155.52	149.460
STS-12	OC-12	622.08	594.432

Tabla 21 Sonet Multiplexing Hierarchy

CANALES

SONET	SDH	Mbps
STS-1		51.84
STS-3	STM-1	155.52
STS-9	STM-3	466.56
STS-12	STM-4	622.08
STS-18	STM-6	933.12
STS-24	STM-8	1244.16
STS-36	STM-12	1866.24
STS-48	STM-16	2488.32

Todos los canales son múltiplos del STS-1.
STS: Synchronous Transport Signal = OC: Optical Carrier.
STM: Synchronous Transport Mode.

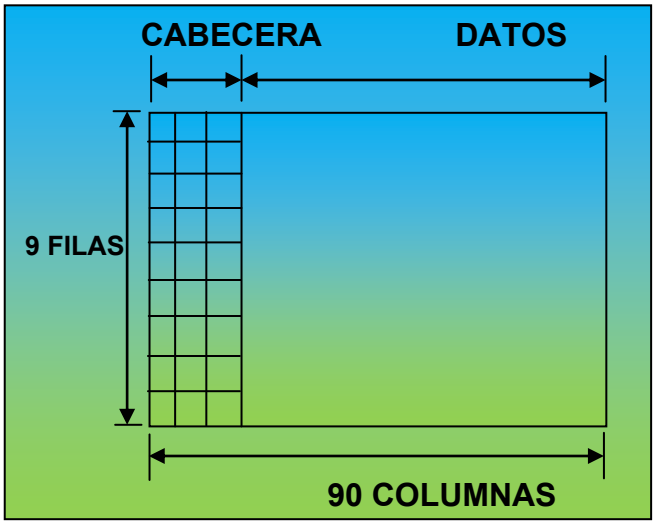


Figura 147

3.4.3.1 MULTIPLEXAJE EN SONET

Además del formato base STS-1, SONET también define formatos síncronos a niveles inferiores del STS-1 llamados **sub-STS-1 *(VT's)***. El STS-1 SPE puede ser subdividido en **Virtual Tributaries** que son señales síncronas usadas para transportar otras señales de más baja velocidad. Los tamaños de los VT's son los de la tabla 22:

Tipo	Transporte para (típico)		VT Rate
VT-1.5	1 DS-1	1.544 Mbps	1.728 Mbps
VT-2	1 CETP 1	2.048 Mbps	2.034 Mbps
VT-6	1 DS-2	6.312 Mbps	6.912 Mbps

Tabla 22 Rates de transmisión de los VT

Dado que la cantidad de tramas de baja velocidad que llegan a un multiplexor es muy grande y además las tramas son de distintos tamaños estas no se pueden agrupar en un simple VT. Para solucionar esto existen 4 tipos distintos de VT's. Si se intercalan 7 de ellos se forma un STS-1. Es decir que un STS-1 esta conformado por 7 grupos de VT's. Un grupo de VT esta conformado por 12 columnas de 9 bytes cada una. De manera que cuatro VT 1.5 forman un grupo, dos VT 3 forman un grupo un VT 6 forma otro grupo y así sucesivamente, figura 148. Los grupos son de un tipo de VT único de manera que no se pueden mezclar VT's en un grupo.

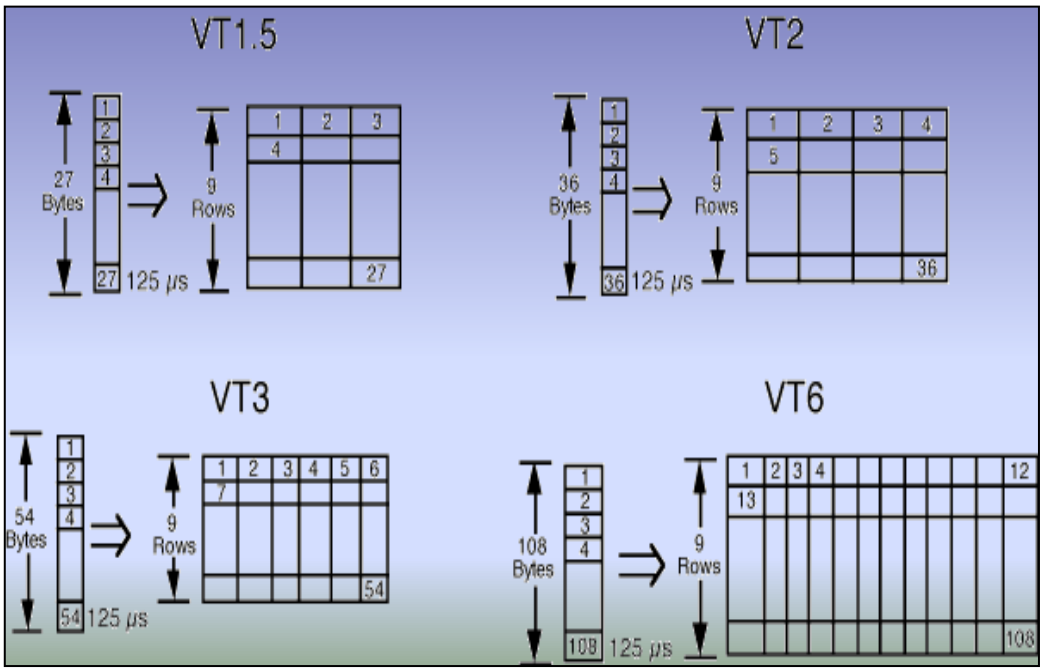


Figura 148 Tipos de VT

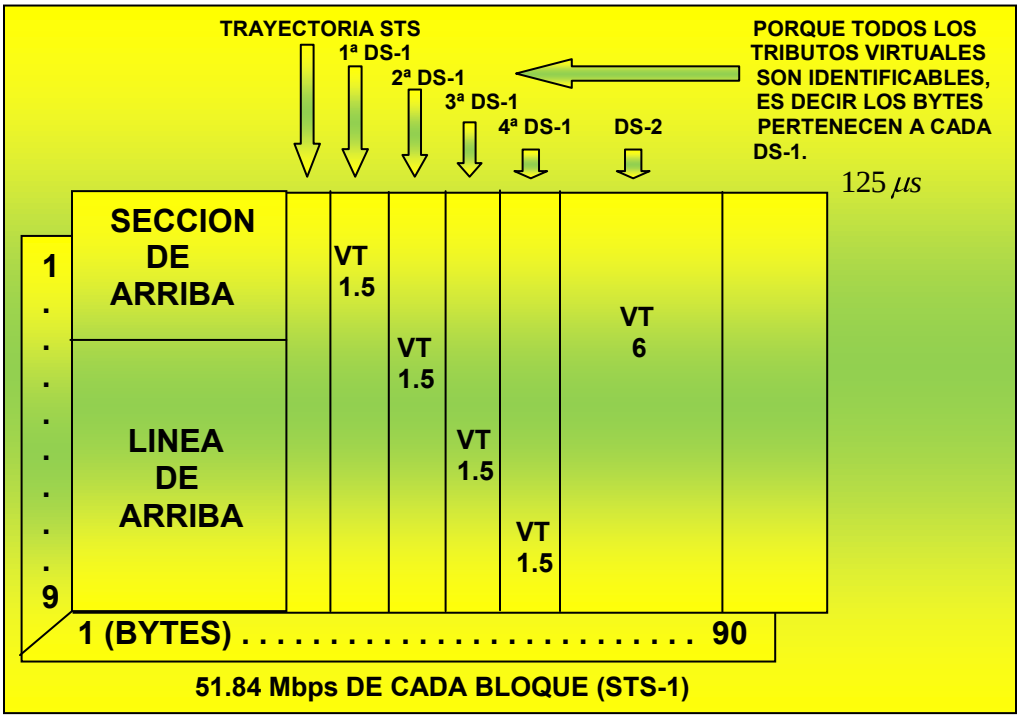


Figura 149 Grupos de VT

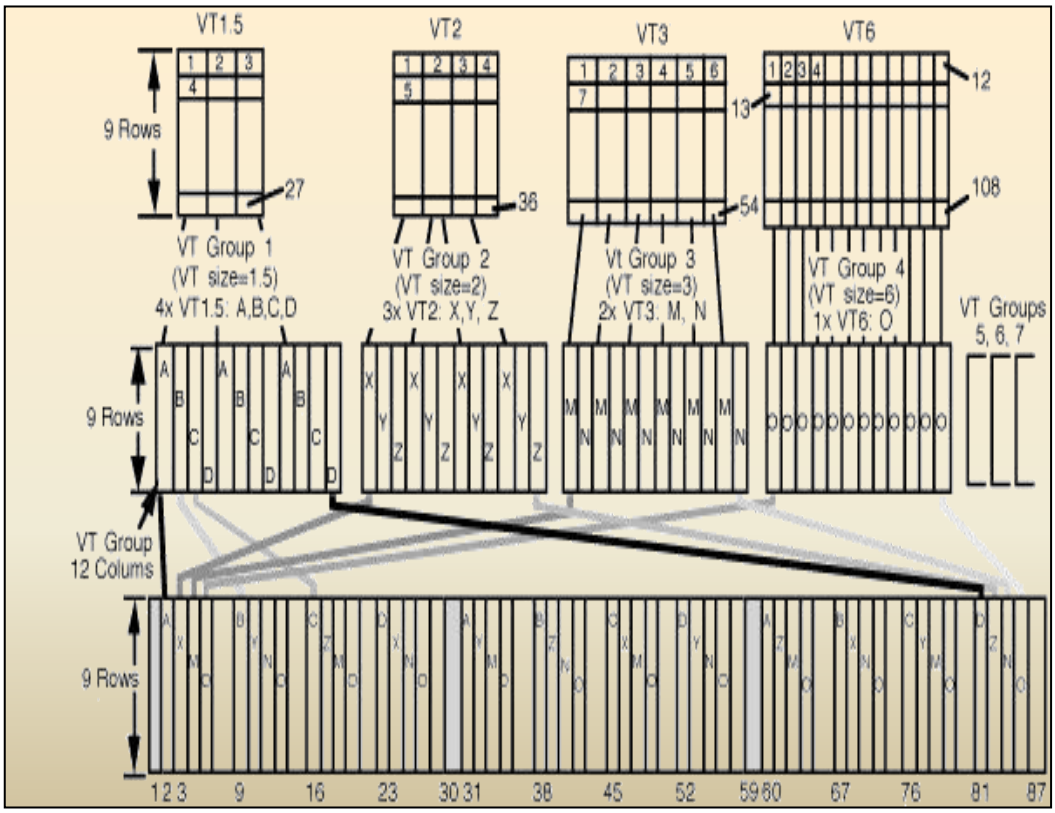


Figura 150 Intercalado de columnas de VT en un STS-1 pasaran a formar parte del contenido (o información real, no de overhead) de los paquetes STS-1.

La figura 151 ilustra básicamente la estructura del multiplexaje de SONET. Cualquier tipo de servicio, desde voz hasta datos y video de alta velocidad, puede ser aceptado por varios tipos de **adaptadores de servicios**. Un adaptador de servicio es el instrumento necesario para convertir estas señales, en señales de más alta velocidad, las cuales **(VT) - Virtual Tributaries.** Nuevos servicios y una gran cantidad de señales pueden ser transportadas, siempre y cuando se posean los **adaptadores de servicios - (Service Adapters)** apropiados para ingresar a una red SONET.

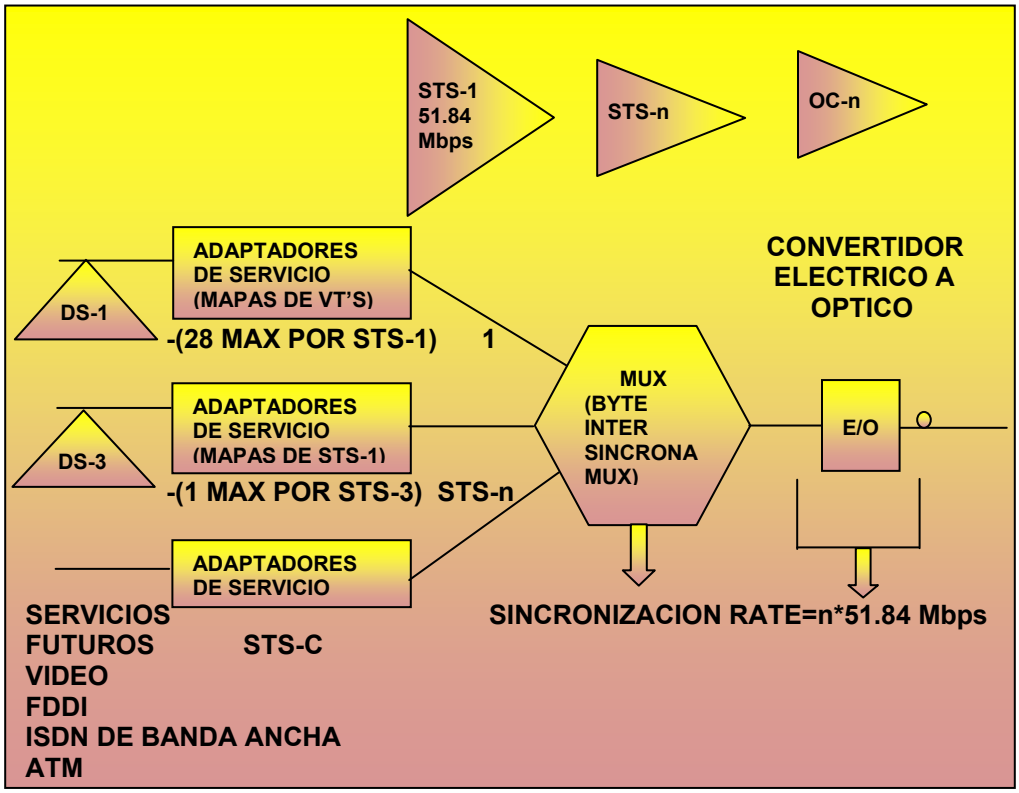


Figura 151 SONET Multiplexing

Todas las entradas son eventualmente convertidas a una señal de formato base (STS-1 - 51.84Mbps o mayor). De manera que las señales de menor velocidad como las **DS-1** son las primeras en convertirse en VT. Después de convertirse en un STS-1 muchos de estos son multiplexados juntos en varias o individuales señales eléctricas STS-n El multiplexaje de los STS es realizado en el **Byte Interleave Synchronous Multiplexer**. Luego del multiplexaje ningún otro proceso es requerido para el procesamiento de la señal, lo único que se necesita es una reconversión de la señal eléctrica a señal óptica.

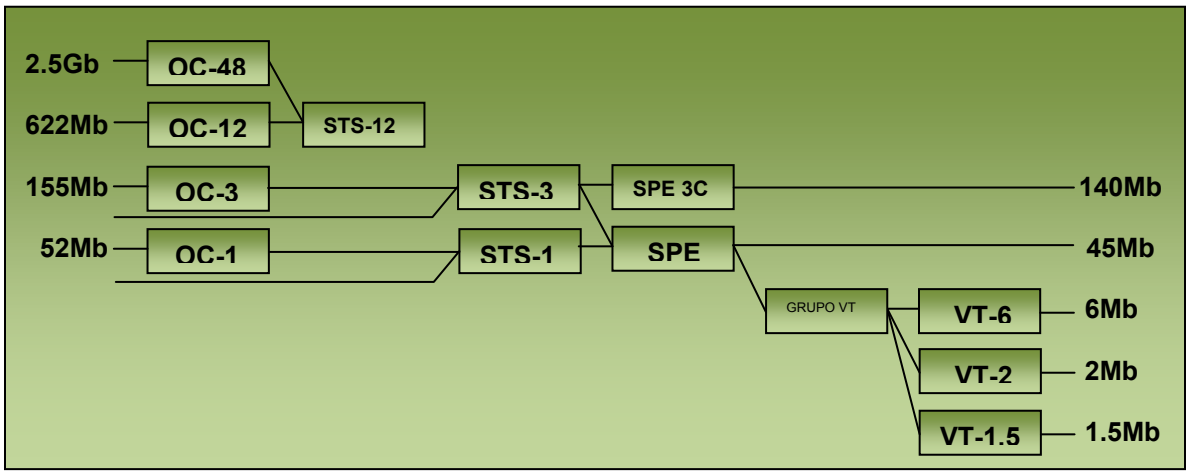


Figura 152 Otra forma de ver el multiplexaje

SONET provee el ancho de banda necesario para transportar información de un switch ISDN (o terminal) a otro.

3.4.3.2 ESTRUCTURA DEL FORMATO DE LA TRAMA SONET

Ahora bien, el formato de la trama de STS-1 es mostrado en la figura 153. En general, la trama puede ser dividido en dos áreas principales: **transport overhead** y **Synchronous Payload Envelope (SPE)**. El SPE puede también ser dividido en dos partes: EL STS **path overhead (POH)** y el payload. El payload es la información en si a ser transportada y enrutada a través de la red de SONET. Una vez que el payload es multiplexado en el SPE, puede entonces ser transportado sin tener que ser examinado y posiblemente demultiplexado en los nodos intermedios. De esta forma, se dice que SONET es un servicio independiente o transparente. Por otra parte, transport overhead esta compuesto de dos partes: **section overhead y line overhead**. El STS-1 POH (Path Overhead) es parte del SPE. El STS-1 payload tiene la capacidad de transportar lo siguiente:

- 28 DS-1s.
- 1 DS-3.
- 21 señales de 2,048Mbps.
- Combinación de cada uno de los anteriores.

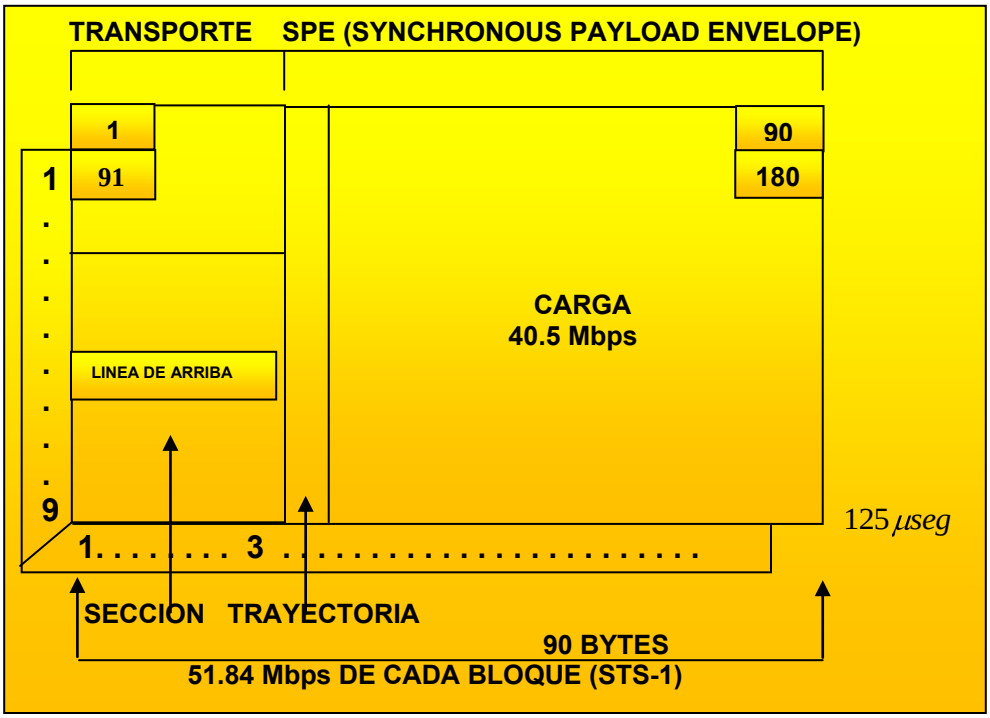


Figura 153 Formato de la trama STS-1

3.4.3.2.1.-ESTRUCTURA DE LA TRAMA STS-1

STS-1 es una secuencia específica de 810 bytes (6,480 bits), los cuales incluyen varios bytes de overhead y otros destinados para información. Puede ser visto como una matriz de 90 columnas por 9 filas. Con una longitud de 125 microsegundos (8,000 muestras por segundo), STS-1 tiene un bit rate de 51,840Mbps. Esta cifra viene de la siguiente formula:

(9) * (90 bytes/frame) * (8 bits/byte) * (8000 frames/s) = 51,840,000bps = 51.480Mbps.

Esta es conocida como la rate señal/rate eléctrica usada principalmente para transportar dentro de una pieza específica de hardware. El equivalente óptico de STS-1 es conocido como OC-1, y es usado para transmitir a través de la fibra. El orden de transmisión de los bytes es fila por fila, de arriba hacia abajo y de izquierda a derecha (comenzando por el bit más significante). Como fue mostrado en la figura 147, las primeras columnas del frame STS-1 son para la parte de transport overhead. Las tres columnas contienen 27 bytes. De estos, 9 bytes son destinados para la capa de sección (por ejemplo, cada section overhead), y 18 bytes son destinados para el line layer (por ejemplo, line overhead). Las restantes 87 columnas constituyen el SPE.

3.4.3.2.2 ESTRUCTURA DEL SPE

La figura 154 muestra la estructura del SPE STS-1, la cual contiene la capacidad de información del STS-1. El SPE STS-1 consiste de 783 bytes, y pueden ser mostrados como una matriz de 87 columnas por 9 filas. La columna 1 contiene 9 bytes, designados como el STS-POH. 2 columnas (columnas 30 y 59) no son usadas para llevar información pero están designadas como columnas fixed-stuff, su uso es como de información de control para la trama. Los restantes 756 bytes en las restantes 84 columnas están designadas como la capacidad de payload o de información del STS-1. Por otra parte, un SPE STS-1 puede comenzar en cualquier sitio de la parte de envelope del SPE. Típicamente comienza en una trama STS-1 y finaliza en la próxima.

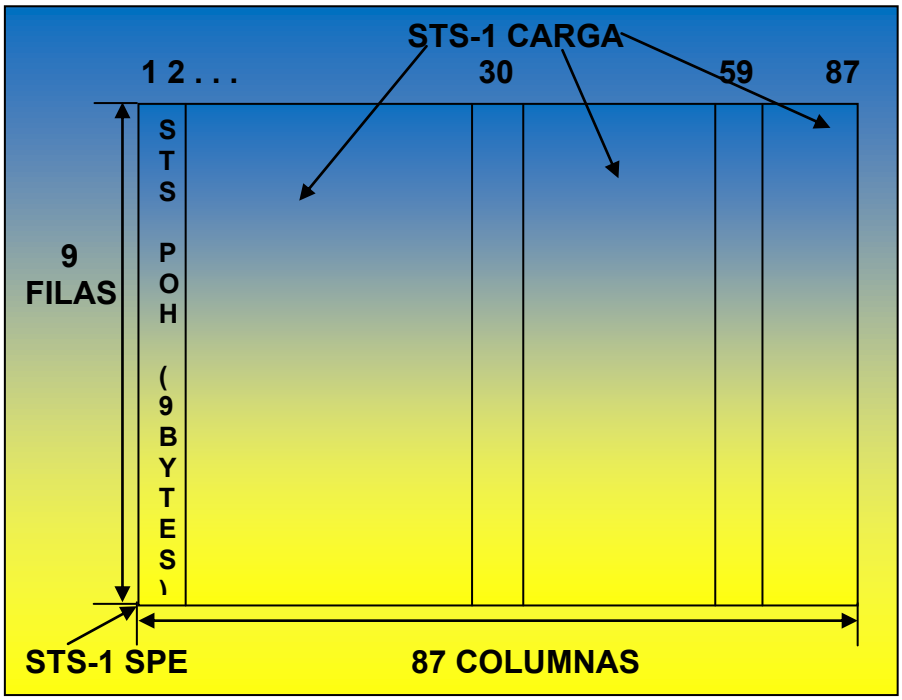


Figura 154 Ejemplo de un SPE STS-1

3.4.3.2.3 ESTRUCTURA DE LA TRAMA STS-N

Un STS-N es una secuencia específica de N * 810 bytes. El STS-N esta formado intercalando módulos de STS-1, figura 155. El transport overhead de los módulos individuales de STS-1 son alineados antes de ser intercalados, sin embargo los SPE asociados no, ya que como se señaló anteriormente, los STS-1 tienen apuntadores que le indican la localización de el SPE.

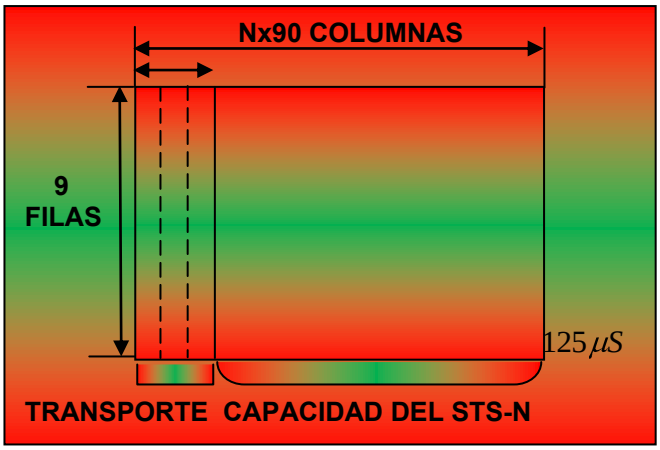


Figura 155 Ejemplo de un STS-N

3.4.3.2.4 OVERHEADS EN SONET

SONET provee información sustancial de overhead, permitiendo un multiplexing sencillo y una gran capacidad de operaciones, administración, mantenimiento y provisionamiento (OAM&P). La información de overhead tiene varias capas, las cuales son mostradas en la figura 156. El **path level overhead** es llevado de punto a punto; este es agregado a las señales DS-1 cuando éstas son mapeadas en VT's y para los payloads de STS-1 que viajen punto a punto. **Line overhead** es para las señales STS-N entre multiplexores STS-N. **Section overhead** es usada para la comunicación entre elementos de redes adyacentes tales como regeneradores.

Section Overhead Contiene: 9 bytes del transport overhead. Este overhead soporta funciones tales como las siguientes:

- Monitoreo de ejecución (señales STS-N).
- Canal de comunicación de datos para transportar información de OAM&P.
- Framing.

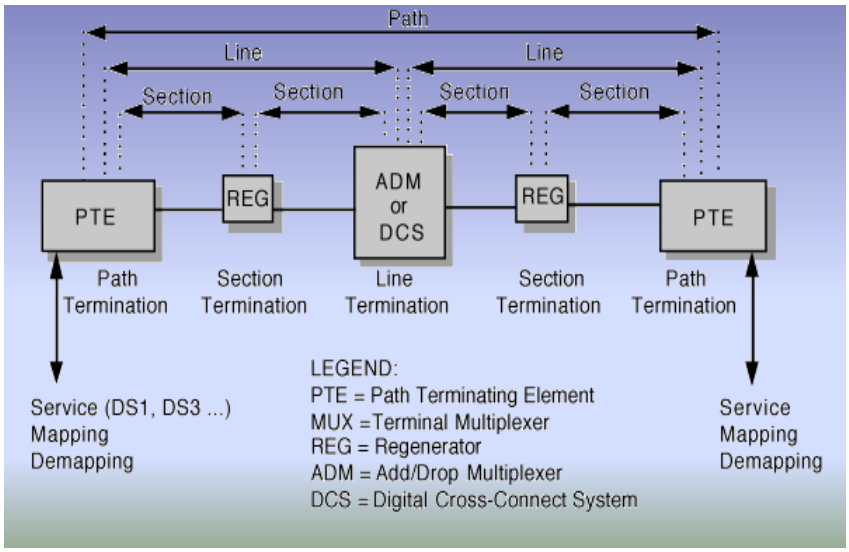


Figura 156 Ejemplo de un STS-N

La tabla 23 muestra section overhead byte por byte

	1	2	3	
1	A1	A2	J0/Z0	J1
2	B1	E1	F1	B3
3	D1	D2	D3	C2
4	H1	H2	H3	H4
5	B2	K1	K2	G1
6	D4	D5	D6	F2
7	D7	D8	D9	Z3
8	D10	D11	D12	Z4
9	S1/Z1	MO ó M1/Z2	E2	Z5

Tabla 23

Line Overhead Contiene 18 bytes de overhead. Este soporta funciones tales como las siguientes:

- Localizar el SPE en al trama.
- Multiplexar y Concatenar señales.

- Monitorear la ejecución.
- Automática protección de switching.
- Mantenimiento de la Línea.

Line Overhead es encontrado en las filas 4-9 de la Tabla24. El significado de sus bytes son:
El **STS POH** contiene 9 POH bytes distribuidos por cada 125 microsegundos de un paquete SONET, empezando en el primer byte del **STS SPE**. El STS POH permite la comunicación entre los puntos de creación del STS SPE y el punto de demultiplexaje o desensamblaje. Este overhead permite las siguientes funciones:

- Monitoreo de desempeño **(performance monitoring)** del STS SPE.
- Estado del STS SPE.
- Estado del **path**.

	1	2	3	
1	A1	A2	J0/Z0	J1
2	B1	E1	F1	B3
3	D1	D2	D3	C2
4	H1	H2	H3	H4
5	B2	K1	K2	G1
6	D4	D5	D6	F2
7	D7	D8	D9	Z3
8	D10	D11	D12	Z4
9	S1/Z1	MO ó M1/Z2	E2	Z5

Tabla 24 POH

VT Path Overhead

El **VT POH**, figura 157 contiene cuatro POH bytes por cada VT SPE comenzando en el primer byte del VT SPE. El VT POH provee la comunicación entre el punto de creación de un VT SPE y el punto de su desensamblaje. Este overhead permite las siguientes funciones:

- Monitoreo de desempeño (performance monitoring) del VT SPE.
- Estado del VT SPE.
- Estado del **path**

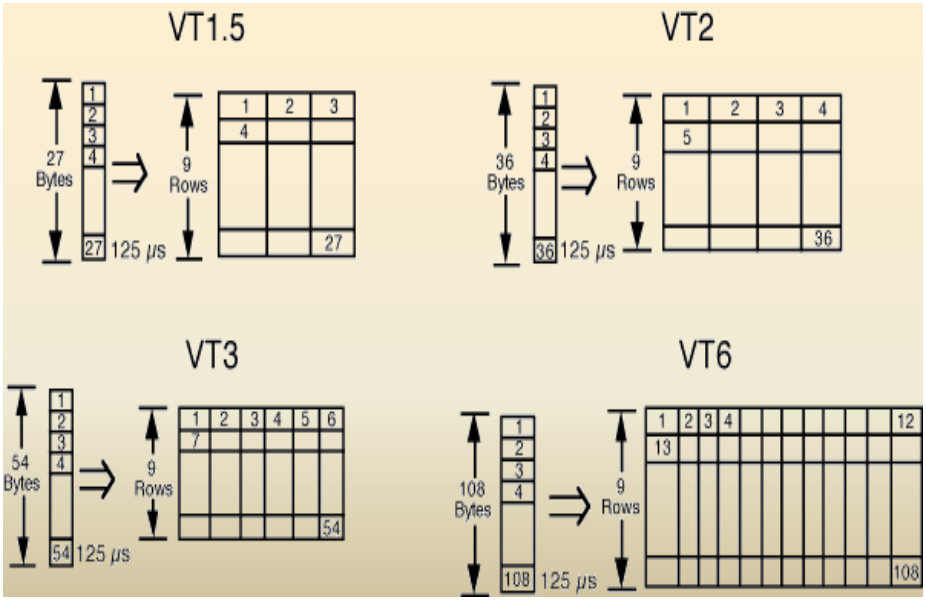


Figura 157 VT POH

Cuatro bytes (V5, J2, Z6 y Z7) están destinados para el VT POH. El primer byte del VT SPE es el V5, mientras que los bytes J2, Z6 y Z7 ocupan las correspondientes posiciones por los 125 microsegundos de la trama. El byte V5 provee la misma función para los *VT* **paths** como los bytes B3, C2 y G1 para los **STS paths (chequeo de errores y estatus del path)**.

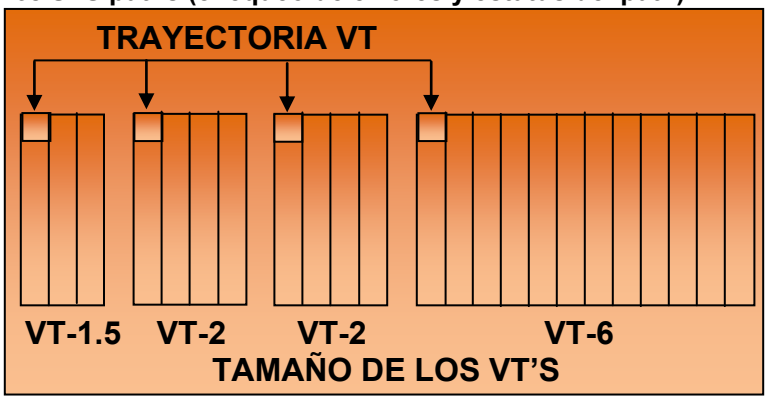


Figura 158 VT POH

SONET usa un concepto llamado **pointers** o apuntadores para compensar las variaciones de frecuencia y fase de las tramas. Los apuntadores permiten un transporte transparente del payload o SPE del STS a través de entes plesiochronous (entre nodos separados con relojes separados que poseen siempre el mismo tiempo). El uso de apuntadores permite controlar los retardos y la perdida de datos asociados con el uso de (tramas mayores a 125 microsegundos) **buffers** para la sincronización. Estos apuntadores permiten una manera simple de alinear flexible y dinámicamente los desfases de los STS o los VT payloads, esto a su vez nos ayuda a controlar la eliminación, inserción e interconexión de payloads en la red. El **wander** y el **jitter** se minimizan en muy buena parte con los apuntadores. La figura 159 nos muestra un apuntador STS-1 (H1 y H2 bytes), el cual permite que el SPE sea separado del **transport overhead (overhead de transporte)**. El apuntador es un simple valor de **offset** que apunta hacia donde el SPE comienza. La figura 159 también nos muestra el típico caso en donde los SPE se cortan entre tramas de 125 microsegundos. Si existe alguna variación en la frecuencia o en la fase el apuntador debe ser incrementado o decrementado.

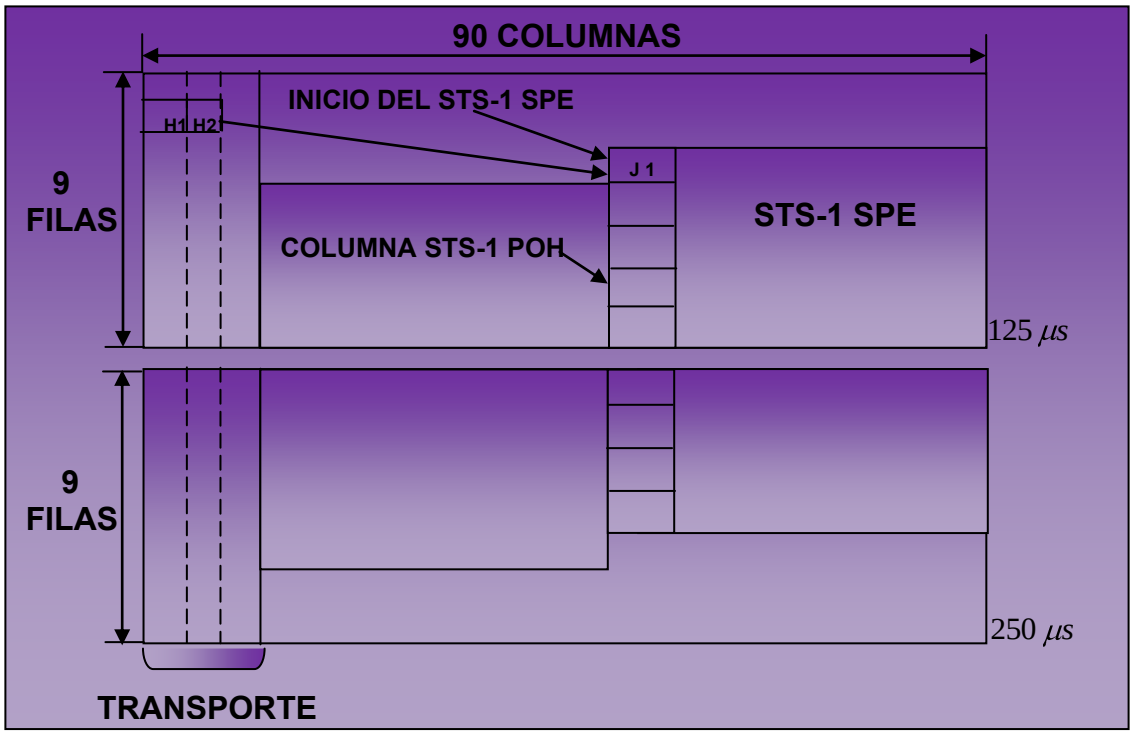


Figura 159 Pointers

Cuando hay una diferencia en la fase o la frecuencia, el valor del apuntador es ajustado. Para hacer esto, un proceso denominado **Byte Stuffing** es usado. En otras palabras, el SPE payload pointer indica en donde empieza un VT y el proceso de **stuffing** permite dinámicamente alinearlo en caso de que se corte en tiempo. Los tipos de **Stuffing** utilizados son:

- **Positive Stuffing**.
- **Negative Stuffing**

Positive Stuffing

Cuando el **frame rate** del SPE es muy lento en relación con el **frame rate** del STS-1, los bits 7, 9, 11, 13 y 15 del apuntador son invertidos en una trama, permitiendo así mayoría de bits de desplazamiento para que el receptor sepa que hay un desfase. Esto bits son conocidos como los I-bits o bits incrementales. Periódicamente, cuando el SPE esta un **byte off - desfasado**, estos bits son invertidos, indicando que un **stuffing positivo** esta ocurriendo. De esta manera un byte adicional es insertado en el SPE del STS, permitiendo la alineación del SPE con respecto al STS con miras hacia el pasado. A este proceso se le conoce como **positive stuffing** figura 160. El byte agregado al SPE es un byte de **no información**, este byte esta colocado después del campo H3. La próxima trama de Sonet que se va a enviar tiene el apuntador incrementado en uno, y así sucesivamente con los apuntadores siguientes.

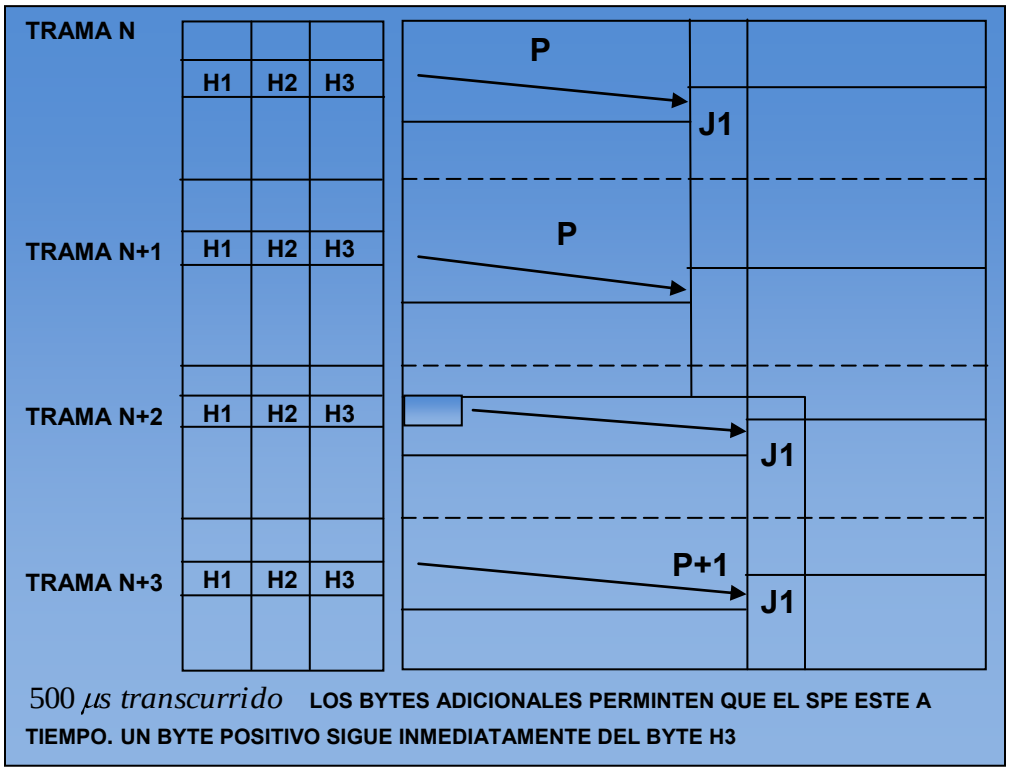


Figura 160 Positive Stuffing

Negative Stuffing

Cuando el **frame rate** del SPE es muy rápido en relación con el **frame rate** del STS-1, los bits 8, 10, 12, 14 y 16 del apuntador son invertidos en una trama, permitiendo así mayoría de bits de desplazamiento para que el receptor sepa que hay un desfase. Esto bits son conocidos como los D-bits o bits decrementales. Periódicamente, cuando el SPE esta un **byte off - desfasado**, estos bits son invertidos, indicando que un "**stuffing negativo**" esta ocurriendo. Dado que la alineación del SPE avanza en el tiempo más rápido que el STS, el SPE debería ser colocado hacia futuro. De esta manera se toma un byte del SPE y se agrega **stuffing** en el campo H3 del **line overhead** de esta manera se avanza un byte en el tiempo. La próxima trama de SONET que se va a enviar tiene el apuntador decrementado en uno, y así estarán los apuntadores sucesivos.

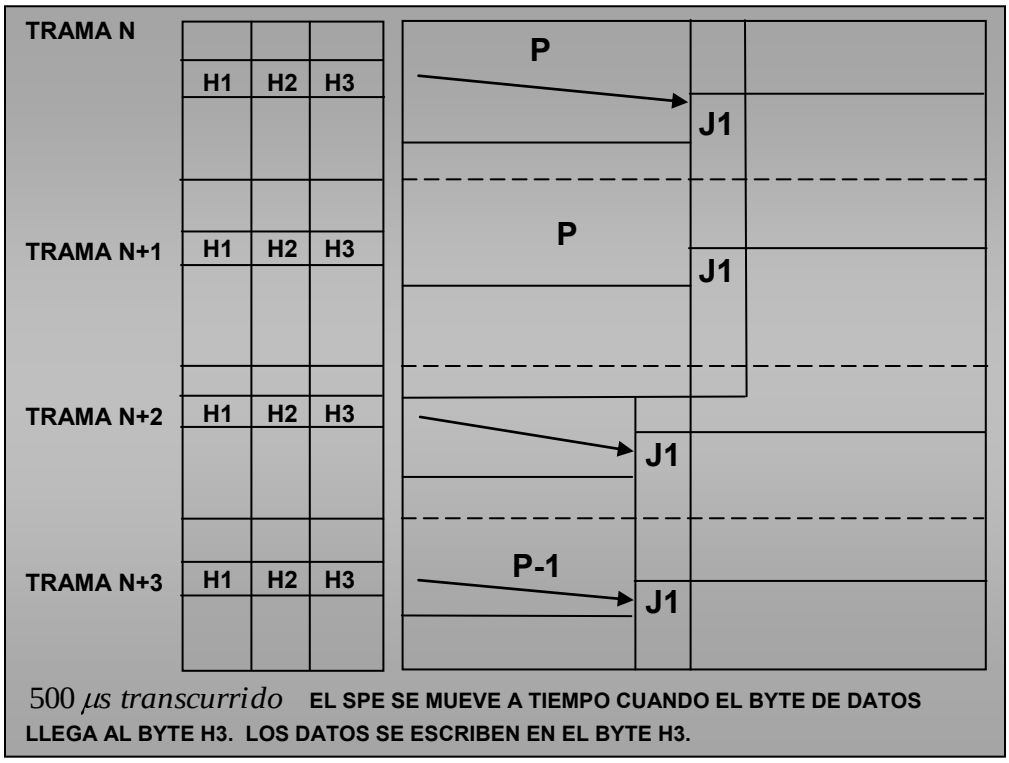


Figura 161 Negative Stuffing

Tradicionalmente los sistemas de transmisión eran asíncronos. En este tipo de transmisión cada máquina tiene su propio reloj por lo que la tasa de datos de cada señal varía. A esto se le une la dificultad de saber exactamente donde esta la información que se necesita, es decir, ¿como saber exactamente donde esta cada uno de los campos en la información que se transmite?. Es por ello que para estas transmisiones se requirió la implementación de técnicas como bit-stuffing para procesar adecuadamente la transmisión, pero su implementación agrega complejidad a los equipos necesarios para manejarlas. Por otro lado las transmisiones sincronas como lo es SONET, logran tener una tasa de bits constante en sus transmisiones, lo cual simplifica el trabajo de sus equipos ya que no necesitan técnicas como bit-stuffing. Para implementar la sincronización Sonet y otras transmisiones sincronas utilizan un esquema de sincronización jerárquica, es decir, se establecen relaciones master-slaves entre los componentes de la red, donde cada nodo master envía señales a los slaves para que se sincronicen. En SONET, la señal de sincronización enviada por una terminal puede derivarse de **un Building Integrated Timing Supply (BITS)** usada por switches y otros equipos, es por ello que estos generalmente son usados como masters.

Sonet provee muchas más capacidades que los sistemas asíncronos existentes. Entre estos beneficios podemos mencionar los siguientes:

CONFIGURACION MULTIPUNTO:

La mayoría de los sistemas asíncronos existentes utilizan únicamente configuraciones punto a punto, mientras Sonet soporta configuraciones multipunto o de hub. Un hub es un sitio que funciona como intermediario, desde el cual el tráfico es distribuido a tres o más **spurs**. **Hubbing** reduce los requerimientos de multiplexaje y desmultiplexaje ***back-to-back***, y permite el **grooming**. Además, una implementación multipunto permite interconexiones entre dos fibras y **mid-span-meet**, permitiendo a los proveedores de red y a sus clientes optimizar el uso de su infraestructura Sonet.

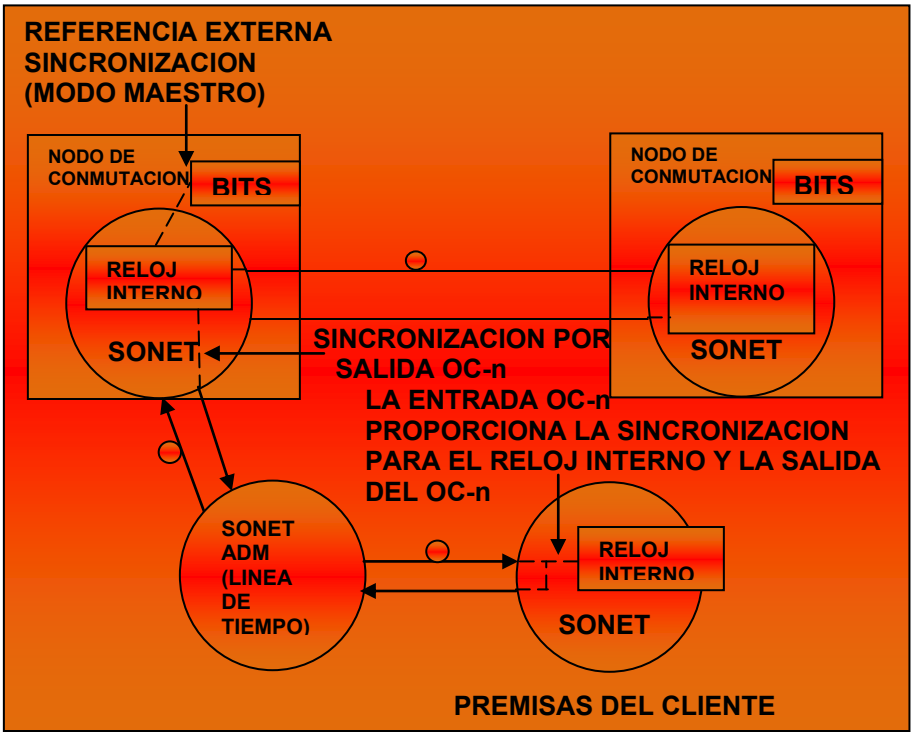


Figura 162 Sincronización de relojes

GROOMING.-Es la consolidación o segregación de tráfico para el uso más eficiente de los recursos. Consolidación significa combinar tráfico de diferentes localidades en una sola. Por otro lado, la segregación es la separación del tráfico. Es posible hacer grooming sobre sistemas asíncronos, sin embargo, esto requiere configuraciones **back-to-back** muy costosas, además de paneles **DSX (multiplexores de señales digitales)** u otros conectores electrónicos. Por otra parte, un sistema SONET puede segregar información en un STS-1 o un VT enviando los datos a los nodos apropiados.

REDUCCION DE MULTIPLEXAJE *BACK-TO-BACK*:

Antes existían multiplexores separados **M13 (DS-1 a DS-3)** y terminales **FOTS (Fiber Optic Terminal System)** para transformar las señales **DS-1 a DS-2**, las **DS-2 a DS-3**, y las **DS-3** a línea óptica. Ahora con SONET, las señales DS-1 pueden ser introducidas en un grupo de VT's de un trama STS-1, es decir, de una señal DS-1 llegamos directamente a línea óptica. En el formato asíncrono existente, se debe tener cuidado cuando se crean los circuitos con el fin de evitar multiplexaje y demultiplexaje excesivo (y su gran costo asociado) en cada momento que una señal DS-1 es procesada. Con SONET, DS-1s pueden ser multiplexadas directamente a una línea óptica. Además, gracias a la sincronización una señal óptica no tiene que ser desmultiplexada, sino únicamente las señales que están en VT's o en los STS's que necesitan ser accesadas.

REDUCE EL CABLEADO Y ELIMINA LOS PANELES DSX

Los sistemas asíncronos son dominados por terminales back-to-back, porque la arquitectura FOTS asíncrona es ineficiente para las redes que no son punto a punto. Para transportar una señal desde un extremo a otro es usado multiplexaje y desmultiplexaje excesivo, ya que los datos atraviesan muchos paneles DSX1 conectados a DSX3. Además de los grandes costos asociados a los paneles, cableado, mano de obra e inconvenientes del decremento de espacio en el piso, se tiene también el problema de los racks congestionados de cables. El sistema SONET permite configuración de hub, reduciendo la necesidad de terminales back-to-back. Además, el grooming es hecho electrónicamente, y de esta forma los paneles DSX son únicamente usados cuando se requiere una interfaz con un equipo asíncrono.

OPTIMIZA OAM&P (Operations, Administrations, Maintenance and Provisioning):

Es una de las labores principales de un proveedor de red. Debido al crecimiento continuo de las redes y a la gran variedad de fabricantes y tipos de equipos ha surgido la necesidad por parte de los proveedores de tener una administración centralizada. Para esto la organización TMN (**Telecommunication Management Network Standards Committee)** estableció una arquitectura OAM&P que satisface esta necesidad. Sonet mejora el manejo de la red al proveer funcionalidad extra para OAM&P en el overhead de transmisión de sus paquetes para simular canales de comunicación entre los controladores o monitores de la red y los nodos de la misma y comunicación entre los nodos. Estos canales de comunicación también son llamados canales de datos de OAM&P. Sonet permite *OAM&P* integrado. Se puede hacer mantenimiento centralizado reduciendo de esta forma los viajes del personal de mantenimiento, lo cual se traduce en ahorros. Además, mucha información de overhead es añadida en la trama Sonet para permitir la resolución rápida de problemas y detección de fallas antes de que estas degraden el **performance** de la red.

INTERCONEXION OPTICA:

Debido a los diferentes formatos ópticos entre los vendedores de productos asíncronos, no es posible conectar una terminal de fibra óptica de un fabricante con otro. Por ejemplo, un fabricante puede dar 570Mbps mientras otro da sólo 565Mbps. Entre las mayores ventajas de SONET esta la de permitir **mid-span-meet** con compatibilidad para varios fabricantes. Hoy día, los estándares de SONET contienen definición para interfaces a nivel físico. Estos estándares, determinan la taza de línea óptica, longitud de la onda, niveles de poder, forma de pulso, y codificado. Los estándares actuales, también definen la estructura de la trama, overhead y mapeos del payload. SONET permite conexión óptica entre proveedores de red sin tomar en cuenta quien hizo el equipo. Los proveedores de red pueden comprar un equipo de un vendedor, e interfaces convenientes para otro vendedor de equipo SONET en los sitios del cliente. Los usuarios pueden ahora obtener el equipo de fibra de su escogencia y usarlo para comunicarse con el equipo de fibra de su proveedor sin preocuparse por problemas de compatibilidad.

TRANSPORTE PARA NUEVOS SERVICIOS COMO ATM (Asynchronous Transfer Mode)

Una red basada en ATM es **bandwidth-transparent**, lo cual permite el manejo dinámico de varios tipos de servicios a diferentes **data-rates**. SONET, gracias a su arquitectura independiente a los servicios, provee soporte para redes ATM.

Remote Provisioning And Reconfiguration

Sonet permite la reconfiguración dinámica de la red remotamente. Esto es habilitar o deshabilitar, desde una conexión remota, circuitos de la red para aislar, bloquear o redireccionar tráfico debido a problemas, peticiones o políticas de servicio de los proveedores. Por ejemplo se ofrece servicio de red a un usuario durante el día pero en la noche es bloqueado. Esta ventaja de Sonet permite la instalación rápida de circuitos para prestar ciertos servicios sin necesidad de gastos en traslado de personal para realizar estas labores, haciendo el sistema más adaptable a cambios rápidos y a diferentes situaciones.

Enhaced Performance Monitoring

El overhead de Sonet esta organizado en tres capas o layers, el **section overhead** es el que es pasado entre dos elementos contiguos en la red, el **line overhead** es el que es pasado entre dos hubs de Sonet que mantienen una comunicación por un canal donde viajan muchos STS-1 multiplexados, y el **path overhead** que es el que se mantiene a lo largo de todo el camino en la red desde el elemento o host de origen hasta el destino. El overhead provee suficiente información para el monitoreo del desempeño y aislar fallas en la red. En caso de una falla, una señal que indica alarma **(AIS)** es enviada desde donde la falla es detectada hacia el destino del mensaje original, esto para indicar al resto de los elementos de la red en el camino que una falla ya fue

detectada en la transmisión y que ellos no deben enviar otra señal de alarma. En este caso el elemento que envió originalmente el mensaje podrá no enterarse de la falla. En una red Sonet al enviar un mensaje desde A hasta B, si ocurre una falla, esta es detectada por un elemento intermedio entre A y B en la red, como por ejemplo un hub, que envía una señal **(AIS)** hacia B igual como ocurre en redes no Sonet, la diferencia en este caso es que B al recibir la alarma envía otra señal de alarma de vuelta hacia A llamada **(Yellow Alarm),** además el hub que detectó la falla al principio también envía otra señal hacia A para notificar de la falla que ocurrió al enviar un mensaje a B, esta ultima señal se llama **FERF (Far End Received Fail Signal).** De esta manera A se entera de la falla, y se hace más fácil la detección de la misma.

Telecommunication Management Network

Esta arquitectura provee de un **OS** para comunicarse con la red y viceversa. El OS es un software que es capaz de obtener información de la red, como alarmas, estadísticas, entre otros, para realizar monitoreo y tareas de administración. El OS puede comunicarse directamente con elementos de la red directamente o a través de dispositivos de mediación o **mediation devices.** Los mediation devices pueden realizar varias funciones como consolidación de enlaces de comunicación con varios elementos de la red, conversión de protocolos y manejo de información para el monitoreo de rendimiento.

Terminal Multiplexer

Este es un equipo terminal que funciona para multiplexar otros tipos de señales digitales sobre una red Sonet. Se encarga de concentrar cualquier tipo de señales como DS1, DS3, STS-3, etc. sobre tramas STS-N. La red Sonet más sencilla esta compuesta por dos de estos elementos conectados por fibra.

Regenerador

Este dispositivo es usado para regenerar las señales atenuadas que viajen largas distancias a través de la fibra.

Add/Drop Multiplexer

Este es un dispositivo intermedio que permite multiplexar/desmultiplexar señales digitales que viajan a través de la fibra sin necesidad de perturbar las demás señales. Dado que Sonet esta basado en un tecnología síncrona a este dispositivo le es posible saber en que momento sacar/meter las señales que le interesan de las tramas STS-N que viajan a través de este. Este dispositivo posee una gran cantidad de usos, puede ser usado como dispositivo intermedio para consolidar señales de dos sitios distintos, puede ser usado para implementar redes tipo anillo, también para implementar distribuciones multinodo haciendo uso de la propiedad **drop & repeat** que permite tomar las señales solicitadas sin sacarlas de la trama.

Broadband Digital Cross-Connects

Este dispositivo tiene la capacidad de interconectar una gran cantidad señales, funciona como un **switch** de señales STS-1 y es por ello que es usado para el **grooming** (consolidación y segregación) dentro de la red. Este dispositivo es ampliamente usado para implementar topologías de tipo Hub.

Wideband Digital Cross-Connects

Funciona de manera idéntica al anterior, la única diferencia es que realiza el **switching** a nivel de VT, mientras que el anterior lo realiza a nivel de STS-1.

Digital Loop Carrier

Este dispositivo fue creado para consolidar grandes cantidades de señales de bajo ancho de banda (como señales de teléfono) y convertirlos en VT's que luego pueden ser tomados por dispositivos como los Terminal Multiplexer para multiplexarlos en paquetes STS-N. Este aparato es ampliamente usado para consolidar líneas POTS (líneas de teléfonos) para ser transmitidas a través de Sonet.

Punto - Punto

Esta configuración es la más sencilla de todas y permite interconectar dos puntos rápida y fácilmente, con la desventaja que no posee la posibilidad de crecimiento como si la tienen topologías como la de HUB. La forma en que se monta una conexión punto-punto Sonet es a través del uso de dos equipos PTE (**Path Terminating Equipment**, como lo son los **Terminal Multiplexer**) unidos a través de una troncal de fibra y si es necesario se montan regeneradores en caso de que las distancias sean muy largas.

Punto - Multipunto

Esta configuración permite distribuir señales que se generan en un sólo punto hacia consumidores ubicados en distintos sitios, puede ser usada para distribuciones de broadcast de televisión. La forma en que se logra montar este tipo de topología es a través del uso de equipos ADM (Add/Drop Multiplexer) que poseen la capacidad de drop&repeat permitiendo aquellos puntos intermedios tomar las señales que necesitan sin perturbarlas para que se continúe con la distribución a los siguientes puntos.

Topología tipo HUB

Esta configuración es la más usada, esta compuesta por un switch central que permite crear nuevos circuitos entre distintos puntos, este tipo de configuración es la más flexible, ya que permite el fácil crecimiento de la red. La forma de montar este tipo de topología es a través del uso de un **DCS** (**Digital Crossconnect Switch** que podría ser un **Broadband Crossconnect Switch** o un **Wideband Crossconnect Switch**) al cual le llegan los distintos MUX (Multiplexores) de los distintos puntos que necesitan circuitos de la red.

Topología tipo Anillo

Este tipo de configuración es la más usada para la interconexión de puntos encerrados en un mismo medio geográfico, como podrían ser edificios dentro de un campus universitario. Para lograr este tipo de configuración sólo es necesario el uso de equipos ADM.

3.5 FRAME RELAY

3.5.1 INTRODUCCION

Frame Relay es un protocolo de transmisión de paquetes de datos en ráfagas de alta velocidad a través de una red digital fragmentados en unidades de transmisión llamadas trama. Frame Relay requiere una conexión exclusiva durante el periodo de transmisión. Esto no es valido para transmisiones de video y audio ya que requieren un flujo constante de transmisiones. Frame Relay es una tecnología de paquete-rápido ya que el chequeo de errores no ocurre en ningún nodo de la transmisión. Los extremos son los responsables del chequeo de errores. (Sin embargo debido a que los errores en redes digitales son extremadamente menos frecuentes en comparación con las redes analógicas). Frame Relay no es sólo por el ahorro de costos: también puede ser implantada por una mejor calidad de servicio. Una red Frame Relay puede ser altamente viable por poder escoger una nueva ruta en el caso del fallo de la línea y, por con siguiente un rico patrón de interconexión, Frame Relay puede reducir el número de saltos entre nodos intermedios dando tiempos de respuesta imprevistos.

Frame Relay transmite paquetes en el nivel de enlace del modelo OSI antes que en el nivel de red. Distintamente a que un paquete, que es de tamaño fijo, una trama 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 1.544Mbps, 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. Las redes y el equipo de cómputo actuales tienen la potencia para trabajar con velocidades mucho más rápidas y transferir grandes cantidades de datos. Con la complejidad de las redes actuales, la administración puede resultar más compleja si no tiene las herramientas adecuadas. Cada ambiente es una combinación única de equipos de diferentes fabricantes. Frame Relay es un método relativamente nuevo para redes de área amplia que está ganando gran popularidad. Utiliza tecnología de conmutación de paquetes, similar a la X.25, pero es más eficiente y puede hacer que su red sea más rápida, sencilla y menos costosa.

Al igual que la X.25, Frame Relay es un protocolo de conmutación de paquetes. Pero su proceso es fluido; es decir, un formato de red más rápido y eficaz. Una red Frame Relay no realiza detección de errores, lo que da como resultado una baja considerable de sobrecarga y un procesamiento más rápido que con X.25. Frame Relay es también independiente al protocolo, acepta datos de muchos protocolos diferentes, que son encapsulados por los equipos Frame Relay, no por la red. Los dispositivos inteligentes de red conectados a una red Frame Relay son responsables de la corrección de errores y el formateado de tramas. El tiempo de procesamiento es más rápido por lo que la transmisión de datos es más eficiente. Además, Frame Relay es totalmente digital, reduciendo la posibilidad de error y ofreciendo excelentes velocidades de transmisión. La Frame Relay típica trabaja de 56 ó 64Kbps a 1.544 ó 2.048Mbps.

Frame Relay envía información en paquetes, llamados tramas a través de una red compartida Frame Relay. Cada paquete contiene toda la información necesaria para enviar la información al destino correcto. Por lo que, cada punto terminal puede comunicarse con muchos destinos desde un sólo enlace de acceso a la red. En lugar de tener asignado una cantidad fija de ancho de banda, los servicios Frame Relay ofrecen una **Tasa Comprometida de Información (CIR)** a la cual los datos son transmitidos. Pero si el tráfico y el contrato de su servicio lo permite, los datos pueden ir a una velocidad más rápida de la que ha sido contratada. Frame Relay con su bajo umbral, es perfecto para las complejas redes actuales. Se pueden enviar múltiples conexiones lógicas sobre una sola conexión física, reduciendo los costos de interconexión de redes. Reduciendo la cantidad de procesamiento necesaria, mejorará el desempeño y el tiempo de respuesta. Debido a que Frame Relay utiliza un sólo protocolo en la capa de enlace, sus equipos únicamente necesitarán cambios en el software o modificaciones sencillas de hardware, por lo que no tendrá que invertir gran cantidad de dinero para actualizar su sistema. Como es independiente al protocolo, puede procesar tráfico de diferentes protocolos de red, tales como IP, IPX y SNA. También es una opción

ideal para conectar WAN que tengan tráfico impredecible o muy pesado. Típicamente, estas aplicaciones incluyen traspaso de datos, CAD/CAM, y servidor-cliente.

Frame Relay ofrece las ventajas de interconexión de WAN. En el pasado, la configuración de las WAN requerían la utilización de líneas privadas o circuitos de conmutación sobre líneas punto a punto. Para realizar conexiones WAN a WAN ya no es necesario utilizar líneas punto a punto, se puede realizar a través de Frame Relay, esto reduce los costos. Frame Relay es una tecnología de conmutación rápida de tramas, basada en estándares internacionales, que puede utilizarse como un protocolo de transporte y como un protocolo de acceso en redes públicas o privadas proporcionando servicios de comunicaciones.

Historia de Frame Relay

La convergencia de la informática y las telecomunicaciones está siendo una realidad desde hace tiempo. Las nuevas aplicaciones hacen uso exhaustivo de gráficos y necesitan comunicaciones de alta velocidad con otros ordenadores conectados a su misma red LAN, e incluso a redes LAN geográficamente dispersas. Frame Relay surgió para satisfacer estos requisitos. Ahora, el mercado demanda un mayor ahorro en los costos de comunicaciones mediante la integración de tráfico de voz y datos. Frame Relay ha evolucionado, proporcionando la integración en una única línea de los distintos tipos de tráfico de datos y voz y su transporte por una única red que responde a las siguientes necesidades:

- Alta velocidad y bajo retardo.
- Soporte eficiente para tráficos a ráfagas.
- Flexibilidad.
- Eficiencia.
- Buena relación costo-prestaciones.
- Transporte integrado de distintos protocolos de voz y datos.
- Conectividad "todos con todos".
- Simplicidad en la gestión.
- Interfaces estándares

En 1988, el ITU-TS (antiguo CCITT) estableció un estándar (I.122), que describía la multiplexación de circuitos virtuales en el nivel 2, conocido como el nivel de trama. Esta recomendación fue denominada Frame Relay. ANSI tomó lo anterior como punto de partida y comenzó a definir estándares que iban siendo también adoptados por el ITU-TSS (CCITT). Condiciones básicas que justifican la utilización de frame Relay:

- La línea de transmisión debe ser buena. Frame Relay sólo funcionará eficientemente si la tasa de error del medio físico es baja.
- Los nodos conectados a Frame Relay no deben ser terminales tontas, sino que correrán sus propios protocolos para control de flujo, recuperación de errores y envío de asentamientos.
- Los estándares ANSI T1.606 y T1.618 definen los procedimientos núcleo de Frame Relay estos procedimientos son usados para manejar las tramas de datos de usuario en un nodo de red Frame Relay. El estándar ANSI T1.617 define los procedimientos de mantenimiento para las redes Frame Relay. Estos especifican los tipos de mensajes intercambiados entre una terminal de usuario y un nodo a través del cual él se conecta a la red.

Antes de que surgiera el estándar ANSI T1.617 anexo D, un consorcio de compañías definió un mecanismo para el manejo de los PVC Frame Relay, llamado **LMI (Link Managament Interface)**. El LMI define una funcionalidad similar a la definida más tarde por el estándar ANSI y actualmente es un estándar ampliamente soportado en las redes Frame Relay existentes.

3.5.2 CIRCUITOS VIRTUALES

Un **circuito virtual permanente (PVC)** es una conexión dedicada a través de una red Frame Relay compartida, sustituyendo una línea punto a punto. Se necesita un PVC para cada

emplazamiento de la red, al igual que una línea privada, el ancho de banda es compartido entre múltiples usuarios. Cada emplazamiento podrá comunicarse con otros sin necesidad de tener múltiples líneas dedicadas. Los PVC funcionan a través de un **Local Management Interface (LMI)**, que proporciona los procedimientos de control que se realizan de tres formas: verificación de integridad del enlace iniciado por el dispositivo del usuario, informe del estado de la red, dando detalles de todos los PVC, y notificación de red si ha cambiado el estado de cualquier PVC, de activo a inactivo, o viceversa. Las **Conexiones de enlace de Datos (DLC)** son preconfigurados en los PVC's en ambos lados de la conexión. **El identificador DLC (DLCI)** se utiliza como una dirección lógica para el multiplexado en la capa de trama. Frame Relay ofrece comunicación de la capa de enlaces de datos orientada a la conexión esto significa que hay una comunicación definida entre cada par de dispositivos y que estas conexiones están asociadas con el identificador de conexión. Este servicio se implementa por medio de un **circuito virtual Frame Relay**, que es una conexión lógica creada entre dos DTE a través de una PSN (Red de Comunicación de Paquetes) de Frame Relay. Los circuitos Virtuales ofrecen una trayectoria de comunicación bidireccional de un dispositivo DTE a otro y se identifica de manera única por medio del **DLCI (Identificador de Conexiones de Enlace de Datos)**. Se puede multiplexar una gran cantidad de circuitos virtuales en un sólo circuito físico para transmitirlos a través de la red. Con frecuencia esta característica permite conectar múltiples dispositivos DTE con menos equipo y una red compleja. Un circuito virtual puede pasar por cualquier cantidad de dispositivos intermedios DCE (Switches) ubicados en la red Frame Relay PSN. Los circuitos virtuales Frame Relay caen dentro de dos categorías: **SVC (Circuitos Virtuales Conmutados)** y **PVC (Circuitos Virtuales Permanentes)**. Ya que Frame Relay no proporciona conversión de protocolo y detección/corrección de errores, los dispositivos de usuario final tienen que ser inteligentes. Normalmente, podrá accesar al servicio Frame-Relay a través de dispositivos Frame-Relay, **ensamblador/ desensamblador (FRAD)**, ruteador, bridges o conmutadores.

Ruteadores.

Los routers frame traducen los protocolos existentes para comunicaciones de datos sobre una red Frame Relay, luego dirigen los datos a través de la red a otro router frame o a otro dispositivo compatible Frame Relay. Los routers frame pueden manejar muchos tipos de protocolos, incluyendo protocolos de Red. Se utilizan en entornos que requieren velocidades de acceso a red E1 o inferiores. Cada router soporta uno de las muchas interfaces de datos físicos y puede proporcionar varios puertos de usuario.

Bridges, routers y FRAD.

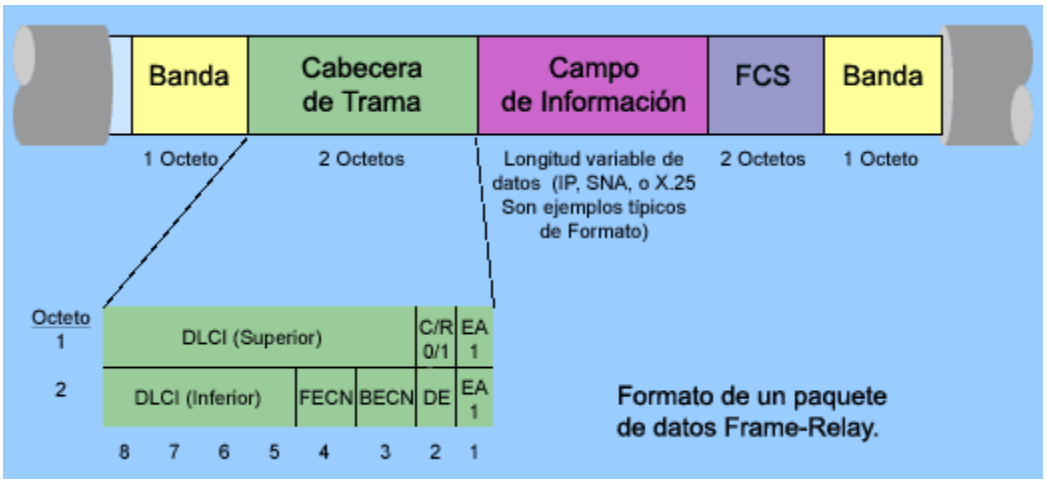
También puede utilizar bridges, ruteadores o FRAD. Estos dispositivos agregan y convierten datos en los paquetes Frame Relay. Los bridges son fáciles de configurar y mantener, normalmente conectan una sucursal a un hub. Los ruteadores pueden manejar tráfico desde otros protocolos WAN, redirigir una conexión, si falla una línea, o proporcionar soporte para control de flujo y control de congestión. Los FRAD formatean los datos salientes para adaptarlos a los paquetes que necesita una red Frame Relay, algunos incluso funcionan como ruteadores. Trabajan bien en aplicaciones donde un emplazamiento ya tenga bridges y routers o cuando se envíe tráfico desde el mainframe sobre la red Frame Relay.

Compresión.-En febrero de 1998, la ITU ratificó una serie de estándares para transmisión simultánea de voz, datos y video sobre IP. Conocida como H.323, este estándar incorpora los nuevos criterios adoptados, tales como G.729 y G.723. Estos estándares especifican algoritmos para la compresión de tráfico de voz (el cual viaja normalmente a la velocidad de 64Kbps bajando hasta 8Kbps para Voz Sobre Frame Relay (VOFR).
Empaquetamiento.-El Foro Frame Relay se ha reunido recientemente para ratificar dos nuevos procedimientos para VOFR. El FRF.11 especifica un proceso para conexión de PBX sobre Frame Relay para llevar tráfico de voz, datos y fax sobre una PVC. El FRF.12 dirige el empaquetamiento y (consecuentemente) su priorización. Estandariza un procedimiento para que Frame Relay divida las tramas grandes en otras más pequeñas. Esta técnica le ayudará a aliviar los problemas de

congestión en la red, en picos de tráfico, cuando grandes bloques de datos se alinien en la cola antes que el tráfico de voz, el cual es muy sensible al tiempo. En lugar de un protocolo **Quality of Service (QoS)**, como el que ha sido implantado por ATM, el FRF.12 confía en paquetes de menor tamaño para asegurar patrones de retardo predecibles y seguir manteniendo la calidad e integridad de las transmisiones de voz. En lugar de tener grandes paquetes de datos viajando por el circuito, se intercalan tramas más pequeñas fragmentadas con el tráfico de voz, reduciendo el jitter y el retardo, limpiando el camino para las llamadas de voz.

Prioritización.-Actualmente, el Resource Reservation Protocol (RSVP) es el único estándar en la industria específicamente diseñado para soportar la prioritización del tráfico. Mientras que el RSVP está bastante limitado, comparado con las capacidades del QoS de ATM, es un mecanismo dinámico que le ayuda a mantener el flujo de tráfico activándose automáticamente cuando en la línea están presentes paquetes de voz.

3.5.3 FORMATO DE LA TRAMA FRAME RELAY



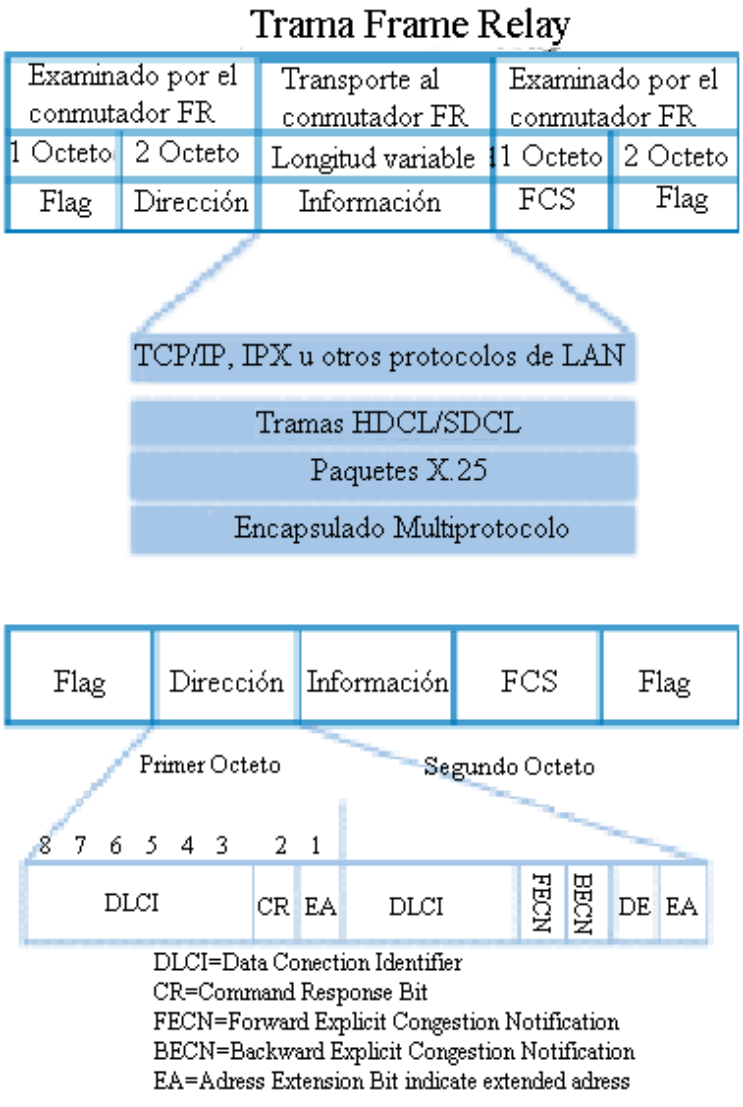


Figura 163

Flags (indicadores).-Delimitan el comienzo y la terminación de la trama. El valor de este campo es siempre el mismo y se representa con el número hexadecimal 7E o el número binario 01111110.
Direcciones: Contiene la información siguiente: el **DLCI** de 10 bits es la esencia del encabezado de Frame Relay. Este valor representa la conexión virtual entre el dispositivo DTE y el switch. Cada conexión virtual que se multiplexe en el canal físico será representada por un DLCI único. Los valores del DLCI tienen significado local solamente, lo que indica que son únicos para el canal físico en que residen; por lo tanto, los dispositivos que se encuentran en los extremos opuestos de una conexión pueden utilizar diferentes valores DLCI para hacer referencia a la misma conexión virtual, figura 164.

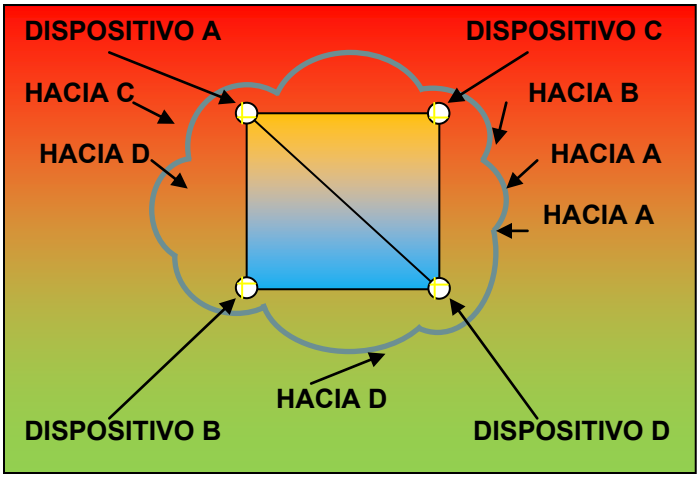


Figura 164 muestra el significado local del DLCI

EA (dirección extendida).-La EA se utiliza para indicar si el byte cuyo valor EA es 1, es el último campo de direccionamiento. Si el valor es 1, entonces se determina que este byte sea el último octeto DLCI. Aunque todas las implementaciones actuales de Frame Relay utilizan un DLCI de dos octetos, esta característica permitirá que en el futuro se utilicen DLCI's más largos. El octavo bit de cada byte del campo de direcciones de utiliza para indicar el EA.
C/R.-El C/R es el bit que sigue después del byte DLCI más significativo en el campo de direcciones. El bit C/R no está definido hasta el momento.
Control de saturación.-Este campo consta de 3 bits que controlan los mecanismos de notificación de la saturación en Frame Relay. Éstos son los bits **FECN, BECN** y **DE**, que son los últimos bits en el campo de direcciones.

- **FECN (notificación de la Saturación Explícita Hacia Adelante)**: Es un campo de un sólo bit que puede fijarse con el valor de 1 por medio de un interruptor para indicar a un dispositivo DTE terminal, como un ruteador, que ha habido saturación en la dirección de la trama del origen al destino. La ventaja principal de usar los campos FECN y BECN es la habilidad que tienen los protocolos de las capas superiores de reaccionar de manera inteligente ante estos indicadores de saturación. Hoy día, los protocolos DECnet y OSI son los únicos protocolos de las capas superiores que implementan estas características.
- **BECN (Notificación de Saturación Explicita Hacia Atrás)**.-Es un campo de un sólo bit que, al ser establecido en 1 el valor por un switch, indica que ha habido saturación en la red en la dirección opuesta a la de la transmisión de la trama desde el origen al destino.
- **DE (Elegibilidad para Descartes)**.-Este bit es fijado por el dispositivo DTE, un ruteador por ejemplo, para indicar que la trama marcada es de menor importancia en relación con otras tramas que se marcan como **elegible para descartes** deben ser descartadas antes de cualquier otra. Lo anterior representa un mecanismo justo de establecimiento de prioridad en las redes Frame Relay.

Datos.-Los datos contienen información encapsulada de las capas superiores. Cada trama en este campo de longitud variable incluye un campo de datos de usuario o carga útil que varía en longitud y podrá tener hasta 16,000 bytes. Este campo sirve para transportar el **PDU (Paquete de Protocolo de las Capas Superiores)** a través de una red Frame Relay.
FCS (Secuencia de verificación de tramas).-Asegura la integridad de los datos transmitidos. Este valor calculado por el dispositivo de origen y verificado por el receptor para asegurar la integridad de la transmisión.

3.5.4 FORMATO DE LA TRAMA LMI

Las tramas Frame Relay que siguen las especificaciones LMI contienen los campos que se muestran en la figura 165.

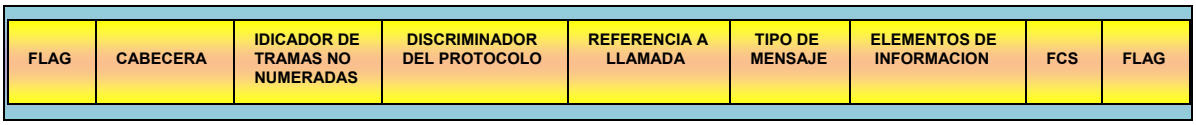


Figura 165

Indicador (flag):-Delimita el comienzo y el final de la trama
LMI-DLCI.-Identifica la trama como una trama LMI en vez de una trama básica Frame Relay. El valor DLCI específico del LMI definido por la especificación del consorcio LMI es DLCI = 1023.
Indicador de la información no numerada.-Fija el bit sondeo/final en cero.
Discriminador de protocolos.-Siempre contiene un valor que indica que es una trama LMI.
Tipo de mensaje.-Etiqueta la trama con uno de los siguientes tipos de mensaje:

- Mensaje de solicitud de status.-Permite que un dispositivo de usuario solicite el estado de la red.
- Mensaje de estado.-Responde a los mensajes de solicitud de estado. Los mensajes de estados incluyen mensajes de sobrevivencia y de estados del PVC.

Referencia de llamada.-Siempre contiene ceros. En la actualidad este campo no se usa ni tiene ningún propósito.
Elementos de información.-Contiene una cantidad variable de **IE's (Elementos Individuales de Información)**. Los IE's constan de los campos siguientes:

- Identificador IE.-Identifica de manera única el IE.
- Longitud del IE.-Indica la longitud del IE.
- Datos.-Consta de uno o más bytes que contienen datos encapsulados de las capas superiores.

FCS (secuencia de la Verificación de Tramas).-Asegura la integridad de los datos transmitidos.

3.5.5 MECANISMOS DE CONTROL DE SATURACIÓN

Frame Relay reduce el gasto indirecto de la red, al implementar mecanismos simples de notificación de la saturación, más que un control de flujo explícito por cada circuito virtual. En general Frame Relay se implementa sobre medios de transmisión de red confiables para no sacrificar la integridad de los datos, ya que el control de flujo se puede realizar por medio de los protocolos de las capas superiores La tecnología Frame Relay implementa dos mecanismos de notificación de saturación: **FECN (Notificación de la Saturación Explicita Hacia Adelante) BECN (Notificación de la Saturación explícita Hacia atrás)**. Tanto FECN como BECN son controlados por un sólo bit incluido en el encabezado de la trama Frame Relay. Este también contiene un bit **DE (Elegibilidad para descarte)**, que se utiliza para identificar el tráfico menos importante que se puede eliminar durante períodos de saturación. El bit FECN es parte del campo de direcciones en el encabezado de la trama Frame Relay. El mecanismo FECN inicia en el momento en que un dispositivo DTE envía tramas Frame Relay a la red. Si la red esta saturada, los dispositivos DCE (switches) fijan el valor de los bits FECN de las tramas en 1. Cuando las tramas llegan al dispositivo DTE de destino, el campo de direcciones (con el bit FECN en 1) indica que la trama se saturó en su trayectoria del origen al destino. El dispositivo DTE puede enviar esta información a un protocolo de las capas superiores para su procesamiento. Dependiendo de la implementación, el control de flujo puede iniciarse o bien la indicación se puede ignorar. El bit BECN es parte del campo de direcciones del encabezado de la trama Frame Relay. Los dispositivos del DCE fijan el valor del bit BECN en 1 en las que viajan en sentido opuesto a las tramas con bit FECN igual a 1. Esto permite al dispositivo DTE receptor saber que una trayectoria específica en la red está saturada. Posteriormente el dispositivo DTE envía información a un protocolo de las capas superiores para su procesamiento. Dependiendo de la implementación, el control de flujo puede iniciarse o bien se puede ignorar la indicación.

BIT DE

El bit DE (Elegibilidad para Descarte) de utiliza para indicar que una trama tiene una importancia menor que otras. El bit DE es parte del campo de direcciones en el encabezado de la trama Frame Relay. Los dispositivos DTE pueden fijar el valor del bit DE de una trama en 1 para indicar que esta tiene una importancia menor respecto a las demás tramas. Al saturarse la red los dispositivos DCE descartaran las tramas con el bit DE fijado en 1 antes de descartar aquellas que no la tienen. Por lo anterior disminuye la probabilidad de que los dispositivos DCE de Frame Relay eliminen datos críticos durante el blindaje de saturación.

VERIFICACION DE ERRORES EN FRAME RELAY

Frame Relay utiliza un mecanismo para la verificación de errores conocido como **CRC (Verificación de Redundancia cíclica)**. El CRC compara dos valores calculados para determinar si se ha presentado errores durante la transmisión del origen al destino. Frame Relay disminuye el gasto indirecto al implementarse la verificación de errores más que su corrección. Frame Relay por lo general se implementa en medios confiables de transmisión de red, por lo que la integridad de los datos no se sacrifica si la corrección de un error se deja a los protocolos de las capas superiores que operan en la parte más alta de Frame Relay.

3.5.6 ESTANDARIZACIÓN DE FRAME RELAY

La propuesta inicial para la estandarización de Frame Relay se presentó el CCITT en 1984. Sin embargo, por su falta de interoperabilidad y estandarización, Frame Relay no tuvo gran aceptación a finales de los 80. En 1990 ocurrió un gran desarrollo en la historia de Frame Relay cuando las compañías Cisco, Digital Equipment, Northern Telecom y StrataCom formaron un consorcio para aplicarse al desarrollo de la tecnología Frame Relay. Dicho consorcio desarrolló una especificación que conformó el desarrollo básico de Frame Relay que se estaba analizando en el CCITT, pero ampliaba el protocolo con características que ofrecían facilidades adicionales en entornos complejos de interconectividad en redes. A estas extensiones de Frame Relay se les conoce en conjunto como **LMI (Interfase de Administración Local)**. Desde que la especificación del consorcio se desarrolló y publicó, muchos proveedores han anunciado su apoyo a esta definición extendida de Frame Relay. La ANSI y el CCITT estandarizaron, posteriormente sus propias variaciones a la especificación LMI original, y actualmente se utilizan dichas especificaciones estandarizadas con mayor frecuencia que la versión original. En el ámbito internacional, la tecnología Frame Relay fue estandarizada por la ITU-T (Unión Internacional de Telecomunicaciones, Sector Telecomunicaciones). En Estados Unidos, Frame Relay es un estándar de ANSI.

3.5.7 VENTAS Y DESVENTAJAS DE FRAMA RELAY

Ventajas

No hay duda de que Frame Relay pasa información más rápidamente que X.25. Esto supondrá que hay un menor trabajo para el procesador. El tiempo que tarda para completar este trabajo debe ser menor, y los retrasos de la tramas reducidos. Hay tres factores que contribuyen a este retraso de extremo a extremos

- **Ejecución del procedimiento**.-Este es el tiempo que tarda un conmutador de paquetes en recibir un paquete o trama desde un enlace de llegada, e interceptar la información apropiada, y pasar el mismo paquete o trama al enlace de salida. Este tiempo normalmente es medido desde la llegada del último bit del paquete o trama al conmutador, hasta que es transmitido el primer bit del paquete o de la trama. Este retraso no se ve afectado por la rapidez de la transmisión de las líneas de llegada o salida, o por el tamaño de la trama, en caso de conmutadores bien diseñados.

- **Retraso en la transmisión.-**Este es el tiempo que tarda el paquete o trama en transitar en un enlace. Es medido desde la salida del primer bit desde del nodo de transmisión, hasta la recepción del último bit en el nodo de recepción. Este tiempo es proporcional a la longitud del paquete, a la velocidad de transmisión del enlace y a la longitud del enlace. Sin embargo, el retraso introducido por la longitud de la línea es normalmente ignorado.
- **Retaso en Cola.-**El encolado ocurre porque un único paquete o trama puede cruzar el enlace en un momento determinado y otro paquete esta listo para ser retransmitido cuando el primero esta siendo transmitido. La probabilidad de que esto ocurra y la longitud del la cola, dependen de la utilización del enlace, a mayor utilización, mayor cola. Para un uso eficiente de la red, hay que tener siempre ciertos niveles de encolado, la falta de una cola muestra que la línea esta disponible, pero que esto no es eficiente.

Los principios generales del diseño indican que para que las operaciones en los enlaces sean económicamente viables se requiere que haya siempre al menos una trama o paquete esperando por la transmisión en el enlace. Esto produce un retaso de la cola para cada trama o paquete de entre uno y dos periodos de retraso de transmisión de un trama o paquete en la cola. Veamos un ejemplo. Asumiendo que el tamaño total de la trama es de 1,024 bytes y la conexión es de 64kbps cada parte, la tabla 25 representa el retraso dentro la red de conmutación de paquetes y dentro de la red de Frame Relay asumiendo los retrasos típicos de procesado de 5 y 2 milisegundos respectivamente.

Actividad	**Conmutación de Paquetes**		**Frame Relay**	
Velocidad de Acceso a 64Kbps	Tiempo (ms)	Porcentaje del tiempo total	Tiempo (ms)	Porcentaje del tiempo total
Acceso al enlace del usuario X a A	128	11.6	128	11.7
Retraso del Conmutador A	5	0.5	2	0.2
Retraso en cola en Conmutador A	192	17.4	192	17.5
Enlace de A a B	128	11.6	128	11.7
Retraso del Conmutador B	5	0.5	2	0.2
Retraso en cola en Conmutador B	192	17.4	192	17.5
Enlace de B a C	128	11.6	128	11.7
Retraso del Conmutador C	5	0.5	2	0.2
Retraso en cola en	192	17.4	192	17.5

Conmutador C				
Acceso al enlace C al usuario a X	128	11.6	128	11.7
Tiempo total de transito	1103		1094	

Tabla 25

La primera tabla muestra que los retrasos en la red para ambos métodos son virtualmente idénticos. El retraso en la conmutación de paquetes representa únicamente un 1.5 %, del retraso total dentro de la red de conmutación de paquetes. Dentro de la red Frame Relay, el retraso de transito a través de los conmutadores representa un 0.6% del retraso total. Incluso reduciendo el retraso del conmutador a 0 tenemos un efecto despreciable sobre el retraso de transito. Entonces ¿dónde está el cuello de botella de la red?. La tabla 26 muestra que cerca del 60% del retraso total es debido al retraso de la transmisión. Este retraso es una función de la velocidad de las líneas y del tamaño de la trama. Si alteramos la velocidad de la línea (a 2Mbps) se alteran los resultados. La tabla 26 detalla el retraso de transito cuando se incrementa la velocidad de la red de enlace de 64Kbps a 2Mbps.

Actividad	**Conmutación de Paquetes**		**Frame Relay**	
Velocidad de Acceso a 2Mbps	Tiempo (ms)	Porcentaje del tiempo total	Tiempo (ms)	Porcentaje del tiempo total
Acceso al enlace del usuario X a A	4	7.3	4	8.7
Retraso del Conmutador A	5	9.1	2	4.3
Retraso en cola en Conmutador A	8	14.5	8	17.4
Enlace de A a B	4	7.3	4	8.7
Retraso del Conmutador B	5	9.1	2	4.3
Retraso en cola en Conmutador B	8	14.5	8	17.4
Enlace de B a C	4	7.3	4	8.7
Retraso del	5	9.1	2	4.3

Conmutador C				
Retraso en cola en Conmutador C	8	14.5	8	17.4
Acceso al enlace C al usuario a X	4	7.3	4	8.7
Tiempo total de transito	55		46	

Tabla 26

Reduciendo el tamaño del paquete también afecta a los resultados, sin embargo existen otras implicaciones al hacer esto. La reducción del tamaño del paquete dentro de la red de conmutación, probablemente, causa a los conmutadores de paquete el fragmentado de los datos de llegada y su recombinación posterior en el punto de destino. Esto es posible por la existencia de un número de secuencia. Sin embargo, esto no es posible en Frame Relay. En ambos casos el afectara al retraso de conmutación en los puntos de fuente y destino. En la tabla 26 se muestra que con el incremento de la velocidad de la línea, el retraso total de la red se reduce (representando una reducción del 95% aproximadamente). Por lo que encontramos que hay todavía una diferencia entre los retrasos totales en conmutación de paquetes y los retrasos dentro de la red de Frame Relay. En los paquetes individuales el retaso de procesamiento en los conmutadores representa un 27% del total del retaso para una red de conmutación de paquetes. Dentro de la red de Frame Relay este mismo retraso representa un 13% del retraso total de la red, la diferencia como podemos ver es grande. Como conclusión podemos observar que se puede proporcionar una reducción significativa en los retrasos de la red al incrementar la velocidad de las líneas. El cambio a tecnologías más rápidas en los conmutadores no tiene ningún efecto si se realiza sobre líneas de baja velocidad. Reducir el tamaño de la trama también tiene una aportación significativa para la reducción del retraso, pero esto también tiene un efecto sobre el incremento de carga de paquetes dentro de la red. Otro factor que afecta el retraso esta relacionado con el mecanismo de control de flujo. Las redes de conmutación de paquetes contiene un control de flujo, que consiste en que el usuario únicamente puede generar un número determinado de paquetes dentro de la red antes de parar y esperar por su reconocimiento Este mecanismo de rotación de ventana tiene un máximo de 127 paquetes, Si el usuario ha mandado esta ventana entera de paquete, no puede mandar más paquetes hasta que reciba el reconocimiento de alguno de los paquetes. Este proceso es conocido como **ventana deslizante**. Una red ideal estaría diseñada de tal manera que el usuario no tendría que suspender nunca el envío de datos a causa del falta de reconocimientos a paquetes anteriores. En Frame Relay no hay concepto de reconocimiento o ventanas, y permite a los usuarios mandar tantos datos como ellos requieran.

Frame Relay puede únicamente proporcionar ventajas sobre las redes de conmutación de paquetes si la velocidad del enlace dentro de la red son incrementados enormemente y su los procesos en los conmutadores son mejorados, proporcionando tiempo de submilisegundos. La discusión asume que Frame Relay ha sido implementado como una arquitectura modificada de la conmutación de paquetes. Esto es cierto en la mayoría de la implementaciones iniciales de Frame Relay. Sin embargo, sin que la comprobación de errores sea obligatoria para las características del protocolo, es posible implementar un conmutador en el cual no se tenga que esperar a que la trama sea completamente recibida antes de mandar otra. Esto tiene como resultado que el retraso del conmutador pueda ser ignorado. Una vez que la cabecera de la tramas sea leída, la trama puede ser dirigida directamente al buffer de salida. Sin embargo el retraso de cola debe ser considerado, porque muchas de las redes se construyen basándose en unos objetivos previamente diseñados donde el encolamiento es un elemento esencial.

Ahorro en los costos de telecomunicaciones.-Con el servicio Frame Relay 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.
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 34Mbps y de los criterios de encaminamiento de la Red de Datos, orientados a minimizar el número de nodos de tránsito.
Flexibilidad del servicio.-Frame Relay 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 del Cliente.
Servicio normalizado.-Frame Relay 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.

Desventajas

Una característica existente en la conmutación de paquetes es una técnica que es actualmente muy considera por los usuarios, el proceso de garantizar el envío de datos. Frame Relay no ofrece esto, no se establece ninguna orden acerca de como las tramas deben pasar a través de la red. La única recomendación de Frame Relay es que las tramas deben llegar en el mismo orden en que fueron mandadas. Para garantizar la correcta secuenciación de la tramas. Este mecanismo de secuenciación no debe confundirse con el proceso de garantizar la integridad de los datos. Las redes de conmutación de paquetes, generalmente garantizan que los datos que son mandados en la red son recibidos por el usuario en la misma secuencia y sin errores. Mediante un número de comprobación de secuencia de paquetes y su validación, una comprobación de error en los paquetes y de las capacidades de buffering. En cambio Frame Relay no garantiza la entrega de los datos. Los requisitos para que los datos sean entregados en la misma secuencia en que fueron recibidos esta relacionado únicamente con que los datos no sean perdidos dentro de la red.

La intención del protocolo de Frame Relay es operar a altas velocidades, en circuitos digitales de excepcionalmente buena calidad, donde los errores en los bits son extremadamente raros. Sin embargo, mientras que el número de errores introducido por el uso de esa infraestructura es pequeño, la red podría perder muchas tramas simplemente por que es incapaz de entregarlas a causa de la congestión. Consideremos el ejemplo de la figura 166 en el que una trama pasa a través de distinto conmutadores de trama en su camino por la red desde un origen a un destino. Cada salto de trama representa el paso entre dos conmutadores. En nuestro ejemplo la trama para ir de extremo a extremo da 5 saltos de trama.

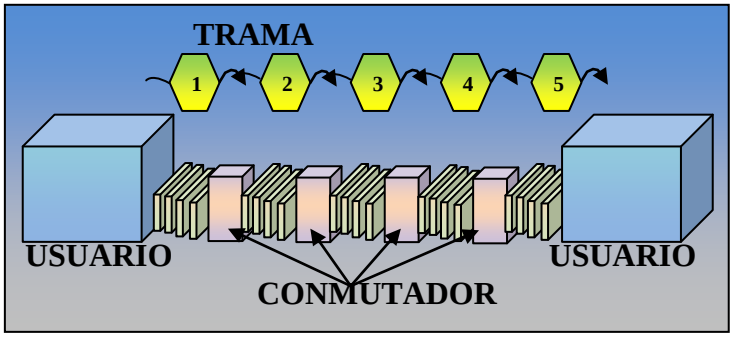


Figura 166

Consideremos el ejemplo anterior asumiendo que la trama es pérdida en el primer salto (o por congestión en el primer conmutador), los saltos de tramas 2 al 6 representan la petición de retransmisión y los saltos del 7 al 11, figura 167 representan la retransmisión. Por tantos para una trama única pasando a través de la red se requieren al menos 11 saltos de procesamiento, más del doble de los requeridos si no ocurre error.

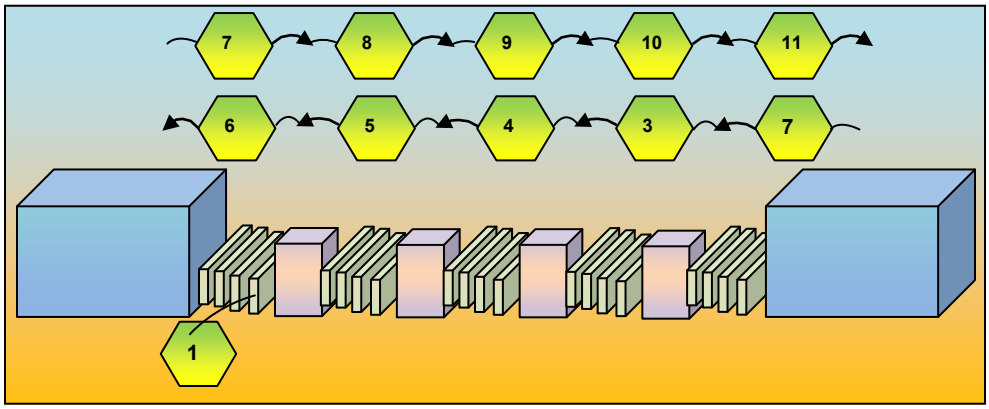


Figura 167

Si una trama es pérdida en el último salto, 14 saltos de procesamiento son necesarios para recuperarla, como se muestra en la figura 168, los saltos del 1 al 5 para el camino inicial, 6 al 10 para la petición de retransmisión, y los saltos del 11 al 15 para la retransmisión, esto representa más de tres veces el procesamiento requerido para el paso de una trama simple.

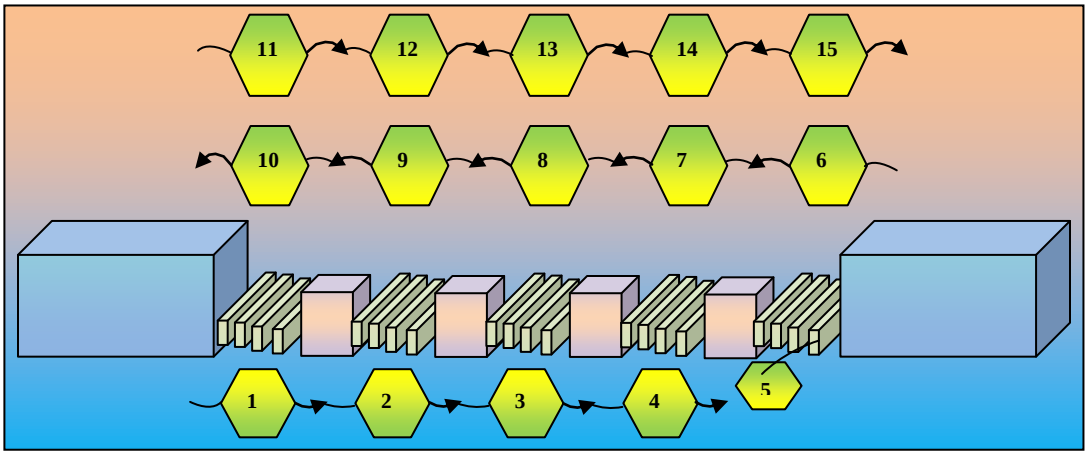


Figura 168

Esta metodología de recuperación es la práctica estándar para redes diseñadas bajo los principios de Frame Relay y puede significar una carga adicional para la red. Los ejemplos sólo muestran la pérdida de una trama y su recuperación. Si hay gran cantidad de tramas pérdidas, la cantidad de tráfico que la red recibe podrá expandirse significativamente. Todo este tráfico adicional es un componente más de los problemas de congestión que probablemente causen el descarte de más tramas. Esta es la razón por la cual algunos vendedores eligen la entrega garantizada como característica añadida Frame Relay. Esta es una combinación de Frame Relay y de la conmutación de paquetes en la cual no hay necesariamente un protocolo de control de errores de extremo a extremo dentro de la red, pero hay asegurada una integridad de los datos y su recuperación en el nivel de enlace. Tomando el ejemplo previo, mostramos los principios básicos sobre el siguiente ejemplo: La trama errónea o pérdida es ahora recuperada localmente en el salto 2, figura 169 solicitando su retransmisión, el salto 3 representa la retransmisión, y los salto 4 al 7 la transmisión de la trama. En este caso un único salto adicional de la trama es requerido para solventar la situación anómala. Naturalmente, la integridad del enlace requiere procesamientos adicionales dentro de la trama, pero este proceso no hay tantos intentos como X.25, y por consiguiente obtiene un retraso situado entre el retraso de Frame Relay y X.25.

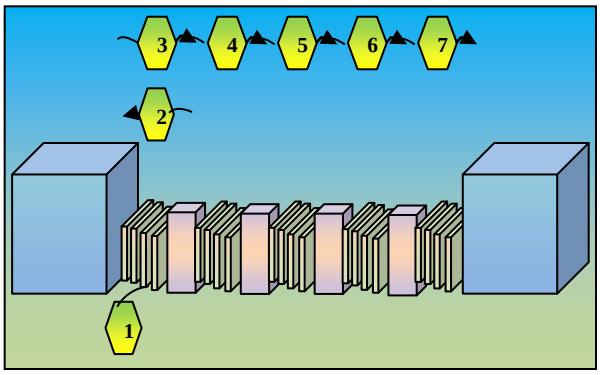


Figura 169

3.5.9 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.

Actualmente, dado el alto grado de informatización que han alcanzado las empresas en los últimos años, es muy común la convivencia de varias de las aplicaciones citadas y otras similares en el entorno de un mismo cliente, lo que hace aún más provechosa la utilización del servicio Frame Relay como medio de transporte único.

IV.-NORMAS Y ESTANDARES DE LAS REDES

4.1 LA FUNCION DE LOS ESTANDARES EN LAS REDES

Los estándares han sido los responsables del éxito y del crecimiento de la industria de los productos y equipos de redes. Cuando un fabricante cumple una serie de estándares, esto significa que dicho fabricante acepta fabricar equipos que se adapten a las especificaciones del estándar o norma. La mayoría de redes incluyen una combinación de hardware y software de varios fabricantes. Esta posibilidad de combinar los productos producidos por distintos fabricantes es posible debido a la existencia de estándares a la industria. Los estándares son directrices a las que los fabricantes se adhieren voluntariamente para conseguir que sus productos sean compatibles con productos de otros vendedores. En general, estos estándares tratan de:

- Tamaño.
- Forma.
- Materiales.
- Función.
- Velocidad.
- Distancia.

Más específicamente, los estándares definen características físicas y de funcionamiento de:

- Equipos para equipos personales.
- Equipos para redes y comunicaciones.
- Sistemas operativos.
- Software.

Por ejemplo, los estándares hacen posible comprar una tarjeta de red producida por un fabricante para un equipo producido por otro fabricante, con una seguridad razonable de que la tarjeta:

- Se adaptará al equipo.
- Funcionará con el cableado de la red.
- Transmitirá las señales del equipo y las enviará hacia la red.
- Recibirá datos de la red y los entregará al equipo.

4.2 EL ORIGEN DE LOS ESTANDARES

Los estándares se han desarrollado principalmente a partir de dos fuentes:

- Aceptación popular (promovido por los clientes).
- Recomendaciones de organizaciones.

Los estándares promovidos por los clientes surgen de la aceptación popular. El mejor ejemplo de esto es el término “PC-compatible”, que implica que un producto funcionará con un equipo personal de IBM o un clónico. Sin embargo, el crecimiento del campo de las redes a mediados y finales de los ochenta, se hizo patente que la popularidad de los clientes no era adecuada para crear e imponer estándares.

4.2.1 LA INFLUENCIA DE LA COMUNIDAD EMPRESARIAL

En los primeros años de las redes, varias grandes empresas, incluyendo IBM, Howelly y Digital Equipment Corporation (DEC), usaban sus propios estándares para determinar como debían conectarse los equipos. Estos estándares describían como debían pasar datos de un equipo a otro, pero los estándares sólo eran aplicables si todos los equipos estaban fabricados por la misma compañía. Hacer que equipos de un fabricante se comunicaran con equipos de otro fabricante era problemático. Por ejemplo, las redes que cumplían la compleja arquitectura de red de IBM, llamada Arquitectura de sistemas de red **(SNA, Systems Network Architecture)** no podían comunicarse directamente con redes que utilizaban la Arquitectura de redes de Digital **(DNA, Digital Network Architecture)** de DEC. A medida que la tecnología de redes maduraba, las empresas y negocios comenzaron a confiar datos cruciales a las redes. Pero a mediados de los ochenta, se presentaron entre fabricantes de redes los mismos problemas de comunicaciones existentes anteriormente

entre fabricantes de mainframes. La creciente necesidad de que las empresas interactuarán y compartieran datos era inevitable

Los fabricantes de equipos descubrieron esta oportunidad de negocio. Vieron que la tecnología de redes que había permitido la comunicación cumpliendo estándares sería mucho más provechoso a largo plazo que los equipos que trabajarán en un entorno particular de un único fabricante. Como resultado, los estándares o normas se convirtieron gradualmente en parte del entorno de redes y los equipos.

4.2.2 LA INFLUENCIA DE LA COMUNIDAD TÉCNICA

Actualmente, ciertas organizaciones nacionales e internacionales, en lugar de los clientes crean y definen prácticamente todos los estándares técnicos sobre redes. Alguna de estas organizaciones existen desde hace muchos años, y otras, tales como el SQL Access Group, han surgido recientemente a medida que han participado nuevas aplicaciones. A su vez, estas han creado nuevos entornos de red que requieren nuevas directrices. Aunque pueda que existan docenas de organizaciones que estén propugnando estándares de todo tipo, sólo algunas han ganado el reconocimiento necesario para encabezar el soporte de los principales fabricantes de equipo. Estas asociaciones y organizaciones se han convertido en la base sobre la que se construye la aceptación de las redes. Por tanto, los ingenieros de redes necesitan estar familiarizados con los nombres de las organizaciones y con las áreas de las redes con las que tienen influencia.

4.3 ORGANIZACIONES DE ESTANDARIZACION

No existe una fuente única para todos los estándares de redes. Generalmente, una organización de estándares coordina las especificaciones de diversas clases de equipos, o define los parámetros para características o funciones. Sin embargo, en ocasiones, la necesidad de un nuevo estándar hará surgir un nuevo proceso y, generalmente, dará lugar a un nuevo estándar mediante el consejo o mediante la actividad del mercado. La mayoría de estándares nacionales e internacionales de redes han surgido dentro de un número limitado de organizaciones. Cada una de estas organizaciones definen estándares para un área distinta de la actividad de las redes. Las organizaciones son:

- El Instituto Nacional de Estandarización Americano **(ANSI, American National Standars Institue)**.
- El Comité Consultivo Internacional de Telegrafía y Telefonía **(CCITT)**.
- La Asociación de Industrias Electrónicas **(EIA, Electronis Industries Association)**.
- El Instituto de Ingenieros Eléctricos y Electrónicos **(IEEE, Institude of Electrical and Electronics Engineers)**.
- La Organización Internacional de Estandarización **(ISO, Institude Organization for Standarization)**.
- El grupo de Gestión de Objetos **(OMG, Object Management Group)**.
- La Fundación de Software Abierto **(OSF, Open Software Foundation)**.
- El Grupo de Acceso SQL **(SAG, SQL Access Group)**.

Es importante conocer estas organizaciones, ya que sus siglas se han convertido en una parte común de la terminología general de las redes.

4.3.1 ORGANIZACIÓN INTERNACIONAL DE ESTANDARIZACION

La Organización Internacional de Estandarización **(ISO, International Organization for Starndardization)** es una organización con sede en París a la que pertenecen varios países, cada uno de los cuales es representado por su organización principal de estandarización. Otras organizaciones representadas por el ISO incluyen:

- Organizaciones gubernamentales.
- Empresas.
- Instituciones de educación.
- Organismos de investigación.

- El CCITT.

La ISO trabaja para establecer estándares internacionales de todos los servicios y productos fabricados.

4.3.1.1 OBJETIVOS DE LA ISO EN COMUNICACIONES ENTRE EQUIPOS

En el área de la informática, el objetivo de la ISO es establecer estándares globales para las comunicaciones y el intercambio de información. Los estándares promoverán entornos de red abiertos que permitan a sistemas informáticos de distintos fabricantes comunicarse entre sí, utilizando protocolos que han sido aceptados internacionalmente por los miembros de la ISO.

4.3.1.2 EL MODELO DE REFERENCIA DE INTERCONEXION OSI

El modelo OSI representa los siete niveles del proceso mediante el cual los datos se empaquetan y se transmiten desde una aplicación emisora a través de cables físicos hacia la aplicación receptora. En 1978, la ISO divulgó un conjunto de especificaciones que describían la arquitectura de red para la conexión de dispositivos diferentes. El documento original se aplicó a siete sistemas que eran abiertos entre sí, debido a que todos ellos podían utilizar los mismos protocolos y estándares para intercambiar información. En 1984 la ISO presento una revisión de este modelo y lo llamó **Modelo de Referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection)**. La revisión de 1984 se ha convertido en un estándar internacional y se utiliza como guía para las redes. El modelo OSI es la mejor guía y la más ampliamente utilizada para la visualización de los entornos de red. Los fabricantes se ajustan al modelo OSI cuando diseñan sus productos para red. Este ofrece una descripción del funcionamiento conjunto de hardware y software de red por niveles para posibilitar las comunicaciones. El modelo también ayuda a localizar problemas proporcionando un marco de referencia que describe el supuesto funcionamiento de los componentes.

4.3.1.3 UNA ARQUITECTURA POR NIVELES

La arquitectura del modelo de referencia OSI divide la comunicación de red en siete niveles. Cada nivel cubre diferentes actividades, equipos y protocolos de red. La división en niveles específica funciones y servicios diferentes en la transferencia de datos desde un equipo hacia otro a través del cableado de red. El modelo OSI define como se comunica y trabaja cada nivel con los niveles inmediatamente superior e inferior. Cada nivel proporciona algún servicio o acción que prepara los datos para entregarlos a través de la red a otro equipo. Los niveles inferiores (1 y 2) definen el medio físico de la red y las tareas relacionadas, como la colocación de los bits de datos sobre las placas de red (NIC, Netwoks Interface Cards) y el cable. Los niveles superiores definen la forma en que las aplicaciones acceden a los servicios de comunicación. Cuanto más alto es el nivel, más compleja es su tarea. Los niveles están separados entre sí por interfaces. Todas las demandas se pasan desde un nivel, a través de la interfaz, hacia el siguiente. Cada nivel se basa en los estándares y actividades del nivel inferior.

4.3.1.4 RELACION ENTRE LOS NIVELES DEL MODELO OSI

Cada nivel proporciona servicios al nivel superior y lo protege de los detalles de implementación de los servicios de los niveles inferiores. Al mismo tiempo, cada nivel parece estar en comunicación directa con su nivel asociado del otro equipo. Esto proporciona una comunicación lógica, o virtual, entre niveles análogos. En realidad, la comunicación real entre niveles adyacentes tiene lugar en un sólo equipo. En cada nivel, el software implementa las funciones de red de acuerdo con un conjunto de protocolos. Antes de pasar los datos de un nivel a otro, se dividen en paquetes, que se transmiten como un todo de un dispositivo a otro sobre la red. La red pasa un paquete del nivel software a otro en el mismo orden de los niveles. En cada nivel, el software agrega información de

formato o direccionamiento del paquete, que es necesaria para la correcta transmisión del paquete a través de la red.

En el extremo receptor, el paquete pasa a través de los niveles en orden inverso. Una utilidad software en cada nivel lee la información del paquete, elimina y pasa el paquete hacia el siguiente nivel superior. Cuando el paquete alcanza el nivel de aplicación, la información de direccionamiento ha sido eliminada y el paquete se encuentra en su formato original, con lo que es legible para el receptor. Con la excepción del nivel más bajo del modelo OSI, ningún nivel puede pasar información directamente a su homólogo del otro equipo. En su lugar, la información del equipo emisor debe ir descendiendo por todos los niveles hasta alcanzar el nivel físico. En ese momento, la información se desplaza a través del cable de red hacia el equipo receptor y asciende por sus niveles hasta que alcanza en nivel correspondiente. La interacción entre niveles adyacentes ocurre a través de una interfaz. La interfaz define los servicios ofrecidos por el nivel inferior para el nivel superior y, lo que es más, define como se accede a dichos servicios. Además, cada nivel de un equipo aparenta estar en comunicación directa con el mismo nivel del otro equipo.

4.3.1.5 PAQUETES DE DATOS Y EL MODELO OSI

Los paquetes se agrupan y se desagrupan de acuerdo con el modelo OSI. El proceso de creación de paquetes se inicia en el nivel de aplicación del modelo OSI, donde se generan los datos. La información a enviar a través de la red comienza en el nivel de aplicación y descienden a lo largo de los siete niveles. En cada nivel, se agrega a los datos información relevante de ese nivel. Esta información es utilizada por el correspondiente nivel del equipo receptor. El nivel de enlace del equipo receptor. En el nivel de transporte, el bloque de datos original se divide en los paquetes reales. El protocolo define la estructura de los paquetes utilizados por los dos equipos. Cuando el paquete alcanza el nivel de transporte, se agrega una secuencia de información que guía al equipo receptor en la desagrupación de los datos de los paquetes. Cuando finalmente, los paquetes pasan a través del nivel físico camino del cable, contiene información de cada uno de los otros seis niveles.

4.3.1.5.1 DIRECCIONAMIENTO DE PAQUETES

La mayoría de los paquetes de la red se dirigen a un equipo específico y, como resultado, obtienen la atención de un único equipo. Cada tarjeta de red ve todos los paquetes enviados de un segmento de cable, pero interrumpe el equipo sólo si la dirección del paquete coincide con la dirección individual de la tarjeta. De forma alternativa, se puede utilizar una dirección de tipo difusión múltiple. Los paquetes enviados con una dirección de tipo difusión múltiple pueden recibir la atención simultánea de varios equipos de red. En sustituciones que envuelvan grandes redes que cubren grandes regiones (o incluso países) y ofrecen varios caminos de comunicación posibles, la conectividad y la conmutación de componentes de la red utilizan la información de direccionamiento del paquete para determinar el mejor camino para los paquetes.

4.3.1.5.2 COMO DIRIGIR LOS PAQUETES

Los componentes de red utilizan la información de direccionamiento de los paquetes para dirigir los paquetes a sus destinos o para mantenerlos alejados de las posiciones de la red a las que no pertenecen. Las dos funciones siguientes juegan un papel principal en la dirección apropiada de paquetes:

- **Reenvío de paquetes**.-Los equipos envían un paquete al siguiente componente de red apropiado en base a la dirección del encabezado del paquete.
- **Filtrado de paquetes**.-Los equipos utilizan criterios, como una dirección, para seleccionar los paquetes específicos.

4.3.2 INSTITUTO DE INGENIEROS ELÉCTRICOS Y ELECTRÓNICOS

El Instituto de Ingenieros Eléctricos y Electrónicos **(IEEE, Institude of Electrical and Electronics Engineers)** es una sociedad creada en Estados Unidos y que publica diversos estándares, incluyendo los relacionados con comunicaciones de datos.

4.3.2.1 EL ESTANDAR IEEE 802.x

Los niveles inferiores del modelo OSI están relacionados en el hardware: la tarjeta de red y el cableado de la red. Para avanzar más en el refinamiento de los requerimientos de hardware que operan dentro de estos niveles, el IEEE ha desarrollado mejoras específicas para diferentes tarjetas de red y cableado. De forma colectiva, estos refinamientos se conocen como proyecto 802

4.3.2.2 EL PROYECTO 802

Cuando comenzaron a aparecer las primeras redes de área local (LAN), como herramientas potenciales de empresa a finales de los setenta, el IEEE observo que era necesario definir ciertos estándares para redes de área local. Para conseguir esta tarea el IEEE emprendió lo que se conoce como proyecto 802, debido al año y al mes de comienzo (Febrero de 1980). Aunque los estándares IEEE 802 publicados realmente son interiores a los estándares ISO, ambos estaban en desarrollo aproximadamente al mismo tiempo y compartían información que concluyo en la creación de dos modelos compatibles. El proyecto 802 definió estándares de redes para las componentes físicas de una red (la tarjeta de red y el cableado) que se corresponden con los niveles físicos y de enlaces de datos del modelo OSI. Las especificaciones 802 definen estándares para:

- Tarjeta de red (NIC).
- Componentes de redes de área global (WAN).
- Componentes utilizadas para crear redes de cable coaxial y de par trenzado.

Las especificaciones 802 definen la forma en que las tarjetas de red acceden y transfieran datos sobre el medio físico. Estas incluyen conexión, mantenimiento y desconexión de dispositivos de red. La selección del protocolo a ejecutar en el nivel de enlace de datos es la decisión más importante que se debe tomar cuando se diseña una red de área local. Este protocolo define la velocidad de la red, el método utilizado para acceder a la red física, los tipos de cables que se pueden utilizar, las tarjetas de red y dispositivos que se instalan. Los comités 802 son:

- 802.1 Interconexión de Redes.
- 802.2 Control de Enlace Lógico (LLC).
- 802.3 Ethernet.
- 802.4 Token Bus.
- 802.5 Token Ring.
- 802.6 Redes MAN.
- 802.7 Grupo Consultor Técnico de Banda Ancha.
- 802.8 Grupo Consultor de Fibra Optica.
- 80.2.9 Redes Integradas de Voz y Datos.
- 802.10 Seguridad en Redes.
- 802.11 Redes Inalámbricas.
- 802.12 Redes con Acceso de Prioridad de Demanda.
- 802.13 Especificación del Método de Acceso y el Nivel Físico de la Televisión por Cable.
- 802.14 Cable módem.
- 802.15 Redes Inalámbricas de área personal.
- 802.16 Redes Inalámbricas Banda Ancha.

4.3.2.3 MEJORAS SOBRE EL MODELO OSI

Los niveles inferiores del modelo OSI, el nivel físico y el nivel de enlace de datos, definen la forma en que múltiples equipos pueden utilizar la red simultáneamente sin que exista interferencia entre ellos. El proyecto IEEE 802 incorporó las especificaciones a esos dos niveles para crear estándares que tengan definidos los entornos LAN dominantes. Tras la decisión de que se necesitaban más detalles en el nivel de enlaces de datos, el comité de estándares IEEE 802 dividió el nivel de enlace de datos en dos subniveles:

- **Control de enlace lógico (LLC, Logical Link Control)**.-Establece y finaliza los enlaces, controla el tráfico de tramas, secuencia las tramas y confirma la recepción de las tramas.
- **Control de acceso al medio (MAC, Media Access Control)**.-Gestiona el acceso al medio, delimita las tramas, comprueba los errores de las tramas y reconoce las direcciones de las tramas.

4.3.2.3.1 SUBNIVEL DE CONTROL DE ENLACE LÓGICO (LLC)

El subnivel LLC gestiona la comunicación de enlace de datos y define el uso de puntos de interfaz lógicos llamados puntos de acceso al servicio **(SAP, Services Acces Points)**. Otros equipos pueden ser referencia y utilizar los SAP's para transferir información desde el subnivel LLC hacia los niveles superiores del modelo OSI. La categoría 802.2 define estos estándares.

4.3.2.3.2 SUBNIVEL DE CONTROL DE ACCESO AL MEDIO (MAC)

El subnivel MAC es el más bajo de los dos subniveles, proporcionado acceso compartido al nivel físico para las tarjetas de red para los equipos. El nivel MAC se comunica directamente con la tarjeta de red y es el responsable del envío de datos libre de errores entre dos equipos de la red. Las categorías 802.3, 802.4, 802.5 y 802.12 definen estándares tanto para este subnivel como para el nivel uno del modelo OSI, el nivel físico.

4.3.3 EL COMITÉ CONSULTIVO INTERNACIONAL DE TELEGRAFIA Y TELEFONIA

El CCITT, tiene su sede en Ginebra, Suiza. Fue establecido como parte de la Unión Internacional para las Telecomunicaciones **(ITU, International Telecomunications Union)** de Naciones Unidas y la ITU sigue siendo su asociada padre. El CCITT estudia y recomienda el uso de estándares de comunicaciones reconocidos en todo el mundo y publica sus recomendaciones cada cuatro años. Cada actualización se distingue por el color de su cubierta.

4.3.3.1 PROTOCOLOS CCITT

Los protocolos CCITT se aplican a:

- Módems.
- Redes.
- Transmisión de facsímiles (faxes).

4.3.3.2 GRUPOS DE ESTUDIO DEL CCITT

El CCITT ha sido dividido en grupos de estudio para el período de 1997-2000; cada grupo de estudio esta preparando recomendaciones para estándares de diferentes áreas temáticas. Estas áreas temáticas incluyen:

- SG 2 Funcionamiento de redes y servicios.
- SG 3 Principios de tarifas y contabilidad, incluyendo cuestiones relacionadas con la política y economía de las telecomunicaciones.
- SG 4 Mantenimiento de redes y telecomunicaciones.
- SG 5 Protección contra los efectos electromagnéticos del entorno.

- SG 6 Plantas externas.
- SG 7 Redes de datos y comunicaciones en sistemas abiertos.
- SG 8 Características de los sistemas telemáticos.
- SG 9 Transmisión de la televisión y el sonido.
- SG 10 Lenguajes y aspectos generales de software para sistemas de telecomunicaciones.
- SG 11 Requerimientos de Señales.
- SG 12 Rendimiento de la transmisión punto a punto de redes y terminales.
- SG 13 Aspectos generales de redes.
- SG 15 Redes de Transporte, sistemas y equipamiento.
- SG 16 Servicios y sistemas multimedia.

4.3.3.3 LA SERIE V

Las recomendaciones para la estandarización del diseño y el funcionamiento de módems (transmisión sobre redes telefónicas) reciben el nombre genérico de serie V. Esta serie incluye:

- V.22 Estándar para módem full-dúplex 1,200 bps.
- V.22bis Estándar para módem full-dúplex 2,400 bps
- V.28 Define los circuitos en la interfaz RS-232
- V.32 Estándar asíncrono y síncrono 4,800/9,600 bps.
- V.32bis Estándar asíncrono y síncrono hasta 14,400 bps.
- V.35 Define altas velocidades de datos sobre circuitos combinados.
- V.42 Define estándares de verificación de errores.
- V.90 Define un estándar para la comunicación vía módem a 56 Kbps.

4.3.3.4 LA SERIE X

La serie X cubre los estándares de Interconexión de Sistemas Abiertos OSI e incluyen:

- X.200 (ISO 7498) Modelo de referencia OSI.
- X.25 (ISO 7776) Interfaz de red de conmutación de paquetes.
- X.400 (ISO 10021) Gestión de mensajes (correo electrónico).
- X.500 (ISO 9594) Servicios de directorio.
- X.700 (ISO 9595) Protocolo de información común de gestión **(CMPI, Common Management Information Protocol)**.

4.3.4 INSTITUTO NACIONAL DE ESTANDARIZACION AMERICANO

El Instituto Nacional de Estandarización Americano **(ANSI, American National Standars Institute)** es una organización de industrias y grupos de negocios de Estados Unidos dedicada al desarrollo de estándares de comunicaciones y funcionamiento en general. ANSI define y publica estándares para:

- Códigos.
- Alfabetos.
- Esquemas de señalización.
- Protocolos de comunicaciones.

4.3.4.1 ANSI EN MICROEQUIPOS

En el área de microequipos, generalmente ANSI interviene en los temas de lenguaje de programación la interfaz **SCSI**. Los lenguajes de programación, tales como C, se adaptan a las recomendaciones ANSI para eliminar problemas al llevar un programa desde un tipo de sistema equipos o entorno a otro.

4.3.4.2 ESPECIFICACIONES Y NORMAS ANSI

Las principales especificaciones y normas ANSI incluyen:

- ANSI 802.1-1985/IEEE 802.5.-Acceso, protocolo, cableado e interfaz de Token Ring.
- ANSI/IEEE 802.3.-Acceso múltiple por detección de portadora en cable coaxial con detección de colisiones **(CSMA/CD, Coaxial-cable carrier-sense múltiple-acces/CD)** para redes Ethernet.
- ANSI X3.135.-Métodos de consulta a base de datos con lenguaje de consulta estructurado (SQL) para clientes front-end y servicios de bases de datos back-end.
- ANSI X3.92.-Un algoritmo de cifrado para privacidad y seguridad.
- ANSI X12.-Intercambio electrónico de datos **(EDI, Electronic Data Interchange)** que define el intercambio de órdenes de compra, albaranes, facturas y otros formularios habituales en contabilidad.
- ANSI X3T9.5.-Especificación de interfaz de datos distribuida de fibra **(FDDI, Fiber Distributed Data Interface)** para transmisión de voz y datos sobre cable de fibra óptica a 100 Mbps.
- Sonet.-Red óptica sincronía **(Synchronous Optical Network)**, una especificación de fibra óptica que define una infraestructura global para transmisión de información sincronía e isócrona (datos sensibles al tiempo, tales como video en tiempo real).

4.3.5 ASOCIACION DE INDUSTRIAS ELECTRÓNICAS

La Asociación de Industrias Electrónicas **(EIA, Electronics Industries Association)** es una organización fundada en 1924 por fabricantes de equipos y dispositivos electrónicos de Estados Unidos. Desarrolla estándares de la industria para la interfaz de equipos de procesamiento de datos y comunicaciones, y ha publicado muchos estándares asociados con las telecomunicaciones y comunicaciones entre equipos. La EIA trabaja estrechamente relacionada con otras asociaciones, tales como la ANSI y la ITU.

4.3.5.1 ESTANDARES DE INTERFAZ SERIE EIA

Los estándares EIA para la interfaz serie entre módems y equipos incluyen:

- RS-232.-Estándar para conexiones serie utilizando conectores DB-9 o DB-25 y longitudes máximas de cable de 18 metros. Define las conexiones entre DTE **(Data Terminal Equipment)** y e DCE **(Data Comunications Equipment)**.
- RS-449.-Una interfaz serie con conexiones DB-37 que define los estándares RS-422 y RS-423 como subconjuntos.
- RS-422.-Define una interfaz balanceada multipunto.
- RS-423.-Define una interfaz digital no balanceada.

4.3.6 GRUPO DE GESTION DE OBJETOS

El Grupo de Gestión de Objetos **(OMG, Objet Management Group)** consta de, prácticamente, 300 organizaciones implicadas en desarrollar un conjunto de lenguajes, interfaces y estándares de protocolos que los fabricantes puedan usar para crear aplicaciones que funcionen en entornos multifabricante. El OMG certifica productos diseñados para cubrir los estándares y especificaciones aceptados por los miembros del OMG. En el camino hacia sus objetivos, el OMG ha desarrollado la arquitectura de gestión de objetos **(OMA, Objet Management Architecture)**, un modelo para aplicaciones y entornos orientados a objetos. La arquitectura OMG ha sido adoptada por la fundación de software abierto (OSF), que esta desarrollando entornos software por cables llamados el entorno de computación distribuida **(DCE, Distributed Computing Environmente)** y el entorno de gestión distribuida **(DME, Distributed, Management Environment)**. Los estándares OMG son similares a elementos de la vinculación e incrustación de objetos de Microsoft **(OLE, Objet Linking and Embedding)**.

4.3.7 FUNDACION DE SOFTWARE ABIERTO

La fundación de software abierto **(OSF, Open Software Foundation)**, miembro del Open Group, crea entornos de computación adquiriendo y combinando tecnología de otros fabricantes y distribuyendo los resultados a los interesados. Estos entornos neutrales, respecto a su fabricante, denominados entornos de software de sistemas abiertos, pueden ser usados para crear un conjunto de tecnologías de sistemas abiertos en las que los usuarios pueden incorporar software y hardware de varias fuentes. El entorno software OSF comprende los siguientes componentes:

- Entorno de computación distribuida (DCE).-Esta plataforma simplifica el desarrollo de productos en un entorno mixto.
- Entorno de gestión distribuida (DME).-Ofrece herramientas para la gestión de sistemas en entorno distribuidos y de varios fabricantes.
- El open software foundation/1 (OSF/1).-En un sistema operativo UNIX, basado en el kernel Match, que soporta multiprocesamiento simétrico, características amplias de seguridad y configuración dinámica.
- OSF/Motif.-Es una interfaz gráfica de usuario que crea un entorno común relacionado con el **Common User Acces (CUA)** de IBM.
- Formato de distribución independiente de la arquitectura OSF **(ANDF, Architecture-Neutral Distribution Format)**.

4.3.8 GRUPO DE ACCESO SQL

El grupo de acceso SQL **(SAG, SQL Acces Group)** es un consorcio de 39 compañías fundado en 1989 por Hewlett Packard, Digital, Oracle Corporation y Sun Microsystem. Su objetivo es trabajar con la ISO para crear estándares que describan la interoperabilidad de sistemas front-end y back-end. El propósito de SAG es promover la interoperabilidad entre estándares del lenguaje de consulta estructurado (SQL), para que varias bases de datos relacionales y herramientas basadas en SQL que pueden trabajar conjuntamente en un entorno de bases de datos de varios fabricantes. Esto hará posible que diversas aplicaciones de bases de datos que se ejecutan en plataformas distintas puedan compartir e intercambiar datos.

4.3.8.1 ESPECIFICACIONES TÉCNICAS DE SAG

SAG ha desarrollado tres especificaciones técnicas:

- Lenguaje de consulta estructurado **(SQL, Structured query language)**.-Es una especificación que sigue las especificaciones internacionales a la hora de implementar el lenguaje SQL.
- Acceso a bases de datos remotas de SQL **(SQL Remote Database Access)**.-Esta especificación define la comunicación entre un servidor de bases de datos remoto y un cliente basado en SQL.
- Interfaz de llamadas de acceso a SQL **(CLI, Call-Level Interface)**.-Es un grupo de API ofrece una interfaz con productos basados en SQL.

4.3.9 LA SOCIEDAD DE INTERNET

La sociedad de Internet es el comité para el diseño, ingeniería y gestión de Internet. Se encarga del propio funcionamiento de Internet, así como de la normalización de los protocolos usados por los sistemas finales. Dentro de la sociedad de Internet hay tres organizaciones responsables tanto del desarrollo de los estándares como de su publicación:

- **El comité para la arquitectura de Internet (IAB, Internet Architecture Board)**.-Responsable de definir toda la arquitectura de Internet, proporciona las directrices y las líneas de actualización del IETF.
- **El comité para la ingeniería en Internet (IETF, Internet Engineering Task Force)**.-Responsable del desarrollo e ingeniería de los protocolos.

- **El comité para la investigación en Internet (IRTF, Internet Research Task Force)**.- Responsable de la gestión de las actividades del IETF, así como del proceso de normalización.

Todo trabajo necesario para la especificación de las normas y los protocolos se lleva a cabo mediante grupos de trabajo. La pertenencia de cada uno de los grupos de trabajo es voluntaria, siendo característico el hecho de que cualquier interesado puede participar en los distintos grupos. Durante el desarrollo de una especificación, el grupo de trabajo hará un borrador del documento final denominado **Borrador Internet (Internet Dratf)** el cual se publicará y estará disponible hasta seis meses, el IESG puede aprobar que el borrador se publique como **RFC (Request For Commente)**. Si el borrador no pasa al estado RFC será eliminado del directorio. El IETF, tras su aprobación por parte del IESG, es el responsable de la publicación del RFC. Los RFC son las notas de trabajo para la comunidad que desarrolla e investiga en Internet

4.3.9.1 Estándares de Internet

Los estándares propuestos, provisionales, y los protocolos estándar figuran en el **"Internet Standards Track" ("Seguimiento de estándares de Internet")**. El seguimiento de estándares es controlado por el *IESG ("Internet Engineering Steering Group")* del IETF. Cuando un protocolo alcanza el estado de estándar, se le asigna un número de estándar (STD). El propósito del STD es indicar claramente que RFC's describen estándares de Internet. Los números STD referencian múltiples RFC's cuando la especificación de un estándar está repartida entre varios documentos. A diferencia de los RFC's, donde el número se refiere a un documento específico, los números STD no cambian cuando un estándar es actualizado. Sin embargo, los STD carecen de número de versión ya que todas las actualizaciones se hacen a través de RFC's y los RFC's son únicos. De este modo, para especificar sin ambigüedades a que estándar se refiere uno, el número de estándar y todos los RFC's que incluye deberían ser mencionados. Por ejemplo, el DNS ("Domain Name System") tiene el STD 13, y se describe en los RFC's 134 y 1035. Para referenciar un estándar, se debería usar una forma como "STD-13/RFC-1034/RFC-1035". Para una descripción de los procedimientos para estándares, remitirse al *RFC 1602 -- Los procedimientos para estándares de Internet - Revisión 2*. Para el seguimiento de algunos estándares, el status del RFC no siempre contiene suficiente información como para ser útil. Por ello se le añade un *descriptor de aplicabilidad*, dado bien en la forma de STD 1 en un RFC separado; este descriptor lo dan particularmente los protocolos de encaminamiento. En este documento se hacen referencias a RFC's y número STD, ya que constituyen la base de todas las implementaciones de protocolos TCP/IP. Cuatro estándares de Internet son de particular importancia:
STD 1 - Estándares de protocolo oficiales en Internet. Este estándar da el estado y el status de cada estándar o protocolo de Internet, y define los significados atribuidos a cada estado o status. El IAB suele emitirlo aproximadamente cada trimestre.
STD 2 - Números asignados de Internet. Este estándar lista los número asignados actualmente y otros parámetros de protocolos en la pila de protocolos de Internet. Es emitido por IANA ("Internet Assigned Numbers Authority").
STD 3 - Requerimientos de host. Este estándar define los requerimientos para el software de Internet del host (con frecuencia a través de referencias a RFC's importantes). El estándar aparece dividido en dos partes: el *RFC 1122 - Requerimientos para hosts en Internet - de la capa de comunicaciones* y el *RFC 1123 - Requerimientos para hosts en Internet - de aplicación y soporte*.
STD 4 - Requerimientos de pasarela. Este estándar define los requerimientos para el software de pasarelas. Su RFC es el 1009.

V.-SINCRONIA

5.1 CONCEPTOS BÁSICOS

5.2 JERARQUÍA DIGITAL PLEOSINCRONA PDH

5.2.1 INTRODUCCION

Es una estructura de jerarquía digital asumida por el ITU-T, antiguamente CCITT, en 1987, que permite el intercambio de información entre países con diferentes estándares. Hay diferentes procedimientos de multiplexado en Europa y en EE.UU.
En Europa:

- Señal digital básica a 64Kbps.
- Primer nivel jerárquico a 2,048Kbps (equivalente a 30 canales telefónicos).
- Segundo nivel jerárquico a 8Mbps (equivalente a 120 canales telefónicos).
- Tercer nivel jerárquico a 34Mbps (equivalente a 480 canales telefónicos).
- Cuarto nivel a 140Mbps (equivalente a 1,920 canales telefónicos).

En EE.UU.:

- DS0 nivel digital 0 a 64Kbps.
- DS1 (T1) nivel digital 1 a 1,544Kbps (equivalente a 24 canales telefónicos).
- DS-1C (T1C) nivel digital 1º a 3,152Kbps (equivalente a 48 canales telefónicos).
- DS2 (T2) nivel digital 2º a 6,312Kbps (equivalente a 96 canales telefónicos).
- DS3 (T3) nivel digital 3º a 44Mbps (equivalente a 672 canales telefónicos).

Ambas obtenidas por la multiplexación síncrona de trenes básicos de 64Kbps. Cada una de estas jerarquías exige en cuanto a sincronización una correcta temporización en ambos extremos para demultiplexar adecuadamente las señales.

5.2.2 DESVENTAJAS DE LA PDH

- La estructura de trama de las centrales hecha por entrelazamiento de octetos a 64Kbps es síncrona, por tanto el empleo de la justificación para adoptar temporización se vuelve innecesario.
- El entrelazamiento de bits hace que canales a 64Kbps. pertenecientes a un tramo de tráfico sólo se puedan bifurcar hasta que se desmultiplexa a nivel de multiplex primario.
- Los canales de n 64Kbps que no se puedan incluir bajo el multiplex primario no se pueden tramitar de ninguna otra forma por la red.
- La información de mantenimiento no esta asociada a vías completas de tráfico, sino a enlaces individuales, por lo cual el procedimiento de mantenimiento para una vía completa es complicado.

5.2.3 SINCRONIZACION

En todo sistema de transmisión digital, la sincronización debe garantizarse en tres niveles diferentes; para transmisión de datos estos niveles son bit, carácter y mensaje. Para transmisión PCM (Modulación de Pulsos Codificados) los niveles son: bit, intervalo de tiempo y trama. Para transmisión de datos existen 2 técnicas de enfrentar la sincronización: Transmisión asíncrona: Cuando los datos viajan por el canal sin una velocidad fija, es decir que el tiempo que transcurre desde la transmisión de un dato, hasta la transmisión del próximo dato es variable. Transmisión síncrona: En este caso los datos son transmitidos a una velocidad fija de bits, por una línea que mantiene viva aún cuando no se esté enviando información. En los sistemas PCM la transmisión es siempre síncrona pues el receptor deriva su propia temporización de la señal entrante, mientras los alineamientos de intervalo y de trama se obtienen utilizando un formato predeterminado. En general se puede decir que muchas de las ventajas de una red digital de telecomunicaciones, son

sólo factibles en una arquitectura de red síncrona. Sin embargo es difícil que todas las temporizaciones de la red tengan la misma frecuencia instantánea.

5.3 JERARQUÍA DIGITAL SINCRONA SDH

5.3.1 INTRODUCCION

SDH es una alternativa de evolución de las redes de transporte, que nace debido al acelerado crecimiento de las actuales redes de transmisión, demanda de nuevos servicios y aparición de nuevos operadores de red. SDH satisface las exigencias de flexibilidad y calidad que requiere un mercado que esta continuamente en cambio. Además de esto, SDH beneficia también a las empresas operadoras en cuanto a la optimización de su rentabilidad, reducción de costos de operación, mantenimiento y facilidad de supervisión. La SDH nace como una solución a la PDH.

5.3.2 CARACTERISTICAS

- Nuevas topologías de red especialmente en la parte de acceso.
- Acceso directo a afluentes de baja velocidad sin tener que demultiplexar toda la señal que viene a alta velocidad, como ocurre con la PDH.
- Facilidad de multiplexación y demultiplexación.
- Mejor capacidad de operación, administración y mantenimiento.
- Adopción de canales auxiliares estandarizados.
- Estandarización de interfaces.
- Fácil crecimiento hacia velocidades mayores, en la medida que lo requiera la red.
- Implementación de sistemas con estructura flexible que pueden ser utilizados para construir nuevas redes (incluyendo LAN, MAN, ISDN).

5.3.3 DESCRIPCION DE LA SDH

La existencia de diversas jerarquías digitales (la Europea y la Americana), hacen que cuando el tráfico sobrepasa las fronteras nacionales, haya necesidad de efectuar conversiones generalmente costosas para llevar la señal a otro país. Esto y las desventajas de PDH forzaron a crear una jerarquía digital que proporcionara un estándar mundial unificado que a su vez ayude a que la administración de la red sea más efectiva y económica. Además satisface las demandas de nuevos servicios y más capacidad de transmisión, por parte de los usuarios. Aparte de ser un estándar mundial y ofrecer un método de multiplexación síncrona, SDH involucra un concepto muy importante: el de red estratificada en capas.

5.3.3.1 ESTRUCTURA BÁSICA DE SDH

SDH trabaja con una estructura básica según lo define la CCITT. Esta estructura es llamada trama básica, la cual tiene una duración de 125 microsegundos, y corresponde a una matriz de 9 filas y 270 columnas, cuyos elementos son octetos de 8 bits; por lo tanto la trama tendrá:

19 940*8 000 = 155 520 Kbps

y como su duración es de 125 microsegundos, o sea que se repite 8,000 veces por segundo, su velocidad binaria será:

19 940*8 000 = 155 520 Kbps

Esta trama básica recibe el nombre de STM_1 **(STM_1 = Synchronous Transport Module 1, Modulo de Transporte Síncrono de Nivel 1)**.

En la trama se distinguen tres áreas:

Tara de Sección (Section OverHead).
Punteros de AU (AU pointer).
Carga Útil (PayLoad).

5.3.3.2 CONTENEDOR VIRTUAL (VC)

Para que un tributario pueda entrar a formar parte de la carga útil de un STM_1 previamente debe ser **empacado adecuadamente**, para ello se procesa con el fin de convertirlo en un contenedor virtual (VC: Virtual Container). Este VC es una señal síncrona en frecuencia con el STM_1 y ocupara un determinado lugar entre la sección de carga útil de la trama.

5.3.3.3 VELOCIDADES BINARIAS EN SDH

Las velocidades de bit para los niveles más altos de las jerarquías SDH van de acuerdo al nivel N del Modulo de Transporte Síncrono (STM). Según la recomendación G.707 del CCITT estas velocidades son mostradas en la tabla 27:

Nivel	Señal	Velocidad	Velocidad Real
1	STM_1	155.520 x 1	= 155.520Mbps
4	STM_4	155.520 x 4	= 622.080Mbps
16	STM_16	155.520 x 16	= 2,488.320Mbps

Tabla 27

A diferencia de la jerarquía digital pleosíncrona, aquí la velocidad del STM_N se obtiene multiplicando la velocidad del modulo básico STM_1, por N, donde N es un entero.

5.3.3.4 TECNICA DE PUNTEROS

En la red síncrona todos los nodos y multiplexores SDH están controlados por un reloj muy estable. Sin embargo pueden surgir perdidas de sincronismo en alguna parte de la red o puede ser necesario efectuar algún ajuste en los puntos donde el tráfico traspasa las fronteras nacionales. Esta tarea de ajustar el sincronismo, se realiza mediante los punteros. Estos indican la posición en que comienza una carga útil. Como cada octeto de una trama STM, tiene un número que lo identifica, el puntero indica uno de tales números, y es donde se encontrara el primer octeto de la carga útil asociada a dicho puntero. De esta forma la carga útil puede por así decirlo "**flotar**" en una trama STM, pues siempre su posición estará indicada por el puntero.

5.3.3.5 SDH: RED ESTRUCTURADA EN CAPAS

Una red basada en SDH proporciona los medios para transportar los contenedores entre diversos puntos, para cargar y descargar contenedores de los STM_1 y para transferir contenedores de un medio de transporte a otro (STM_N). Estas acciones determinan las funciones básicas que se deben realizar en una red SDH. En los puntos de acceso a la red se ensamblan los VC adecuados a la señal a transmitir, una vez conformado el VC debe ser transportado a través de la red, durante el viaje del VC por la red SDH puede presentarse el caso en que un VC o varios deben ser descargados del STM_1 o también casos en que deban ser cargados en los STM_1. En su recorrido por la red, el VC pasara por diferentes rutas y con diferentes velocidades.

5.3.3.6 EQUIPOS PARA SDH

Los equipos necesarios en una red SDH son los siguientes:

- Multiplexor Terminal.
- Multiplexor Add-Drop.
- Multiplexor Cross-Connet.

La función del **multiplexor terminal** es combinar las funciones de interfaz, ensamblado y desensamblado de los diversos paquetes. El **cross-connet** realiza el enrutamiento del tráfico entre nodos de la red y se puede clasificar de acuerdo al tipo de VC que intercambie y al nivel jerárquico

de las señales. Se pueden clasificar en 3 tipos: los que realizan intercambio a nivel VC-4 o a nivel superior, los que realizan intercambio a nivel del VC de orden inferior y los que son combinaciones de los anteriores.

5.3.3.7 GESTIÓN SDH

La SDH es la primera tecnología que incluye dentro de las normas que la soportan, algunas dedicadas a especificar las facilidades de gestión bajo las directrices de la **TMN (telecomunication Management Network)**. La TMN se concibe como una red superpuesta a la red de telecomunicaciones, que interactúa con ella a través de interfaces normalizadas en ciertos puntos y obtiene información que le permite monitorear y controlar su operación. Su objetivo es dar soporte par a gestión a los operadores de la red. A continuación se muestra una organización de las normas del CCITT sobre SDH:
ESTÁNDARES SDH G.707-G.708-G.709
ARQUITECTURA DE RED: G.803 (Arquitectura de Redes) G.804
EQUIPOS G.781, G.782, G.783 (multiplexores) G.987 (Interópticas) G.958 (Sistemas de Línea) G.SDX 1,2,3 (Cross-connet) Reg.750 (Arquitectura de sistemas de radio)
GESTIÓN DE RED DE RED M.3010 G.803 (Arquitectura de Redes) G.773 (Int. Q) G.804 G.774 (Modelo inform)

5.3.3.8 RED DE GESTIÓN SDH

Los aspectos de gestión de la red SDH, se tratan básicamente en la recomendación G de la UIT. En el modelo de organización de gestión se distinguen 2 componentes principales:

- Sistemas de operaciones o dispositivos de mediación **SO/DM**.
- Elementos de red **ER**.

La diferencia entre estos dos componentes radica en el tipo de función que soportan. Los SO/MO realizan funciones del sistema de operaciones: procesar la información, controlar las funciones de gestión dentro de las cuales hay funciones básicas, funciones de red y funciones de servicio. Realizan funciones de mediación que garantizan la comunicación entre el SO y el ER como control de las comunicaciones, conversión de protocolos, manejo de datos, transferencia de primitivas. Los ER realizan funciones de elemento de red sustentando los servicios de transporte de red basados en SDH, como multicanalización, regeneración, transconexión. Se comunican con el SO a fin de ser supervisados y controlados.

5.3.3.9 FORMATO DE LA TRAMA

La señal básica el SDH es STM (Synchronous Transport Module) la cual consiste en 2,430 bytes que puede ser visto como una matriz de 270 columnas por 9 filas la cual es transmitida a 155Mbps y es equivalente a la señal STS-3 de Sonet, figura 170.

Esta dividido principalmente en dos áreas:

- **Payload** (2,349 bytes).-En la cual se transportan las señales de baja tasa de bits.
- **SOH, Section Overhead** (81 bytes).-Contiene características del transporte y soporte de las señales, manejo de operaciones y monitoreo de errores.

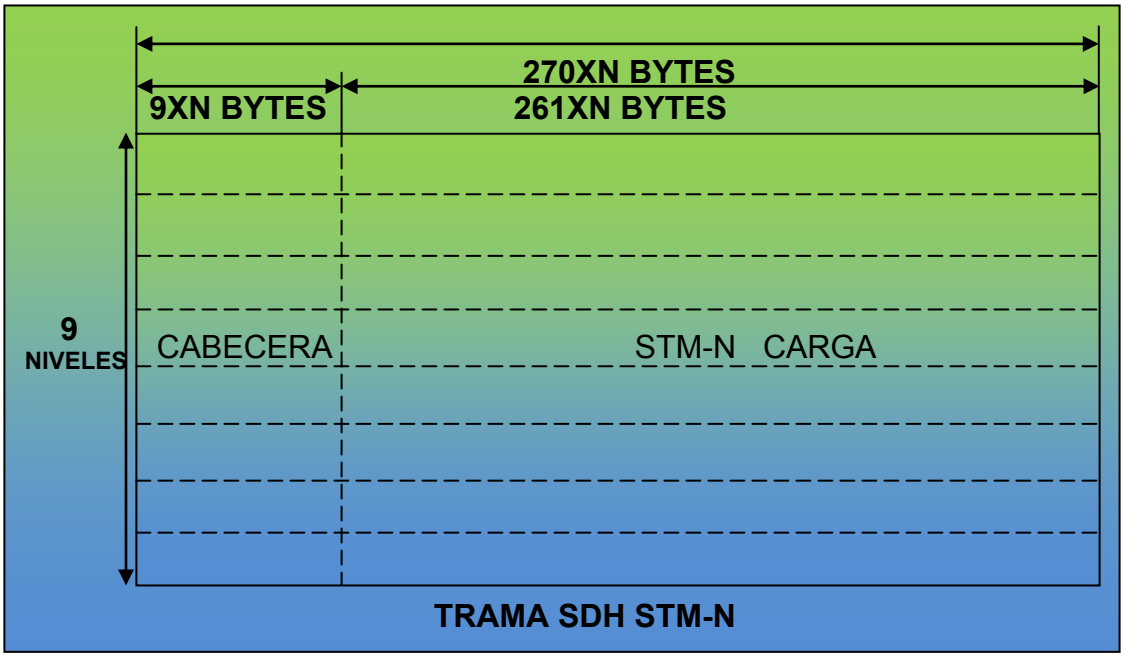


Figura 170 Formato de la trama SDH

5.3.3.10 CONFIGURACION DE UNA RED SDH

Add/Drop multiplexer.-Permiten la inserción y eliminación de la señal SDH
Termimate unit.-Similar al Add/Drop pero esta diseñado para terminar con una señal SDH
Digital cross connet.-Pueden proveer un enlace entre señales STM de distinto nivel
Repeater.-Amplifica la señal SDH, figura 171.

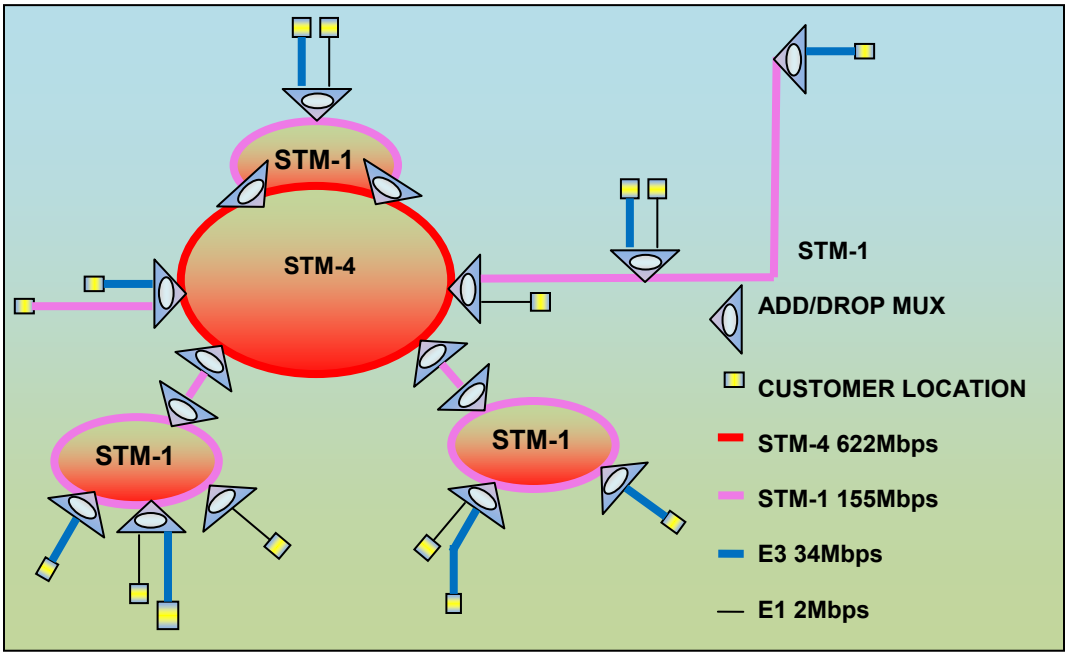


Figura 171 Típica Red SDH

5.3.3.11 ALGUNOS BENEFICIOS DE SDH

- Soporta una gran variedad de servicios (voz, datos, video, etc.).
- Redes más sencillas (simplificadas).
- Como es un estándar, los equipos de transmisión de distinta manufactura pueden trabajar sin problemas, brindando libertad de escogencia.
- Facilita el trabajo entre las jerarquías de transmisión europeas y americanas.
- Puede servir como transporte a servicios de alta velocidad.

VI.-LAS NUEVAS REDES CONVERGENTES

6.1 ATM

6.1.1 INTRODUCCION

ATM **(Asynchronous Transfer Mode, Modo de Transferencia Asíncrono)** es el corazón de los servicios digitales. La actual demanda de aplicaciones relacionadas con información multimedia, como son la videoconferencia, audioconferencia, video bajo demanda **(VoD)** o sistemas colaborativos (pizarras compartidas, teletrabajo, telemedicina, etc.) y su coexistencia con aplicaciones más clásicas (bases de datos, transferencias de ficheros, WWW, etc.), requiere tecnologías de comunicaciones capaces de ofrecer elevadas prestaciones. Estas elevadas prestaciones están directamente relacionadas con la calidad de servicio **(QoS)** y concretamente con conceptos claramente parametrizables como el ancho de banda y la velocidad de transmisión **(throughput)**, el retardo de las transferencias **(delay)**; la variabilidad en el retardo **(jitter)**; la fiabilidad **(reliability)** de las transmisiones; las características de multidifusión a grupos dispersos de usuarios **(multicast)** y la posibilidad de gestionar múltiples clases de servicio o flujos de información en redes multiclass. Para que las nuevas tecnologías en comunicaciones puedan ofrecer estas características es necesario revisar, potenciar y ampliar las actuales arquitecturas, servicios y protocolos de comunicaciones. En los últimos años, las investigaciones en el campo de ATM están dado lugar a importantes propuestas cuyo principal objetivo es ofrecer a las aplicaciones demandadas actualmente algunas o todas las características citadas anteriormente.

Inicialmente propuesto por la Industria de las Telecomunicaciones, rápidamente se ha convertido en la tecnología más promovida dentro de las industrias de Comunicaciones y Computadoras. Las recomendaciones iniciales propuestas por el CCITT en 1988 fueron que, ATM y Sonet formasen la base de la Red Digital de Servicios Integrados de Banda Ancha (B-ISDN), un nuevo estándar en desarrollo para la integración en red de: Datos, Voz, Imagen y Vídeo, a velocidades de transmisión desde 34 Mbps a varios Gigabits por segundo. Emplea el concepto de **Conmutación de Celdas (Cell Switching)**, el cual combina los beneficios de la Conmutación de Paquetes tradicionalmente utilizada en redes de datos, y la Conmutación de Circuitos utilizada en redes de voz. ATM se basa en el concepto de **Conmutación Rápida de Paquetes (Fast Packet Switching)** en el que se supone una fiabilidad muy alta a la tecnología de transmisión digital, típicamente sobre fibra óptica, y por lo tanto la no necesidad de recuperación de errores en cada nodo. Ya que no hay recuperación de errores, no son necesarios los contadores de número de secuencia de las redes de datos tradicionales, tampoco se utilizan direcciones de red ya que ATM es una tecnología orientada a conexión, en su lugar se utiliza el concepto de **Identificador de Circuito o Conexión Virtual (VCI)**.

El tráfico con tasa de bit o **Velocidad Binaria Constante (CBR)**, por ejemplo voz PCM o vídeo no comprimido, tradicionalmente es transmitido y conmutado por redes de conmutación de circuitos o Multiplexores por División en el Tiempo (TDM), que utilizan el **Modo de Transmisión Síncrono (STM)**. En STM, los multiplexores por división en el tiempo dividen el ancho de banda que conecta dos nodos, en contenedores temporales de tamaño pequeño y fijo o ranuras de tiempo **(Time Slots)**. Cuando se establece una conexión, esta tiene estadísticamente asignado un **slot** (o varios). El ancho de banda asociado con este slot está reservado para la conexión haya o no transmisión de información útil. Una pequeña cantidad de ancho de banda para control, se utiliza para la comunicación entre los conmutadores, de forma que estos conocen los slots que tiene asignados la conexión. Esto se conoce como direccionamiento implícito. El conmutador receptor sabe a que canales corresponden los slots y por lo tanto no se requiere ningún direccionamiento adicional. Este procedimiento garantiza la permanente asignación de un ancho de banda durante el tiempo que dura la llamada, así como un tiempo de latencia pequeño y constante. En contraste, los datos son normalmente transmitidos en forma de tramas o paquetes de longitud variable, lo que se adecua bien a la naturaleza de ráfagas de este tipo de información. Sin embargo, este mecanismo de transporte tiene retardos impredecibles, la latencia tiende a ser alta y en consecuencia la

conmutación de paquetes no es adecuada para tráfico con tasa de bit constante como la voz. Tampoco la conmutación de circuitos se adecua para la transmisión de datos, ya que si se asigna un ancho de banda durante todo el tiempo para un tráfico en ráfagas, se derrocha mucho ancho de banda cuando este no se utiliza. ATM ha sido definido para soportar de forma flexible, la conmutación y transmisión de tráfico multimedia comprendiendo datos, voz, imágenes y video. En este sentido, ATM soporta servicios en modo circuito, similar a la conmutación de circuitos, y servicios en modo paquete, para datos, figura 172.

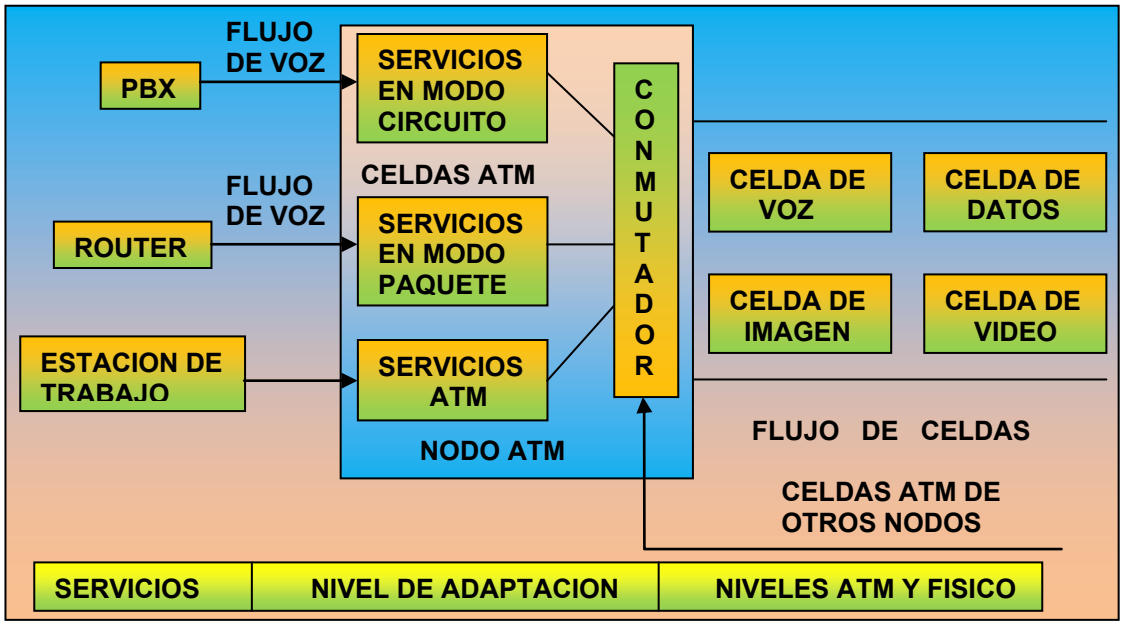


Figura 172 Funcionamiento de un Nodo ATM

Sin embargo, a diferencia de la conmutación de circuitos, ATM no reserva slots para la conexión. En su lugar, una conexión obtiene slots o celdas, sólo cuando está transmitiendo información. Cuando una conexión está en silencio no utiliza slots o celdas, estando estas disponibles para otras conexiones. Con esta idea en mente, se decidió que la unidad de conmutación y transmisión fuese de tamaño fijo y longitud pequeña. Esta unidad es conocida como **Celda**, y tiene una longitud de 53 bytes divididos en 5 de cabecera y 48 de información o carga útil. Esta celda es quien viene a sustituir al Time Slot o contenedor del STM figura 173.

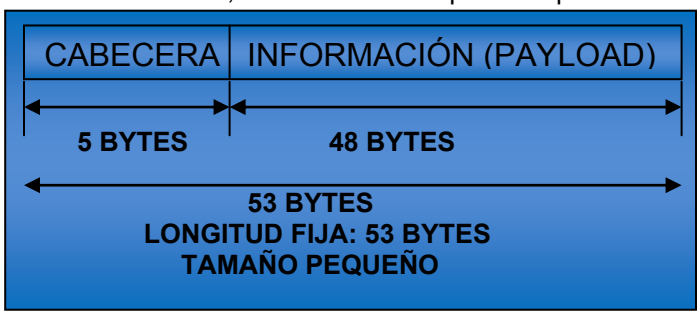


Figura 173 Celda ATM

Las celdas pequeñas y de longitud constante son ventajosas para tráfico con tasa de bit constante (voz, video) y son muy útiles en general ya que permiten un tiempo de latencia muy bajo, constante y predecible, así como una conmutación por hardware a velocidades muy elevadas. También, en el caso de pérdida de celdas por congestión o corrupción, la pérdida no es muy grande siendo en muchos casos remediable o recuperable. De hecho, el tráfico de voz y video, no es muy sensible a pequeñas pérdidas de información, pero si es muy sensible a retardos variables, sucediéndole lo contrario al tráfico de datos. En una red ATM, donde las celdas no están reservadas sino asignadas bajo demanda, el conmutador receptor no puede determinar por adelantado a que canal corresponde cada celda. La Celda ATM a diferencia del Time Slot en STM, debe transportar la identificación de la conexión a la que pertenece, de esta forma no existirán

Celdas vacías ya que serán utilizadas por conexiones pendientes. Esta es una diferencia fundamental del ATM frente al STM. La cabecera presente en cada celda, consume aproximadamente un 9.5% del ancho de banda, siendo este el precio que hay que pagar por la capacidad para disponer de ancho de banda bajo demanda, en lugar de tenerlo permanentemente reservado y eventualmente desperdiciado.

La adopción de una cabecera de 5 bytes ha sido posible, porque no se realiza recuperación de errores en los nodos intermedios, tampoco se emplean direcciones válidas a nivel de toda la red, tales como la dirección MAC en Ethernet o IP en redes tipo TCP/IP, figura 174.

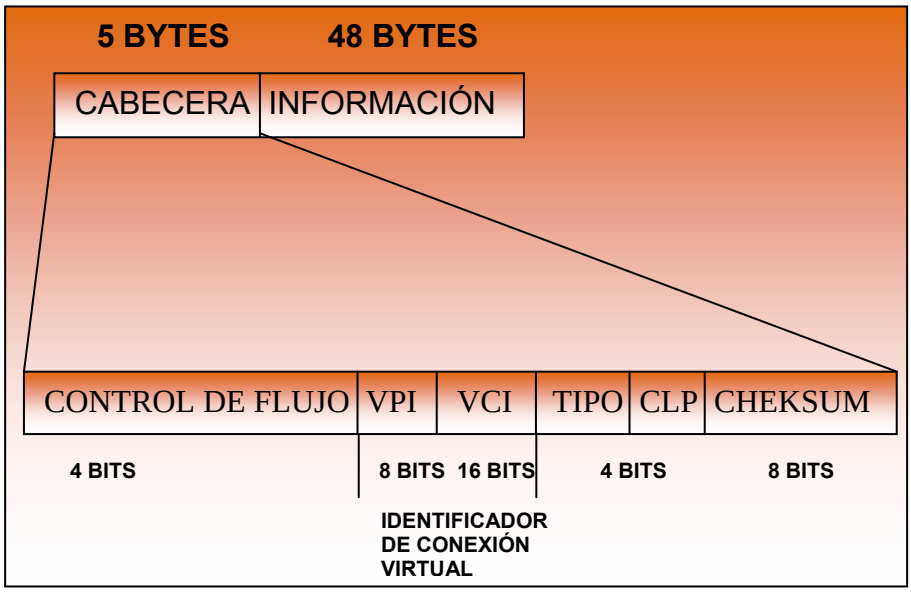


Figura 174 Cabecera de la Celda ATM

Al igual que en las redes de conmutación de paquetes (X.25 y Frame Relay), la tecnología ATM está **Orientada a Conexión**. Esto significa que antes de que el usuario pueda enviar celdas a la red, es necesario realizar una llamada y que esta sea aceptada para establecer una conexión virtual a través de la red. Durante la fase de llamada un **Identificador de Conexión Virtual (VCI)** es asignado a la llamada en cada nodo de intercambio a lo largo de la ruta figura 175.

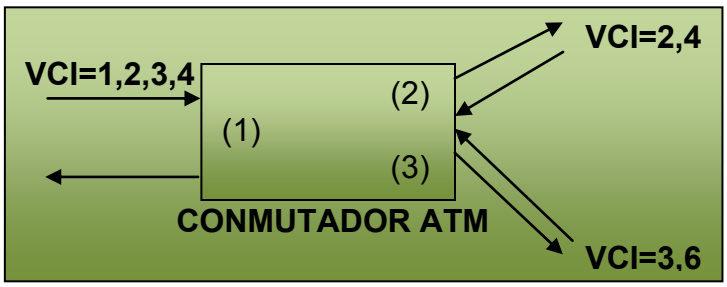
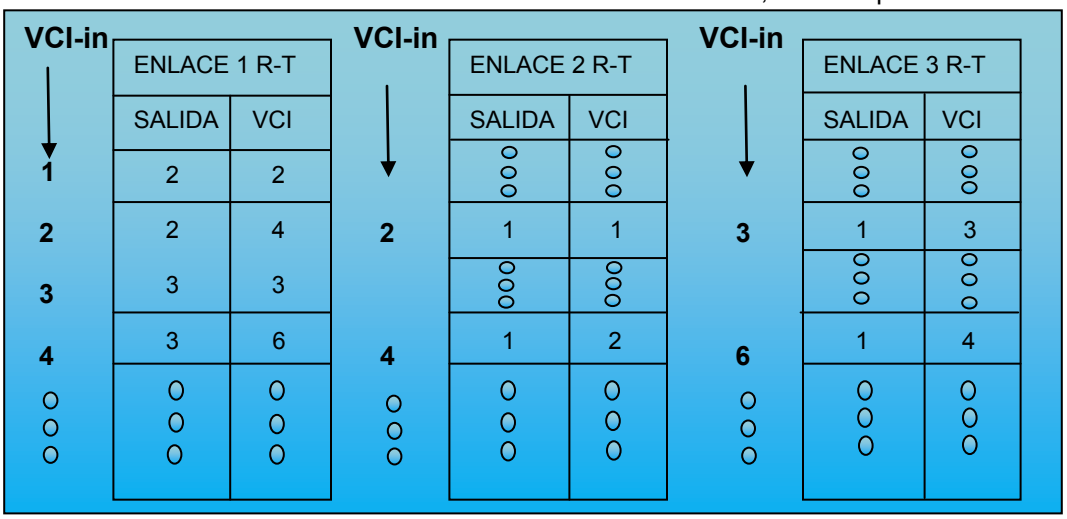


Figura 175 Identificador de conexión virtual (VCI)

El identificador asignado, sin embargo, sólo tiene significado a nivel del enlace local, y cambia de un enlace al siguiente según las celdas pertenecientes a una conexión pasan a través de cada conmutador ATM. Esto significa, que la información de encaminamiento (**routing**) transportada por cada cabecera puede ser relativamente pequeña. Asociado con cada enlace o puerto entrante del conmutador ATM, hay una tabla de encaminamiento que contiene el enlace o puerto de salida y el nuevo VCI que va a ser utilizado en correspondencia a cada VCI entrante figura 176. De este modo el encaminamiento de celdas en ambas direcciones a lo largo de la ruta es extremadamente rápido, ya que consiste en una simple operación de consulta en una tabla. Como resultado, las celdas procedentes de cada enlace pueden ser conmutadas independientemente a velocidades muy altas. Esto permite el uso de arquitecturas de conmutación paralelas y circuitos de alta velocidad hasta Gigabits, cada uno operando a su máxima capacidad. Celdas procedentes de diferentes fuentes son multiplexadas juntas de forma estadística a efectos de conmutación y transmisión. Un conmutador ATM podría describirse como una caja que mantiene en su interior una gran cantidad de Ancho de Banda, siendo este recurso cedido o recuperado dinámicamente

según el aumento o disminución de las necesidades. En este sentido, se dice que ATM



proporciona Ancho de Banda bajo demanda.

Figure 176 Tablas de encaminamiento

6.1.2 PROTOCOLO ATM

El protocolo ATM consiste de tres niveles o capas básicas, ver figura 177. **La primera capa** llamada **capa física (Physical Layer)**, define las interfaces físicas con los medios de transmisión y el protocolo de trama para la red ATM, es responsable de la correcta transmisión y recepción de los bits en el medio físico apropiado. A diferencia de muchas tecnologías LAN como Ethernet, que específica ciertos medios de transmisión, (10 base T, 10 base 5, etc.) ATM es independiente del transporte físico. Las celdas ATM pueden ser transportadas en redes Sonet, SDH, T3/E3, TI/EI o aún en módems de 9600 bps. Hay dos subcapas en la capa física que separan el medio físico de transmisión y la extracción de los datos:

- La subcapa **PMD (Physical Medium Depedent)**.-Tiene que ver con los detalles que se especifican para velocidades de transmisión, tipos de conectores físicos, extracción de reloj, etc., Por ejemplo, la tasa de datos Sonet que se usa, es parte del PMD.
- La subcapa **TC (Transmission Convergence)**.-Tiene que ver con la extracción de información contenida desde la misma capa física. Esto incluye la generación y el **Chequeo del Header Error Corrección (HEC)**, extrayendo celdas desde el flujo de bits de entrada y el procesamiento de celdas **idles** (falsas) y el reconocimiento del límite de la celda. Otra función importante es intercambiar **Información de Operación y Mantenimiento (OAM)** con el plano de administración.

La segunda capa es **la capa ATM**. Ella define la estructura de la celda y como las celdas fluyen sobre las conexiones lógicas en una red ATM, esta capa es independiente del servicio. El formato de una celda ATM es muy simple. Consiste de 5 bytes de cabecera y 48 bytes para información. Las celdas son transmitidas serialmente y se propagan en estricta secuencia numérica a través de la red. El tamaño de la celda ha sido escogido como un compromiso entre una larga celda, que es muy eficiente para transmitir largas tramas de datos y longitudes de celdas cortas que minimizan el retardo de procesamiento de extremo a extremo, que son buenas para voz, video y protocolos sensibles al retardo. A pesar de que no se diseñó específicamente para eso, la longitud de la celda ATM acomoda convenientemente dos Fast Packets IPX de 24 bytes cada uno.

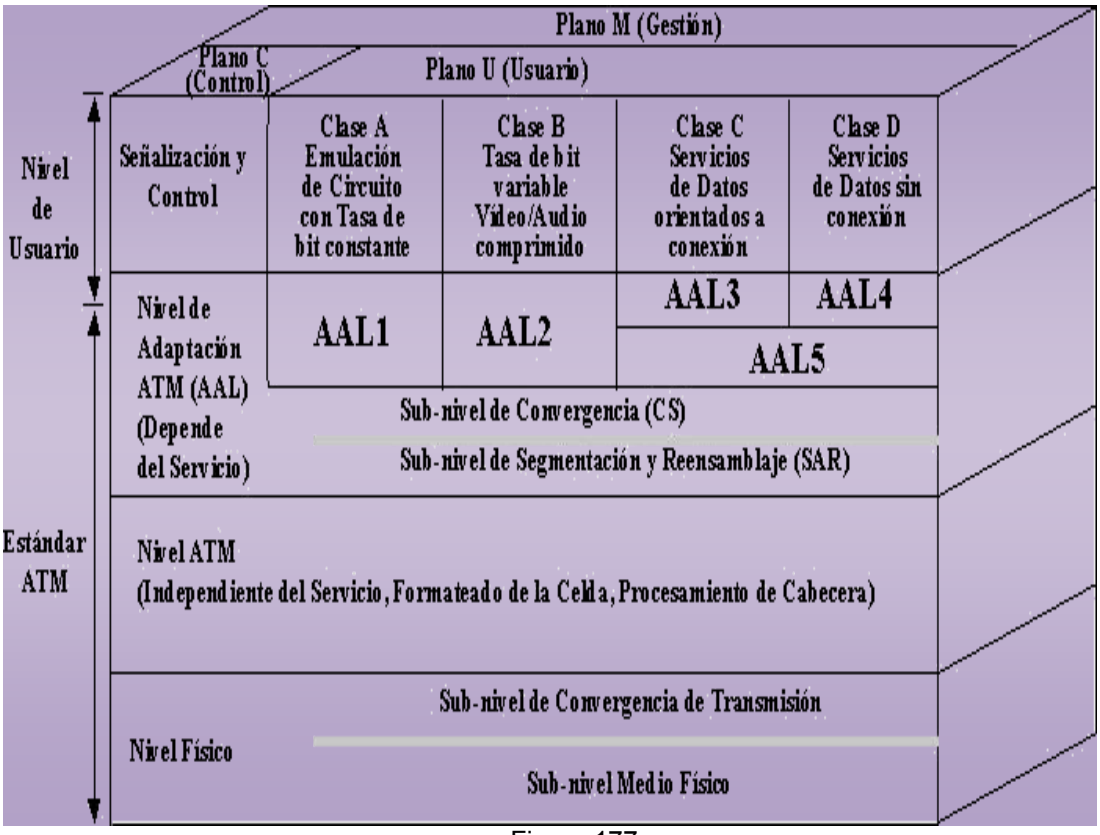


Figura 177

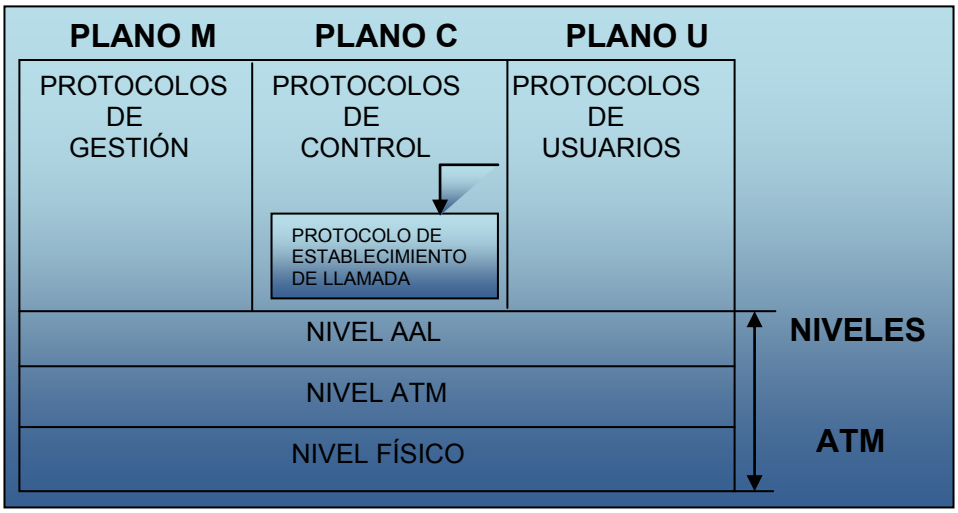


Figura 178

Los comités de estándares han definido dos tipos de cabeceras ATM: los **User-to-Network Interface (UNI)** y la **Network to Network Interface (NNI)**, figura 179. La UNI es un modo nativo de interfaz ATM que define la **Interfaz entre el Equipo del Cliente (Customer Premises Equipment)**, tal como hubs o routers ATM y la red de área ancha ATM (ATM WAN). La NNI define la interfaz entre los nodos de la redes (los switches o conmutadores) o entre redes. La NNI puede usarse como una interfaz entre una red ATM de un usuario privado y la red ATM de un proveedor público **(carrier)**. Específicamente, la función principal de ambos tipos de cabeceras de UNI y la

NNI, es identificar las **Virtual Paths Identifiers (VPI)** y los **Virtual Circuits o Virtual Channels (VCI)** como identificadores para el ruteo y la conmutación de las celdas ATM.

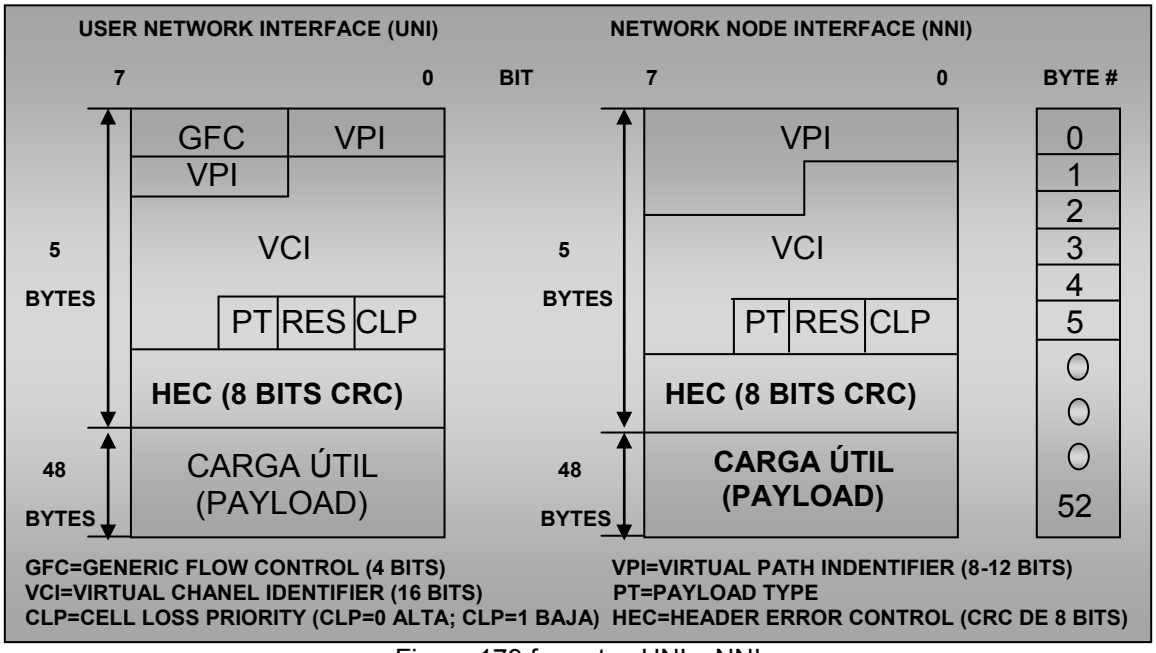


Figura 179 formatos UNI y NNI

El campo **Control de Flujo Genérico (GFC)** tiene significado únicamente en este enlace y se incluye para asignar prioridades a las diferentes celdas, dependiendo del tipo de información que transportan, y que estas sean colocadas en diferentes colas de salida según su prioridad. No está presente dentro de la red, y en su lugar se amplia el campo VPI. El campo **Tipo de Carga Útil (PT)** se utiliza para permitir que las celdas de los planos C y M, se distingan de las celdas conteniendo información de Usuario, y también para informar de la existencia de congestión. El protocolo AAL-5 utiliza un bit del campo PT para indicar el **Fin del Mensaje (EOM)** de una trama AAL-5 (PT=0x1). El bit **CLP** permite que las celdas tengan una de dos prioridades: alta (CLP=0) y baja (CLP=1). Debido a que un conmutador ATM opera por multiplexación estadística de sus entradas, es posible que múltiples entradas compitan por una misma salida, dando lugar a que un buffer temporal se desborde en un enlace de salida de un nodo ATM. El bit CLP se utiliza para marcar aquellas celdas que en caso de congestión se puedan descartar primero. El campo HEC es un CRC de 8 bits para detección de errores en la cabecera (sólo), especialmente si el direccionamiento es correcto. Si falla, la celda es descartada. Si es correcto, se puede proceder inmediatamente a la conmutación. Celdas vacías también son descartadas y se caracterizan por que su VPI/VCI es cero.

La tercer capa es **la ATM Adaptation Layer (AAL)**. La AAL juega un rol clave en el manejo de múltiples tipos de tráfico para usar la red ATM, y es dependiente del servicio. Específicamente, su trabajo es adaptar los servicios dados por la capa ATM a aquellos servicios que son requeridos por las capas más altas, tales como **Emulación de Circuitos (circuit emulation)**, vídeo, audio, Frame Relay, etc. La AAL recibe los datos de varias fuentes o aplicaciones y las convierte en los segmentos de 48 bytes. Cinco tipos de servicio AAL están definidos. La capa de Adaptación de ATM yace entre el ATM layer y las capas más altas que usan el servicio ATM. Su propósito principal es resolver cualquier disparidad entre un servicio requerido por el usuario y atender los servicios disponibles del ATM layer. La capa de adaptación introduce la información en paquetes ATM y controla los errores de la transmisión. La información transportada por la capa de adaptación se divide en cuatro clases según las propiedades siguientes:

- Que la información que esta siendo transportada dependa o no del tiempo.
- Tasa de bit constante/variable.
- Modo de conexión.

La capa de adaptación se divide en dos subcapas:

- **Capa de Convergencia (CS, Convergence Sublayer)**.-En esta capa se calculan los valores que debe llevar la cabecera y los payloads del mensaje. La información en la cabecera y en el payload depende de la clase de información que va a ser transportada.
- **Capa de Segmentación y Reensamblaje (SAR, Segmentation and Reassembly)**.-Esta capa recibe los datos de la capa de convergencia y los divide en trozos formando los paquetes de ATM. Agrega la cabecera que llevara la información necesaria para el reensamblaje en el destino.

La figura 180 aporta una mejor comprensión de ellas. La subcapa CS es dependiente del servicio y se encarga de recibir y paquetizar los datos provenientes de varias aplicaciones en tramas o paquete de datos longitud variable.

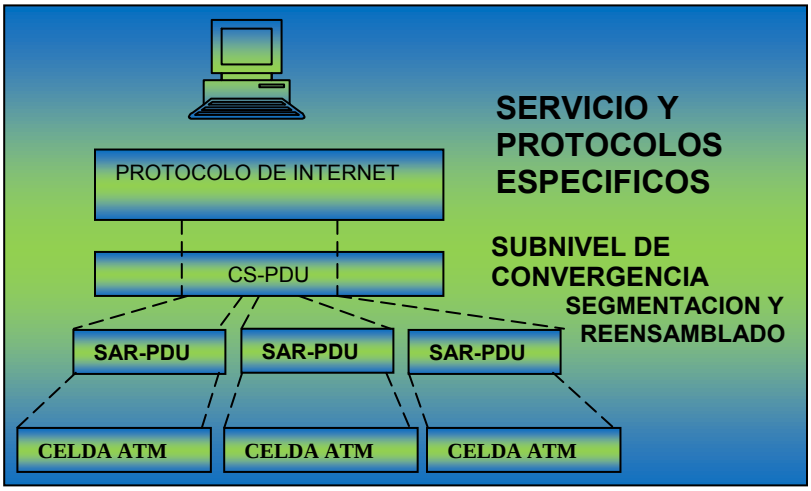


Figura 180

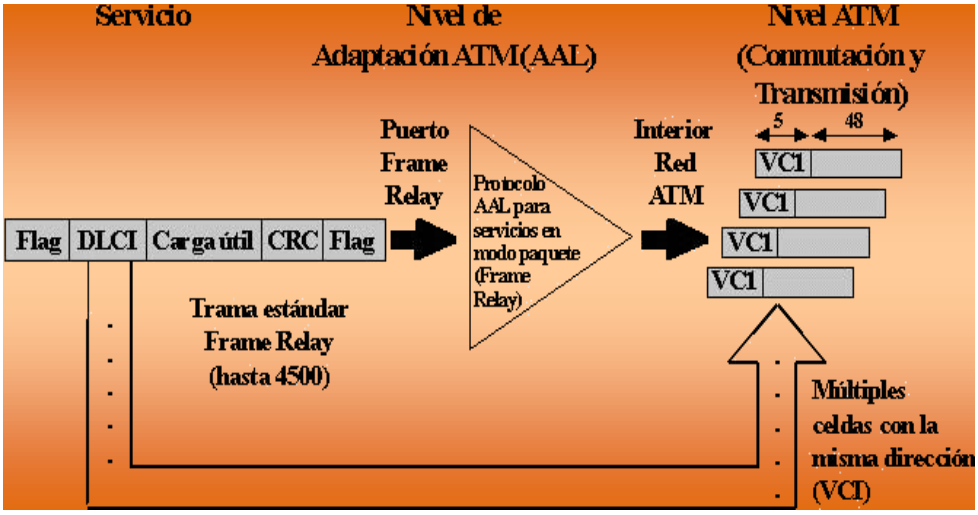


Figura 181

Estos paquetes son conocidos como **CS – PDU, Convergence Sublayer Protocol Data Units** Luego, la subcapa recibe los SAR CS - PDU, los reparte en porciones del tamaño de la celda ATM para su transmisión. También realiza la función inversa (reemsamblado) para las unidades de información de orden superior. Cada porción es ubicada en su propia unidad de protocolo de segmentación y reemsable conocida como **SAR – PDU. Segmentation And Reamssembler Protocol Data Unit**, de 48 bytes. Finalmente cada SAR - PDU se ubica en el caudal de celdas ATM con su header y trailer respectivos.

- **AAL-1**.-Se usa para transferir tasas de bits constantes que dependen del tiempo. Debe enviar por lo tanto información que regule el tiempo con los datos. AAL-1 provee recuperación de errores e indica la información con errores que no podrá ser recuperada. Capa de convergencia las funciones provistas a esta capa difieren dependiendo del

servicio que se previo. Provee la corrección de errores. Capa de segmentación y reensamblaje en esta capa los datos son segmentados y se les añade una cabecera.

- **AAL-2**.-Se usa para transferir datos con tasa de bits variable que dependen del tiempo. Envía la información del tiempo conjuntamente con los datos para que esta pueda recuperarse en el destino. AAL-2 provee recuperación de errores e indica la información que no puede recuperarse. Capa de convergencia esta capa provee para la corrección de errores y transporta la información del tiempo desde el origen al destino. Capa de segmentación y recuperación el mensaje es segmentado y se le añade una cabecera a cada paquete. La cabecera contiene dos campos. Número de secuencia que se usa para detectar paquetes introducidos o perdidos. El tipo de información es:
  - BOM, comenzando el mensaje.
  - COM, continuación de mensaje.
  - EOM, fin de mensaje o indica que el paquete contiene información de tiempo u otra.

  El payload también contiene dos de campos:
  - Indicador de longitud que indica el número de bytes válidos en un paquete parcialmente lleno.
  - CRC que es para hacer el control de errores.
- **AAL-3**.-Se diseña para transferir los datos con tasa de bits variable que son independientes del tiempo. AAL-3 puede ser dividido en dos modos de operación:
  - **Fiable**.-En caso de pérdida o mala recepción de datos estos vuelven a ser enviados. El control de flujo es soportado.
  - **No fiable**.-La recuperación del error es dejado para capas más altas y el control de flujo es opcional.

  Capa de convergencia la capa de convergencia en AAL 3 es parecida al ALL 2. Esta subdividida en dos secciones:
  - Parte común de la capa de convergencia. Esto es provisto también por el AAL-2 CS. Añade una cabecera y un payload a la parte común. **Capa de segmentación y reensamblaje** en esta capa los datos son partidos en paquetes de ATM. Una cabecera y el payload que contiene la información necesaria para la recuperación de errores y reensamblaje se añaden al paquete. La cabecera contiene 3 campos:
  - Tipo de segmento que indica que parte de un mensaje contiene en payload. Tiene uno de los siguientes valores:
    - **BOM**.-Comenzando el mensaje.
    - **COM**.-Continuación de mensaje.
    - **EOM**.-Fin del
    - **+** mensaje.
    - **SSM**.-Mensaje único en el segmento.
  - Número de secuencia usado para detectar una inserción o una pérdida de un paquete.
  - Identificador de multiplexación.-Este campo se usa para distinguir datos de diferentes comunicaciones que ha sido multiplexadas en una única conexión de ATM.

    El payload contiene dos campos:
    - Indicador de longitud que indica el número de bytes útiles en un paquete parcialmente lleno.
    - CRC es para el control de errores.
- **AAL-4**.-Se diseña para transportar datos con tasa de bits variable independientes del tiempo. Es similar al AAL3 y también puede operar en transmisión fiable y no fiable. AAL-4 provee la capacidad de transferir datos fuera de una conexión explícita. AAL 2, AAL 3/4 y AAL 5 manejan varios tipos de servicios de datos sobre la base de tasas de bits variables tales como **Switched Multimegabit Data Service (SMDS)**, Frame Relay o tráfico de redes de área local (LAN). AAL 2 y AAL 3 soportan paquetes orientados a conexión, figura 177. Los servicios han sido clasificados de acuerdo con tres criterios, figura 182

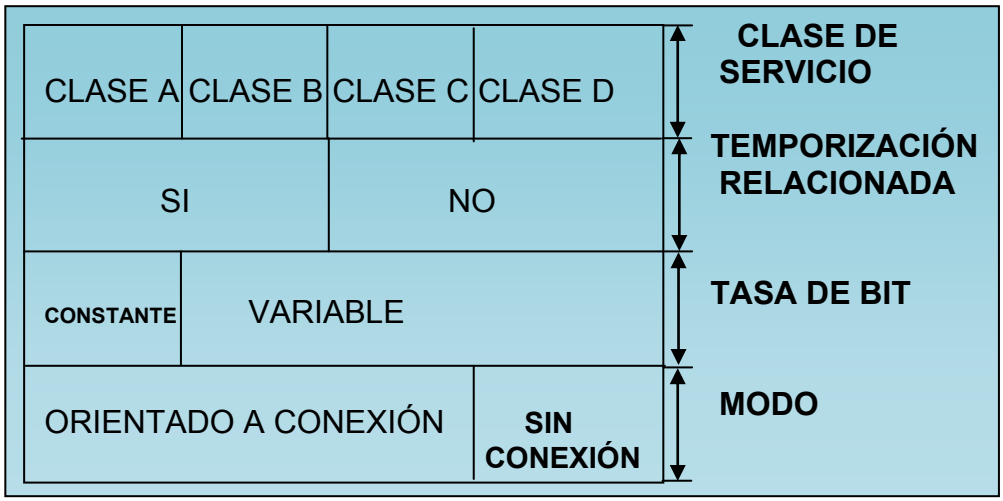


Figura 182 Servicios proporcionados por ATM

La existencia de una temporización relacionada entre los usuarios origen y destino (por ejemplo voz). La tasa de bit, o velocidad binaria asociada con la transferencia (constante/CBR o variable/VBR). El modo de conexión (con conexión o sin conexión).

Los servicios en clase A y B están orientados a conexión y existe una temporización relacionada entre los usuarios origen y destino. La diferencia entre las dos clases, es que la clase A proporciona un servicio con tasa de bit constante, mientras que en la clase B la tasa de bit es variable. Un ejemplo de uso de la clase A, es la transferencia de un flujo constante de bits asociada con una llamada de voz, por ejemplo a 64Kbps (Similar a un canal B en ISDN). La clase A es también conocida, como Emulación de Circuito Conmutado. Un ejemplo de uso de la clase B, es la transmisión de un flujo de bits variable asociado con video comprimido. Aunque el video produce tramas a velocidad constante, un codec de video produce tramas conteniendo una cantidad variable de datos comprimidos.

Las clases C y D no tienen temporización relacionada entre el origen y el destino. Ambas proporcionan servicios en modo paquete, con velocidad binaria variable entre origen y destino. La clase C está orientada a conexión y la clase D es sin conexión. Para realizar las funciones anteriores, el nivel AAL está dividido en dos subniveles:

- El Subnivel de Convergencia (CS), que realiza las funciones de convergencia entre el servicio ofrecido al usuario y el proporcionado por el nivel ATM.
- El Subnivel de Segmentación y Reensamblado (SAR), que realiza las funciones de ensamblado/segmentación de los datos de origen para colocarlos en el campo de información de la celda y la correspondiente función de desensamblado/reensamblado en el destino.

Asociada con cada clase de servicio está un tipo de **Punto de Acceso al Servicio (SAP)** y un protocolo asociado. Clase A tiene un SAP de tipo 1, clase B de tipo 2 y así sucesivamente, figura 183.

Los cuatro tipos o clases de servicios utilizan los 48 bytes del campo de carga útil en cada celda de forma diferente, pudiendo opcionalmente contener un campo de hasta 4 bytes para adaptación ATM.

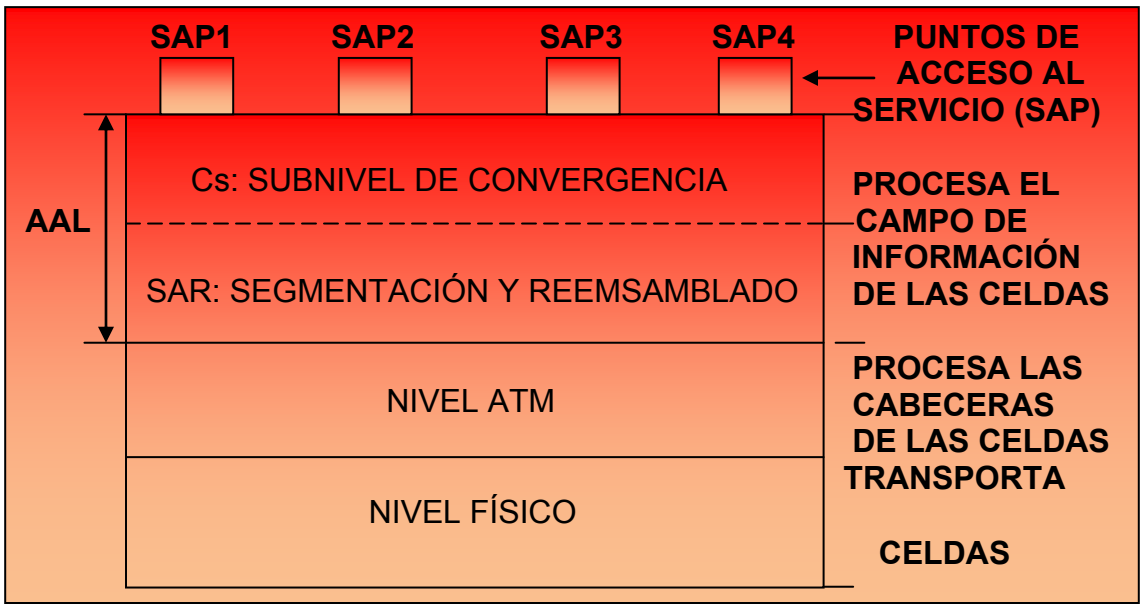


Figura 183 Puntos de Acceso al Servicio (SAP's)

Velocidad Binaria Constante (CBR)

En este tipo de servicio, el protocolo de AAL1 se esfuerza en mantener un flujo con tasa de bit constante entre los SAP's de origen y destino (entrega sincronizada). La velocidad binaria está en el rango de pocos Kbps, por ejemplo para voz comprimida, a decenas de Mbps, por ejemplo en video no comprimido. Sin embargo, la velocidad binaria acordada debe ser mantenida, incluso con pérdidas ocasionales de celdas o variaciones en el tiempo de transferencia de las mismas. Este servicio se asemeja al proporcionado por el sistema telefónico existente, ya que garantiza un número fijo de celdas por unidad de tiempo para la aplicación. El formato del campo de información de la celda, conocido como segmento, incluye un **Número de Secuencia (SN)** de 4 bits y un campo asociado de 4 bits utilizado para **Proteger el Número de Secuencia (SNP)** contra errores de un bit figura 184.

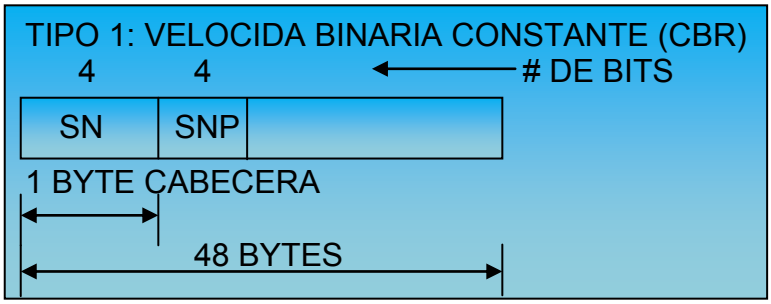


Figura 184 Formato del segmento CBR

De esta forma es posible detectar pérdidas de segmentos. Las pérdidas de celdas se superan de forma acordada; por ejemplo, insertando segmentos ficticios en el flujo entregado. Variaciones en el retardo de transferencia de celdas, son compensadas mediante buffereado en el destino; la salida de segmentos correspondiente a una llamada, únicamente se comienza después de que se hayan recibido un número predeterminado de segmentos, este número viene determinado por la velocidad binaria del usuario. Valores típicos son 2 segmentos a velocidades de Kbps y 100 segmentos a velocidades de Mbps. Claramente este retardo se sumará al retardo de ensamblaje/desensamblaje ya identificado. El uso de buffereado en destino también proporciona un modo sencillo de superar cualquier pequeña variación entre las velocidades binarias en origen y destino; por ejemplo si cada uno está basado en diferente reloj. Una solución mejor, es que la red proporcione los relojes de entrada y salida, normalmente extraídos de la codificación en línea del flujo de bits transmitido.

Velocidad Binaria Variable (VBR)

En este tipo de servicio, aunque exista una temporización relacionada entre los SAP's fuente y el destino, la velocidad de transferencia real de información, puede variar durante la conexión. Como con el CBR, el segmento contiene un Número de Secuencia de 4 bits para la recuperación de celdas pérdidas figura 185.

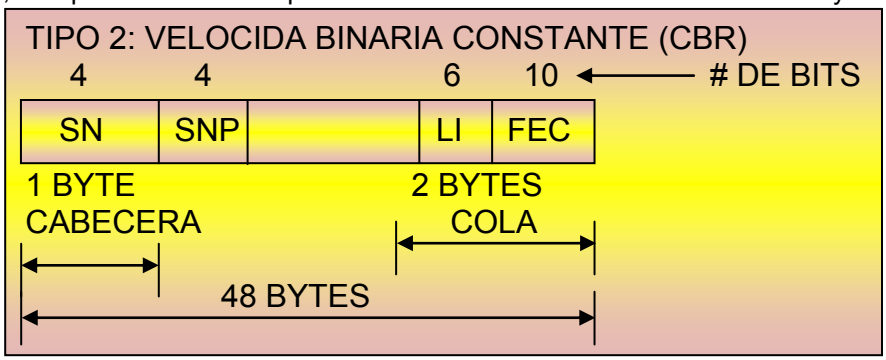


Figura 185 Formato del segmento VBR

El campo de **Tipo de Información (IT)** indica, o bien la posición relativa del segmento con relación al mensaje remitido, por ejemplo, una trama comprimida procedente de un video codec, o si el segmento contiene información de temporización, o de otro tipo. Los tres tipos de segmento con relación a la información posicional son: **comienzo de mensaje (BOM), continuación de mensaje (COM) y fin de mensaje (EOM)**. Debido al tamaño variable de las unidades de mensaje remitidas, un **Indicador de Longitud (LI)** en la cola del segmento indica el número de bytes útiles en el último segmento. Finalmente, el campo **FEC** habilita la detección y corrección de errores.

Datos Orientados a Conexión

El protocolo AAL3/4 proporciona dos tipos de servicios para la transferencia de datos: uno **Orientado a Conexión (CO)** y otro **Sin Conexión (CLS)**. La diferencia entre los dos es que con el primero, antes de que cualquier dato pueda ser transmitido, debe establecerse una Conexión Virtual. El servicio orientado a conexión tiene dos modos operacionales: asegurado y no asegurado, cada uno soportando envíos de **Unidades de Datos del Servicio (SDU)** o mensajes de usuario, de tamaño fijo o variable. El modo asegurado proporciona un servicio fiable que garantiza que todas las SDU's son entregadas sin errores y en la misma secuencia con que fueron remitidas. Este es un servicio similar al proporcionado por una red de conmutación de paquetes tipo X.25 y, para proporcionar este servicio, todos los segmentos generados por el subnivel CS están sujetos a procedimientos de control de flujo y recuperación de errores. Para el modo no asegurado, los segmentos son transmitidos sobre la base del mejor intento; esto es, cualquier segmento corrompido es simplemente descartado y se deja a los niveles de protocolo de usuario superar esta eventualidad. El Tipo de Segmento (ST) indica si es el primero (BOM), continuación (COM), último (EOM), o el único (SSM) de una SDU remitida figura 186.

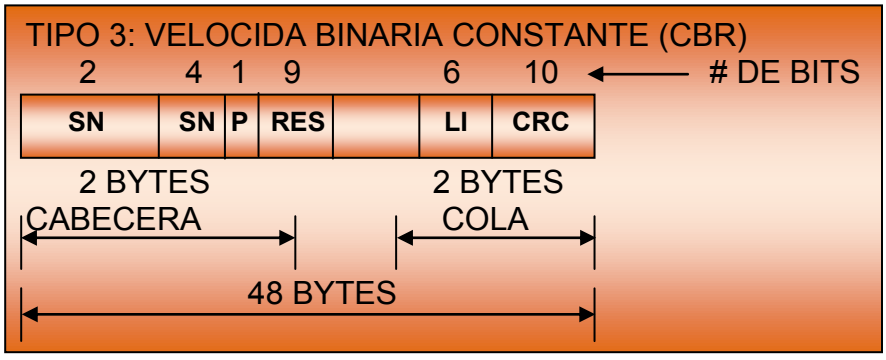


Figura 186 Formato del segmento con conexión

El **Número de Secuencia (SN)** se emplea para detectar segmentos perdidos o duplicados y también para control de flujo. Un único bit de **Prioridad (P)** permite que los segmentos tengan uno de dos niveles de prioridad. En la cola, el **Indicador de Longitud (LI)** indica el número de bytes

útiles en el segmento y el **CRC**-10 está presente para la detección y eventual corrección de errores. Claramente LI solamente tiene significado en el último segmento de una SDU o si es el único segmento.

Lo segmentos generados por el subnivel SAR del protocolo AAL3/4, son compatibles con la especificación IEEE 802.6 utilizada en el servicio SMDS. El funcionamiento del protocolo del **Subnivel de Convergencia (CS)** se puede describir mejor, considerando el formato de los mensajes o Unidades de Datos del Protocolo (CS-PDU) que genera, en relación con la SDU remitida por el usuario, y el modo que esta es transportada por el subnivel SAR figura 187.

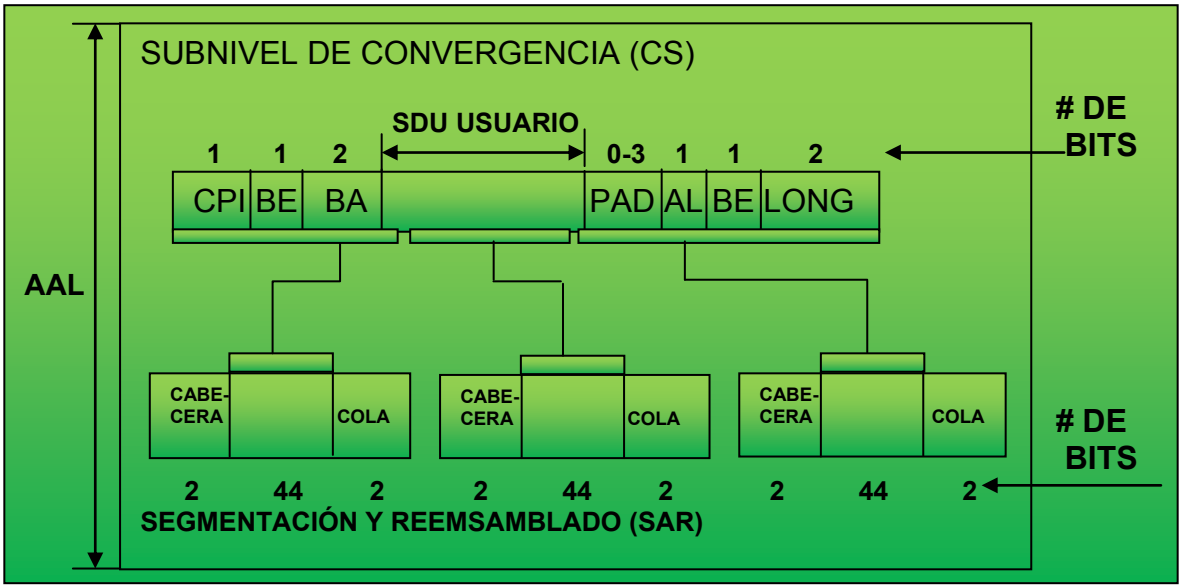


Figura 187 Protocolos AAL

Los campos de cabecera y cola añadidos por el protocolo CS en origen a la SDU remitida, se utilizan para habilitar al protocolo CS receptor la detección de SDU's pérdidas o malformadas. El **Identificador de Protocolo CS (CPI)**, se utiliza para identificar el tipo de protocolo CS que está siendo utilizado. El identificador **comienzo-fin (BE)** es un número de secuencia módulo 256 y se repite en cola para añadir capacidad de reacción. Se utiliza para asegurarse que las SDU's son entregadas en la misma secuencia en la que se remitieron. El campo de **Asignación de Buffer (BA)** se inserta en la cabecera para ayudar al protocolo CS receptor, a reservar una cantidad de memoria suficiente (buffer) para contener una SDU completa. En la cola, el **campo de relleno (PAD)** se utiliza para hacer que el número de bytes de la unidad de datos del protocolo CS, sea un múltiplo de 4 bytes. De forma similar, el byte de **Alineamiento (AL)** es un byte de relleno para hacer que la cola tenga 4 bytes. El campo de **longitud (Length)** indica la longitud total de la unidad de datos del protocolo completa y entonces ayuda al receptor a detectar cualquier SDU malformada.

Datos sin Conexión

El servicio de datos sin conexión es probablemente el primero que va a ser soportado. Está pensado, por ejemplo, para la interconexión de LAN's a alta velocidad. A diferencia del tipo 3 no hay señalización de llamada ni terminación, en su lugar conexiones permanentes o semipermanentes están siempre establecidas entre cada par de SAP's origen y destino. Aparte de esto, los dos servicios utilizan los mismos formatos en el Subnivel de Convergencia CS y segmento, figura 188. Sin embargo, con los servicios sin conexión, el campo **RES (reservado)** está sustituido por el **Identificador del Mensaje (MID)**. Normalmente celdas relacionadas con diferentes tramas estarán en tránsito en cualquier instante, el campo MID se utiliza para habilitar al subnivel SAR de destino relacionar cada celda recibida a su SDU específica. La utilización del MID permite la multiplexación de múltiples sesiones en una misma conexión virtual VPI/VCI.

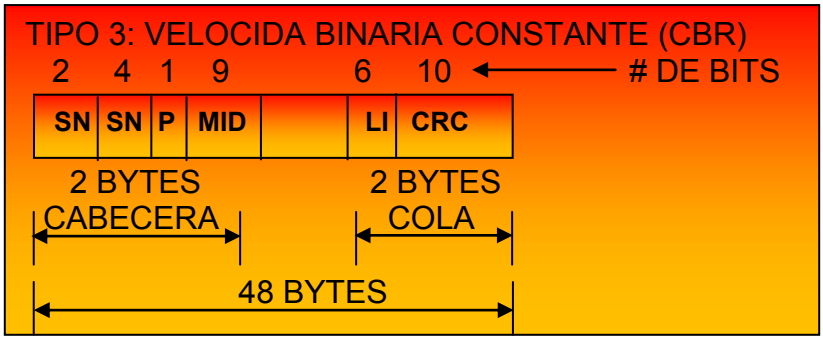
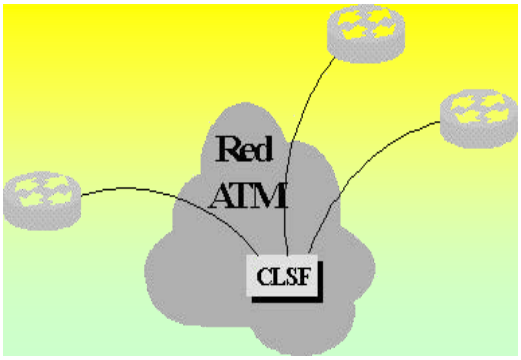


Figura 188 Formato del segmento sin conexión

Como se puede deducir de lo anteriormente expuesto, la pregunta que surge con los servicios sin conexión es como el origen determina el VPI correcto a utilizar, con sólo las direcciones origen y destino (digamos MAC) de la trama remitida (SDU). Claramente, esto implica un nivel de encaminamiento por encima del fundamental proporcionado por el nivel ATM. Una solución para esto, es que el nivel ATM en cada nodo envíe todas las celdas a un nodo dado de destino conocido, en el cual está localizada una utilidad de encaminamiento de tramas, la cual conoce el camino o ruta a todas las direcciones de destino figura 189.



Conexiones virtuales a un Servidor de la Función de Sin Conexión (CLSF)

Figura 189 Servicios sin conexión ATM

Usualmente esta información será introducida por el gestor de la red y para minimizar la sobrecarga se deben utilizar varios de estos nodos. Estos son conocidos como **Servidores de la Función Sin Conexión (CLSF)**. Otro tema con este tipo de servicio se relaciona con el asignamiento de MID's. Está claro que, si dos nodos fuente utilizan simultáneamente el mismo MID y las tramas son para el mismo destino, el procedimiento de reensamblado no funcionará. En consecuencia, para superar esta eventualidad, el CLSF puede también cambiar el MID durante su operación de retransmisión, si este ya está en uso en un nodo de destino dado.

Mecanismos de Control en Redes ATM

Es necesario, sin duda alguna, tener una idea completa de lo que el manejo de información significa en redes ATM. El control de tráfico es un tema práctico que surge en la implementación del ATM. Para cualquier tipo de red de comunicaciones con recursos compartidos la capacidad de vigilar y regular el flujo de tráfico es muy importante. Si no hubiera control de tráfico, no habría restricciones en cuanto a la demanda de recursos compartidos, como buffers, ancho de banda o procesadores, y esto puede reducir seriamente las salidas de la red, así como su eficiencia. El control de tráfico es necesario tanto para conservar la calidad de los servicios hacia el usuario, como para asegurar la eficiencia en el uso de los recursos de la red. Los mecanismos de tráfico de control se deben implementar dentro de sistemas de conmutación y las capas superiores del protocolo de red. Es evidente que el papel del control de tráfico es esencial, y así pues uno de los grupos de trabajo del Forum ATM se dedica al manejo de tráfico. Este grupo está conduciendo sus esfuerzos hacia un nuevo servicio de **Bit Rate Disponible (ABR)** y un esquema relacionado al control de tráfico. Una herramienta que puede ser utilizada para el control de tráfico es la técnica de trayectoria virtual. Agrupando varios canales virtuales dentro de una trayectoria virtual, tanto el control de admisión de llamada y del parámetro de uso de la red, se reducen a ser sólo el tráfico agregado a una trayectoria virtual que se debe manejar.

Principios Básicos de Control de Tráfico

El control de tráfico es el conjunto de acciones que lleva a cabo la red para evitar condiciones de congestionamiento. El control de congestionamiento son los movimientos que lleva a cabo la red para minimizar la intensidad, área y duración del congestionamiento. Esta puede ser provocado por ciertas condiciones de flujo de tráfico y fallas dentro de la red. Las siguientes funciones brindan a las redes ATM un marco de trabajo para el manejo y control del tráfico.

- **Manejo de Recursos de Red (NRM)**.-Se usa para la distribución de recursos de la red con la finalidad de separar diferentes flujos de tráfico de acuerdo a las características de servicios.
- **Control de Admisión de Conexión (CAC)**.-Son aquellas funciones que ejecuta la red durante la instalación de una llamada para determinar si una VCC/VPC (Virtual Channel Conection/Virtual Path Conection) se acepta o rechaza. Los esquemas del CAC son medidas de prevención para evitar que el valor promedio de cargas en el enlace no alcancen la capacidad máxima y el UPC pueda regular el valor pico. Dichos esquemas permiten al usuario mantener un mínimo de salida. La prioridad de programación de tiempos en un nodo puede incrementar el uso de una manera significativa si los requerimientos van de 1ms a unas décimas de ms por nodo. En este caso los servicios que toleran retrasos pueden utilizar buffers más grandes que aquellos que no toleran retrasos.
- **Controles de Retroalimentación**.-Son los movimientos que ejecutan tanto la red como los usuarios para regular el tráfico en redes ATM de acuerdo al estado de la red.
- **Control de Parámetro de Uso/Red, (UPC/NPC)**.-Vigila y controla el tráfico en términos de oferta y validez de tráfico de la conexión ATM, a nivel de acceso del usuario y de la red. Su propósito principal es el de proteger la red de malos funcionamientos, que puedan afectar las conexiones existentes.
- **Control de Prioridad**.-Permite al usuario asignar diferentes prioridades de flujo de tráfico utilizando el bit CLP en el header de la celda. En una red congestionada, las celdas de baja prioridad son eliminadas.
- **Técnica de Codificación por Niveles**.-Permite llevar a cabo ajustes en la velocidad dependiendo de los recursos disponibles.
- **Formación de Tráfico**.-Es un mecanismo que altera las características de una corriente en una VCC o VPC para lograr la modificación apropiada para esas características de tráfico.
- **Manejo Rápido de Recursos**.-Opera en función del tiempo de la propagación de retraso de una conexión ATM completa.

El control por retroalimentación y los esquemas de UPC/NPC deben ejecutarse mediante el mecanismo de **leaky-bucket**, o un mecanismo de espaciamiento como el **algoritmo virtual de programación en tiempo (VSA)**. Estos mecanismos fortalecen el ancho de banda promedio y el factor de explosión de una fuente. Una forma de implementar el leaky-bucket es mediante el uso de tokens, es decir cuando una celda llega entra en un paquete; en caso de que éste esté lleno, las celdas se eliminan. Para entrar a la red, una celda debe primero obtener un permiso o token. Si no tiene token, la celda debe esperar en el paquete hasta que se genere un nuevo token en un **token-pool (recipiente de tokens)**. Los tokens se generan a un valor determinado correspondiente al valor promedio de conexión. Si el número de tokens en el token-pool sobrepasa un valor de umbral predeterminado entonces se interrumpe el proceso de generación de tokens. Este valor de umbral corresponde a la capacidad de explosión de la transmisión. Los dos casos extremos es cuando se cuenta con un buffer de entrada y cuando no se dispone de él. El primer caso un gran número de celdas deberán eliminarse. En el segundo las celdas pueden estar sujetas a un tiempo de espera muy grande, sin permitir que recobren un flujo asíncrono. Mediante la elección adecuada del tamaño de paquete de entrada, se puede hallar un punto medio entre estos dos extremos. Uno de los factores más importantes para llevar a cabo un control de congestionamiento eficiente es el lapso de duración del congestionamiento, por ejemplo, para el caso de llamadas telefónicas el rango de cien a cientos de milisegundos. Para el caso de video, el valor pico puede ser de varios segundos, pero estas medidas se llevaron a cabo sin tener en consideración el control de flujo y el control de congestionamiento. Los resultados de los esquemas de control de congestionamiento

reactivo, como son el CAC y el UPC, en el congestionamiento interno merecen ser objetos de un estudio más a fondo. Si el periodo de congestionamiento es menor a la duración del retraso de un viaje redondo, un control de flujo reactivo no es aplicable. Por otro lado, si el tiempo de congestionamiento es extenso la situación debe controlarse mediante la ayuda del CAC y el UPC en conjunto con el OAM para garantizar un QoS mínimo.

Para poder llevar a cabo un control de tráfico es necesario tener la capacidad de detectar situaciones de congestionamiento en los elementos de conmutación y ajustes del valor de transmisión del nodo fuente. Un elemento de conmutación que esté congestionado puede modificar el valor **PTI (Payload Type Identifier)** en el header de una celda para indicar el congestionamiento. Pero el uso de la información de congestionamiento depende del usuario. El trabajo que se hace en aquellas celdas que se pierden o insertan, así como las que tienen error se puede hacer mediante el uso de los canales del **OAM (Operation And Manteinance)**, sin embargo, puede resultar difícil utilizar el desempeño de la información con el fin de ajustar los parámetros de flujo dinámicamente. El único canal mediante el cual se puede transferir un estado de sobrecarga hacia el nodo destino es el campo PTI. El nodo destino puede retroalimentar la información a la fuente a través del canal OAM o bien mediante celdas especiales. Las capacidades del lazo de retroalimentación permiten la inserción de información a lo largo del VC o VP para ciertas operaciones. Esto es posible mediante la inserción de una celda OAM, en cualquier punto accesible en la conexión virtual, con instrucciones en la carga para que regrese a uno o dos puntos fáciles de identificar a lo largo de la conexión. La retroalimentación de celdas se usa para funciones en el control de tráfico de congestionamiento. Por ejemplo durante periodos de congestionamiento excesivo, un switch detectado mediante este mecanismo, puede empezar la eliminación de celdas ATM con el propósito de maximizar la entrega del tráfico de más alta prioridad. Durante estos periodos, los switches también pueden transmitir una notificación de congestionamiento ya sea en adelanto o en atraso a lo largo de la transmisión VPC/VCC. Una vez que se ha recibida la notificación, los nodos toman acción para solucionar el congestionamiento. La técnica de codificación por niveles y sus variantes han sido propuestas para servicios de audio y video. Permiten el ajuste del valor de código dependiendo de los recursos disponibles. El concepto principal de este tipo de codificación es dividir el video y audio en niveles. Cada nivel contiene información jerárquica, como por ejemplo resolución de información; ya sea alta, media o baja. El nivel adecuado se puede seleccionar en la inicialización considerando del ancho de banda disponible, y se pueden añadir o eliminar niveles durante el tiempo que dure la conexión. Como se ha mencionado ya, el servicio básico de las redes ATM es el transporte secuencial de celdas extremo a extremo. El servicio se inicia con una solicitud de conexión virtual hecha por el usuario. El **Grado de Servicio (GOS)** pertenece al ofrecimiento de tráfico en términos de probabilidad de bloqueo a nivel de admisión o rechazo de conexiones. En caso de ser aceptada, las celdas que se acarrean sufren dos tipos de deterioros dentro de la red; retraso y pérdida.

Calidad del Servicio, QoS

El QoS, calidad del servicio, se encarga del grupo de parámetros tales como retraso de celdas, variación en el retraso y pérdida de celdas; los cuales pertenecen a los deterioros observados por el tráfico acarreado. La red es la responsable de mantener el nivel de QoS esperado por los usuarios. Dentro de la clasificación de servicios, existen requerimientos específicos para cada una de las cuatro clases. Una clase la cual carezca de un QoS específico, sin requisitos de retraso de celda o pérdida de celda puede auxiliarse por una red ATM. Sin diferencias de tráfico en las clases, la red puede necesitar el manejo de los requisitos más estrictos para el tráfico. El desempeño de la red en cuanto a QoS se refiere a los parámetros que miden la habilidad de la red para proporcionar servicios entre los usuarios. Así como el QoS es importante a los usuarios en el punto de acceso al servicio, el desempeño de la red se define desde el punto de vista del proveedor de red a puntos dentro de la red. Al nivel de llamada, los parámetros de funcionamiento de la red pueden incluir el retraso en la inicialización de la conexión, retraso en la liberación de la conexión y probabilidades de bloqueo. Al nivel de celda, los parámetros del trabajo realizado por la red incluyen los índices de error de celdas, pérdida de celdas, inserción errónea retraso extremo a extremo y variación del retraso.

Debido a que el ATM está orientado tanto a conexión como a celdas, es posible encontrar problemas de congestionamiento en ambos niveles; conexiones y celdas. A nivel conexión, los procesadores de llamadas estarán ocupados llevando a cabo intentos infructuosos de llamadas. Mientras, a nivel celdas los enlaces de transmisión se saturan, y los buffers experimentan un sobre flujo de celdas. Por lo tanto, al no tener control de un congestionamiento, esto se manifestará mediante el aumento de bloqueo de llamadas, retraso de celdas, y pérdida de celdas. Los intentos de control de congestionamiento intentan detectar y reaccionar al mismo, y de esta forma decrecer su intensidad, área y duración.

Aislamiento y recursos compartidos

La decisión entre compartir los recursos o el aislamiento entre los flujos de tráfico para la protección del QoS hace difícil el control del tráfico, debido a lo conflictivo de los dos objetivos. Para obtener una ganancia en la eficiencia se multiplexan aquellas conexiones VBR cuyo valor pico total exceda el valor del enlace físico de transmisión, el valor promedio total es menor al del enlace. Si se tienen varias corrientes de tráfico y son independientes, la probabilidad de que su valor instantáneo total exceda el valor del enlace es mínima. Para efectuar la multiplexión con ganancia, razón del valor pico total entre el valor del enlace, se debe mantener un factor de uso alto y maximizar el grado de operaciones compartidas de los recursos de la red. Una de las consecuencias desfavorables de la multiplexión es la posibilidad de que el QoS de una conexión sea afectado por el tráfico de otras conexiones. Por ejemplo, si una corriente llegase a reventar el buffer del multiplexor se puede saturar causando el incremento del retraso de celdas para todas las corrientes. Puede darse el caso de que varias corrientes revienten simultáneamente y ocasionen un sobre flujo en el buffer. La probabilidad de que existan sobre flujos en el buffer o retrasos excesivos de paquete es mayor en cargas grandes. Por lo tanto es conveniente mantener un factor de uso bajo, el cual no es económicamente factible, o en su defecto llevar a cabo el aislamiento de las corrientes de tráfico y de esta forma reducir el efecto de explosión de una de las corrientes en el QoS de otra corriente. Las prioridades son una importante ayuda para el aislamiento o modificación de los efectos que tienen las corrientes. Las prioridades de retraso dictaminan el orden en el cual las celdas que han sido formadas se programan para la transmisión en un enlace compartido; las prioridades de pérdida especifican el lugar que preferentemente se ha de ocupar dentro del buffer compartido.

Niveles de Control

El flujo de tráfico se puede dividir en entidades tales como: llamadas, VPC, VCC, fragmentos (consistentes de celdas consecutivas) y celdas individuales. El control de tráfico consiste en un grupo de mecanismos de control que pueden ser aplicados en diferentes entidades de tráfico de cada nivel. Cada mecanismo de control tiene características en la escala del tiempo. Los mecanismos que operan en celdas individuales son los más rápidos puesto que las decisiones de control dependen únicamente de las condiciones locales dentro de un conmutador. Por ejemplo, la eliminación selectiva de celdas depende del nivel de congestionamiento en los buffers del conmutador. Existen otros mecanismos que trabajan a lo largo de la red en la escala del tiempo de propagación retrasos de extremo a extremo. Estos mecanismos involucran el paso en un sólo sentido de la información entre dos puntos a lo largo de una conexión virtual. Otros mecanismos operan en escalas en el tiempo más grandes; las cuales comprenden intercambio bidireccional de mensajes y repuestas.

Control Preventivo y Control Reactivo

Teniendo en cuenta que ATM es una técnica que se basa en celdas, es posible concebir la idea de que aquellos mecanismos de control de flujo de retroalimentación que se utilizan en redes convencionales se apliquen a redes ATM. Sin embargo, se deben tener en cuenta los siguientes puntos:

- No es propio usar dichos mecanismos en fuentes de tiempo real, de las cuales no se espera por lo general, que la red las pueda controlar.

- La eficacia del control retroalimentado se limita principalmente por el retraso de propagación.
- El tiempo de transmisión de una celda es mucho más pequeño que el tiempo de detección de congestionamiento y el proceso para que la fuente reaccione. Las fuentes de alta velocidad en ATM son capaces de enviar varias celdas adentro de la red antes de que la información de la retroalimentación se pueda propagar a través de la red con el propósito de controlar dichas celdas.

Por lo tanto existe un acuerdo en el que el control de retroalimentación, y de una manera más general cualquier tipo de control reactivo, tendrán usos limitados en redes ATM de altas velocidades, excepto en servicios especializados como el ABR. Se cree que en las redes ATM se prefieren principalmente los métodos preventivos, en vez de los métodos reactivos. Los primeros tratan de evitar el congestionamiento asegurando que las conexiones permanezcan dentro de los límites que la red utilice para alojar los recursos de la misma durante el establecimiento de la conexión. Los métodos preventivos realizan primeramente dos funciones: control de admisión de conexión y el **Control del Parámetro de Uso (UPC)** para la regulación de la cantidad de tráfico que entra a la red. Los métodos reactivos incluyen eliminación selectiva de celdas, indicación explícita de congestionamiento más adelante, y reconfiguración dinámica de ruteo, la cual reacciona con el arranque de congestionamiento.

Control de Flujo

La capacidad de las redes ATM, de Gbps, genera un juego de requisitos para el control de flujo diferente de los mecanismos de control de flujo en el proceso de red TCP, los cuales son desenlaces reactivos. En caso de que el control de flujo trabajara con retroalimentación, al tiempo en que se recibe el mensaje en la fuente, ésta ya envió varios Mbytes de datos dentro del conducto ATM, y de esta forma, agraviando el congestionamiento. De la misma forma cuando la fuente reaccione al mensaje de control de flujo, es probable que el congestionamiento haya disminuido, o bien desaparecido obligando a la fuente a bajar su ritmo, o pararla por completo, innecesariamente. La constante de tiempo de extremo a extremo en el lazo de retroalimentación puede ser tan grande que resulta impráctico el confiar en las conexiones de usuario para la preservación de una red dinámica. La condiciones de congestionamiento en redes ATM se espera que sean extremadamente dinámicas cumpliendo los requisitos de mecanismos de hardware rápidos con el propósito de suavizar el estado estable de la red, esto comprende también la capacidad de la red para lograr este estado estable por sí misma. Entonces una aproximación simple de control reactivo de lazo cerrado (retroalimentado) de extremo a extremo no es suficiente para redes ATM. El acuerdo al que han llegado los investigadores en este campo es el del uso de una aproximación al control de flujo. Se recomienda utilizar una colección de esquemas de control de flujo junto con la asignación y distribución adecuadas de los recursos de las redes, todos unidos tratando de evitar el congestionamiento, para la evaluación y detección tempranas del congestionamiento; vigilando de cerca los paquetes dentro de los conmutadores ATM, y así reaccionar gradualmente hasta que los paquetes alcancen diferentes límites, y de esta forma tener un control en la inyección de la conexión de datos dentro de la red en un UNI cuya velocidad de inyección sea modulada antes de tener que ir hacia una conexión de usuario para conseguir así sofocar la fuente de una manera más drástica. Se trata de llevar a cabo un control de flujo a nivel hardware a altas velocidades, gradualmente, y anticipando las acciones. Los esquemas, basados en las velocidades, que inyectan una cantidad controlada de datos a una velocidad específica la cual está sincronizada con el tiempo de establecimiento de conexión, y automáticamente modular la velocidad teniendo en cuenta a la conexión por sí misma y el congestionamiento que esté sufriendo la red en ese mismo instante. La UNI puede saber el estado en el que se encuentra la red generando una celda de control de flujo, en el momento en el que se deposita una celda en algún nodo de la red debido al congestionamiento; como cuando se empiezan a llenar los paquetes. La UNI puede entonces regular la conexión mediante el cambio de su velocidad de inyección, o notificando a la conexión de usuario con el fin de sofocar la fuente dependiendo del grado y la condición de congestionamiento.

Las acciones más complicadas son las de evaluación y corrección de corrientes que causan congestionamientos, sin afectar otras corrientes que presenten un comportamiento normal. Al mismo tiempo, permitir a la corriente de conexión el uso máximo del ancho de banda que necesite, en caso de que no haya congestionamiento. Dentro del header de las celdas existe un campo formado por cuatro bits; este campo es utilizado por el **Control de Flujo Genérico (GFC)**. El protocolo GFC tiene un valor inicial de 0, es decir 0000, esto implica que dicha función no se encuentra en uso. Este mecanismo es auxiliar en el control del flujo de tráfico de las conexiones ATM. El mecanismo GFC maneja tanto las configuraciones punto a punto como las multipunto. En configuraciones en las cuales cada terminal se conecta a la terminal de red por medio de su propia línea, se puede utilizar el GFC para reducir el flujo de celdas en cada terminal. Debido a que el GFC no tiene relación con el resto del header, es imposible llevar a cabo el control individual de VPC's, VCC's y terminales que estén conectadas a un medio común. En configuraciones donde se tiene un medio compartido, se usa el GFC para el control de acceso al medio. El Control de Flujo Genérico (GFC) debe satisfacer los siguientes requisitos:

- El GFC debe ser capaz de asegurar que todas las terminales puedan accesar sus facilidades. Esto es necesario para todas las terminales CBR, así como para las VBR que tengan un elemento de facilidades seguras.
- El protocolo GFC tiene la obligación de manejar diferentes requisitos de retraso y variaciones de retraso.
- La comunicación directa de extremo a extremo puede ser posible en una configuración de medios compartidos. Esto requiere de una implementación simétrica del procedimiento GFC.
- El protocolo GFC debe ser insensible a la mezcla de tráfico, por ejemplo el número de fuentes CBR o VBR activas o la mezcla de bit rate, así como a los parámetros del sistema como el número de terminales y distancia entre terminales.
- Debe ser lo suficientemente fuerte y completo para soportar los problemas de pérdida, inserción errónea o mala información. del GFC.

Una red ATM no proporciona el tipo de control de flujo que se encuentra en una red de paquetes y no tiene la facilidad de guardar las celdas por un periodo de tiempo largo. Por lo tanto no hay necesidad de tener un GFC dentro de una red ATM. El GFC sólo controla las terminales que se conectan a una red de usuario. El procedimiento exacto del GFC no se ha definido aún, sin embargo se han propuesto algunos procedimientos basados en un algoritmo de sucesión **(queueing)** conocido gracias a la red DQDB. Se llevaron a cabo algunas modificaciones con el fin de poder manejar tráfico CBR y diferentes topologías de redes de usuario. Otras topologías utilizan una modificación de un protocolo llamado **Orwell**, para tener control sobre el flujo de celdas de las terminales. Para poder decidir cual es el "mejor" protocolo, los valores de algunos parámetros tanto del sistema como del tráfico se han analizado, tales como; el número de terminales activas, distancia entre terminales, servicios, bit rates, etc. No obstante, no es posible tomar una decisión basada únicamente en los resultados de dicho análisis. También se deben tomar en cuenta el costo de implementación, así como la confiabilidad.

Control de Admisión de Conexión

Una de las razones por las cuales el ATM se diseñó orientado a conexión es que las conexiones son el método más natural para servicios que incluyen conversaciones de tiempo real, tales como audio y video. Las conexiones también presentan ventajas al proveedor de red puesto que las decisiones de ruteo por celda se simplifican, además de que si se mantiene la secuencia se facilita el reensamblaje de los datos originales del usuario. Por lo tanto el **Control de Admisión de Conexión (CAC)** es una de las partes más importantes en el control de tráfico en ATM. El CAC y el Control del Parámetro de Uso (UPC) son las funciones principales en el control de tráfico preventivo. Así como en las redes telefónicas, el CAC consiste de:

- Negociación de una solicitud nueva de conexión con los usuarios.
- Admisión o rechazo de la nueva conexión (decisiones).
- Alojar los recursos de red apropiados.

Entre los puntos más importantes se encuentra la caracterización de la fuente de tráfico y los requisitos de QoS, así como el ruteo y la política de admisión o rechazo de conexiones. Mediante el ruteo se trata de maximizar la salida de la red distribuyendo de manera uniforme el tráfico y de esta forma utilizar la red de una manera más eficiente, al mismo tiempo que se minimizan los retardos de extremo a extremo. Si se necesitan conexiones múltiples, la admisión o rechazo se determina por medio de cada conexión virtual. Las solicitudes de conexión, así como la negociación o conexión de parámetros, se hace mediante el cambio de información de señalamiento. El CAC utiliza la solicitud de conexión para llevar acabo la estimación del QoS resultante en caso de que la conexión nueva haya sido aceptada, también determina los parámetros de tráfico para el UPC, y por último determina los recursos de la red que vayan a ser alojados a lo largo de la ruta. La admisión de una conexión nueva es posible si la red estima que la conexión se puede establecer con el QoS requerido, manteniendo el QoS de las otras conexiones ya existentes. La solicitud de conexión viaja a través de la ruta. Cada nodo decide si puede alojar los recursos necesarios. La solicitud se acepta en caso de que cada nodo la acepte. El aceptar una conexión nueva implica un acuerdo en un contrato de tráfico el cual especifica las obligaciones entre el usuario y la red. Una vez que se establece el contrato, los parámetros de conexión virtual pueden cambiar sólo a través de la renegociación entre el usuario y la red.

Contrato de Tráfico

Para hablar de un contrato de tráfico es necesario mencionar primero una descripción de tráfico. Se denomina **ATM Traffic Descriptor (descriptor de tráfico ATM)**, al conjunto de parámetros que se pueden utilizar para caracterizar una conexión. Un **Descriptor de Tráfico de Fuente (Source-Traffic Descriptor)** es un subconjunto del descriptor tráfico ATM que se usa durante la inicialización de la conexión para caracterizar una conexión que se ha solicitado. Un **Descriptor de Tráfico de Conexión (Conection-Traffic Descriptor)** se encarga de caracterizar la conexión en el UNI, y consiste de un descriptor de tráfico de fuente, tolerancia de variación de retraso de celda y definición de conformidad. El descriptor de tráfico de conexión lo utiliza la red durante la instalación de la conexión para alojar los recursos de la red y derivar los parámetros para el UPC. La definición de conformidad la usa el UPC para poder distinguir entre celdas conformes e inconformes sin ambigüedad. Si la red admite una conexión nueva, esto implica un arreglo en el contrato de tráfico que especifique las obligaciones entre la red y el usuario. El contrato de tráfico está constituido por descriptor de tráfico de conexión, clase QoS solicitada y definición de conexión pasiva. Esta última la determina el proveedor de red y difiere de la definición de conformidad, la cual se aplica a celdas individuales. Un aspecto importante que hay que cuidar es el juego de parámetros que deben incluirse en el descriptor de tráfico de fuente. Todos los parámetros deben ser fáciles de determinar por el usuario, así como útiles al CAC para la distribución de recursos, y poder ser reforzados por el UPC. Dicho juego debe ser pequeño, y sin embargo tener espacio suficiente para los diversos tipos de tráfico en ATM. Algunos de los parámetros propuestos para el descriptor de tráfico de fuente son:

- Valor pico de celdas y tolerancia de variación del retraso de celdas.
- Razón de mantenimiento de celdas y tolerancia de explosión.
- Tiempo mínimo entre llegada de celdas.
- Tiempo mínimo promedio entre llegada de celdas en un periodo de tiempo especificado.
- Velocidad promedio.
- Longitudes máximas y media de explosión.
- Valor Pico de Celda y Variación del Retraso de Celdas.

Estos son de los parámetros más importantes; el primero no es simplemente el valor recíproco del tiempo mínimo de llegadas entre celdas transmitidas consecutivamente, teniendo en cuenta que el valor pico puede ser muy limitado, el Forum ATM ha propuesto un algoritmo denominado **algoritmo de valor genérico de celdas**. Este algoritmo se ha propuesto a manera de modelo de referencia con el fin de definir ciertos parámetros de una corriente de celdas. Estos parámetros son muy útiles durante el establecimiento de la conexión. El **Algoritmo de Valor Genérico de Celdas (GCRA)** comprende dos parámetros; un **incremento I** y **un límite L**. Este algoritmo puede ser visto de dos formas diferentes; ya sea un algoritmo de temporización virtual o algoritmo de cubo de goteo (leaky-bucket).

En el primero, como se aprecia en la figura 190, la llegada en el tiempo de la n-ésima la celda, t(n), se compara con su llegada teórica T(n), la cual es la llegada en tiempo que se espera bajo el supuesto de que las celdas son igualmente espaciadas en el tiempo con una distancia I. Este algoritmo intenta asegurar que la razón de celdas no sea mayor a I^{-1} en el promedio, con cierta tolerancia dependiente de L; es decir, las celdas no van a llegar mucho antes que sus llegadas teóricas esperadas. La celda debe satisfacer la condición: t(n) T(n)-L, de lo contrario sería celda no conforme. La llegada teórica para la siguiente celda T(n+1), se calcula en función de t(n). Si la n-ésima celda es conforme y t(n) T(n), entonces la siguiente llegada teórica se establece a T(n+1) = T(n) + I. Si la celda es conforme y t(n) T(n), entonces la siguiente llegada teórica se evalúa en T(n+1) = T(n) + I. Las celdas no conformes no se cuentan para la actualización de los tiempos de las llegadas teóricas.

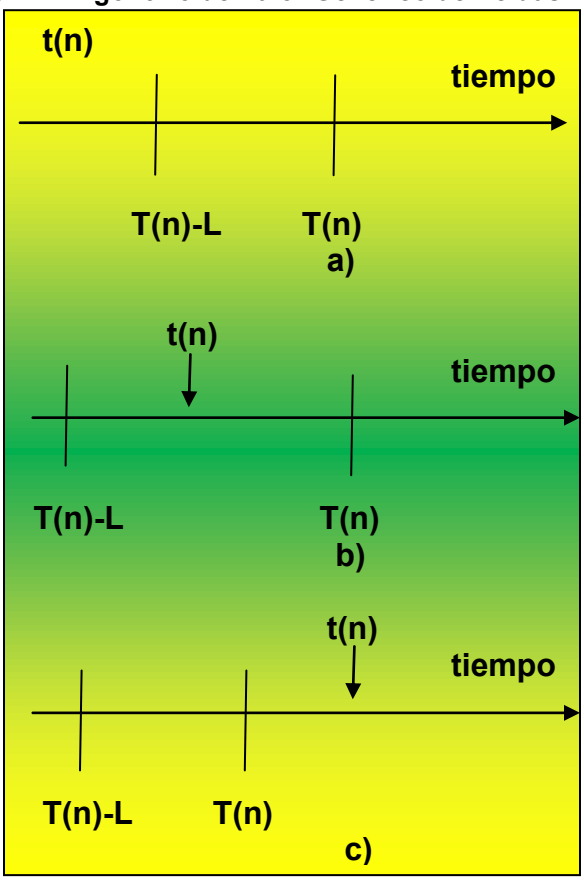


Figura 190

Algoritmo de temporización virtual, a: la celda llegó antes y no es conforme, b: la celda llegó antes pero es conforme y T(n+1) = T(n) + I, la celda es conforme y T(n+1) = t(n) + I. El Valor Pico de Celda y la **Tolerancia de Variación en el Retraso de Celdas** se definen utilizando el modelo de terminal equivalente del GCRA. Este es el modelo conceptual para la representación del proceso de generación de una corriente de celdas del usuario. Esto no significa que la terminal del usuario lleve a cabo estas funciones, sólo enfatiza el hecho de que la corriente de celdas que cruza el UNI aparece como hubiera sido generada desde una terminal equivalente. En un principio las celdas se generan en la Capa ATM y se les da forma, a manera de que sean celdas conformes con respecto al GCRA (I_p,0) en el punto de acceso al servicio de la Capa Física (PL-SAP). Este es un punto teórico en el cual las celdas de la Capa ATM se presentan a la Capa Física para ser transmitidas. La Tolerancia de Variación en el Retraso de Celdas se encuentra estrechamente relacionada con el Valor Pico de Celda. Después de que las celdas han sido presentadas al PL-SAP para la transmisión, se introduce un proceso aleatorio en el espaciamiento de la corriente de celdas; debido a la multiplexión, inserción de celdas OAM, o la espera de ranuras de tiempo. Por lo tanto, la corriente de celdas no son conformes con el GCRA (I_p,0). El límite superior de distorsión de la corriente de celdas es la Tolerancia de Variación en el Retraso de Celdas (L_p). Entonces la corriente de celdas es conforme al GCRA (I_p,L_p) en la terminal de salida. Es evidente que si se tienen valores muy altos de L_p existe una desviación mayor de la corriente de celdas ideal en la

cual las celdas van separadas por un periodo de tiempo, exacto; igual a I_p. Esto permite una mayor agrupación de celdas, o grupos de celdas consecutivos.

Distribución de Recursos

Aunque los parámetros de tráfico están sujetos a la estandarización, los proveedores de red implementan sus propios métodos de distribución de recursos, así como las políticas de admisión de conexión. La distribución de recursos es un problema complicado en ATM debido a que existen conexiones con características y requisitos de desempeño de red diferentes. De tal forma que no está claro aún el como poder determinar la aceptación o rechazo de conexiones entre los diferentes servicios de una manera justa y equitativa. Por ejemplo, la aceptación de una conexión de banda ancha alta puede quedar en el bloque de conexiones de banda ancha baja; y sería preferible rechazar la primera y aceptar la segunda puesto que involucra a más usuarios. Las llamadas que comprenden conexiones múltiples aumentan el problema aún más. Otro problema que surge es la distribución de recursos para las conexiones VBR multiplexadas por estadísticas. Una política de admisión conservativa basada en los valores pico podría ser el bajo uso de red. Sin embargo, si se aprovecha el uso de la multiplexión, se puede causar que las explosiones de valor pico ocasionen sobre flujos en los buffers o retrasos excesivos de sucesión. El uso de trayectorias virtuales en el manejo de recursos puede ser importante, por lo menos al principio. Si se mantiene el exceso de capacidad de VPC's anticipando las VCC's venideras, se puede reducir el monto de procesamiento requerido para el establecimiento de VCC's nuevas. Las VCC's que lleguen se pueden establecer mediante la aceptación de conexión en las terminales de la VPC, y de esta forma se elimina el proceso de conexión de VPC. La decisión depende únicamente de que la capacidad de la VPC que ya existe. En tal caso no toma tiempo el establecer una nueva VPC para cada VCC que sea solicitada.

Por otro lado, las VPC's permiten una eliminación lógica de clases QoS mientras se lleva a cabo la multiplexión de las VPC's. Las VCC's con requisitos de QoS similares se pueden agrupar en la misma VPC. Las VPC's simplifican el manejo de VCC's, con lo cual se reducen los costos de manejo y control. Finalmente, el control dinámico de ruteo a nivel de VPC hace posible un método más simple para la reconfiguración adaptiva de red. El ruteo de trayectoria se puede modificar con sólo cambiar la información en los puntos de conexión de la VPC. En algunas aplicaciones, tales como transferencia de datos LAN a LAN, la fuente de tráfico se caracteriza por explosiones a un valor pico separadas por periodos de inactividad. El valor pico es el único parámetro conocido, los demás parámetros de tráfico no son importantes. Para este tipo de tráfico no es necesario llevar a cabo una instalación de conexión larga con el fin de negociar un contrato de tráfico detallado. Una mejor solución puede ser la negociación del valor al principio de cada explosión, a lo cual le sigue un proceso de instalación simple llamado protocolo de reservación rápida. Una celda especial antecede la explosión para solicitar los recursos de red. Las explosiones pueden ser admitidas o bloqueadas. En caso de ser admitidas, los recursos se liberan de forma instantánea después de la explosión. Este procedimiento reduce el señalamiento del tiempo y asegura un transporte confiable de celdas correlacionadas que pertenecen a una unidad de datos grande. Esto puede ser una alternativa para aquellos servicios que no requieren de un QoS garantizado, o son más sensibles a la pérdida de celdas que al retraso o bien que tienen características de tráfico impredecibles.

Control del Parámetro de Uso/Red

El control del parámetro de uso es necesario para poder vigilar y regular el flujo de tráfico venidero en la UNI para de esta forma asegurar el respeto al acuerdo de los contratos de tráfico. En la NNI, la función de vigilancia se llama control del parámetro de red (NPC). Su finalidad es proteger la red de que se desvíe de los parámetros de tráfico establecidos, ya sea de forma intencional o no, afectando al QoS de otras conexiones. Existen tareas específicas como lo son la comprobación de los valores VPI/VCI y asegurarse de que los valores del tráfico que proviene de VPC/VCC activas concuerden con los parámetros acordados. Un mecanismo de **Control del Parámetro Uso/Red (UPC/NPC)**, debe tener las siguientes características:

- De fácil implementación y entendimiento para el usuario.

- Respuesta rápida a violaciones.
- Permitir un margen de tolerancia debido a aspectos prácticos inciertos.
- Ser transparente en caso de que la fuente sea conforme.

Además la UPC/NPC debe minimizar el problema de falsa alarma, cuando reacciona estando la fuente conforme, o alarma tardía; la cual falla en el momento de reaccionar cuando la fuente no es conforme al contrato de tráfico. Debido a ciertas inseguridades de origen práctico, es necesario permitir elasticidad. Por otro lado se tiene la difícil tarea de vigilar el valor pico. En caso de que sea desconocido, se puede calcular con una muestra pequeña de tráfico, aunque esto comprende, por supuesto, una probabilidad de error. Si se obtiene el valor pico utilizando una muestra más grande se obtiene un valor más preciso, sin embargo esto aumenta el tiempo de reacción a violaciones. Aún no se ha establecido un mecanismo UPC/NPC estandarizado, aunque el Forum ATM haya especificado un algoritmo leaky-bucket llamado GCRA El uso de este algoritmo no implica una implementación particular, aunque el GCRA es funcionalmente equivalente a un algoritmo leaky-bucket de estado continuo. Además el GCRA comprende algunos mecanismos ya propuestos como la ventana deslizante rectangular, ventana deslizante triangular y ventana de salto. El usuario es responsable de satisfacer los parámetros del contrato de tráfico. En caso de que existan celdas que se encuentren violando el contrato, el UPC tiene la capacidad de marcar o etiquetarlas (cambiando su CLP a 1) con una prioridad de pérdida o bien puede eliminarlas. Si se lleva a cabo la etiquetación, estas celdas se unen con otras que posean un CLP=1 antes de que entren a un mecanismo UPC. Una vez dentro de red las celdas con un CLP=1 se eliminan primero en caso de que ocurra un congestionamiento.

Etiquetamiento de Celdas y Formación del Tráfico

El etiquetamiento de celdas puede ser una buena opción cuando las celdas marcadas pueden viajar a través de la red sin problemas y sin afectar el desempeño de la red. Esta puede ser una muy buena opción en sistemas que no requieren de un QoS muy estricto. Si la probabilidad de transportar el tráfico etiquetado es baja, entonces no se recomienda ocupar este método puesto que las celdas etiquetadas utilizan recursos de red valiosos y esto aumenta el nivel de congestionamiento. El usuario debe darle forma al tráfico ya sea antes de que éste entre a la red o bien inmediatamente después del UPC. El propósito de que el usuario de forma al tráfico es asegurar conformidad con el contrato de tráfico y evitar la pérdida de celdas en el UPC. Cuando la red le da forma al tráfico se busca la reducción del valor pico de celda o la explosión de la fuente de tráfico VBR. Esto reduce la sucesión, y por lo tanto retrasos y pérdidas de celdas, dentro de la red.

Algoritmo Leaky-Bucket

El algoritmo leaky-bucket ha sido utilizado para la regulación de sobrecargas en los controles de los sistemas de conmutación controlados por programas almacenados. De hecho fue el primer algoritmo propuesto para el UPC en ATM y ha sido tomado en cuenta, principalmente debido a su implementación tan sencilla. EL algoritmo leaky-bucket básico como un esquema de token-queueing. Un buffer, o recipiente **(bucket)** para tokens, cuyo tamaño se denomina **B** que contiene tokens se drena a una razón constante **R**, figura 191. Una celda que viene llegando intenta incorporar un token al buffer, y ésta puede pasar en caso de que el recipiente de tokens no esté lleno. Si el recipiente está lleno, la celda se descarta. Se puede decir que los tokens pueden verse como las llegadas a un servidor simple sucesión de capacidad finita con servicios de tiempos determinados. Esto aparenta que el leaky-bucket refuerza la razón promedio R y permite explosiones temporales por arriba del valor R dependiendo del valor B. La implementación requiere de un contador bidireccional simple para llevar la cuenta del número de tokens en el recipiente arriba.

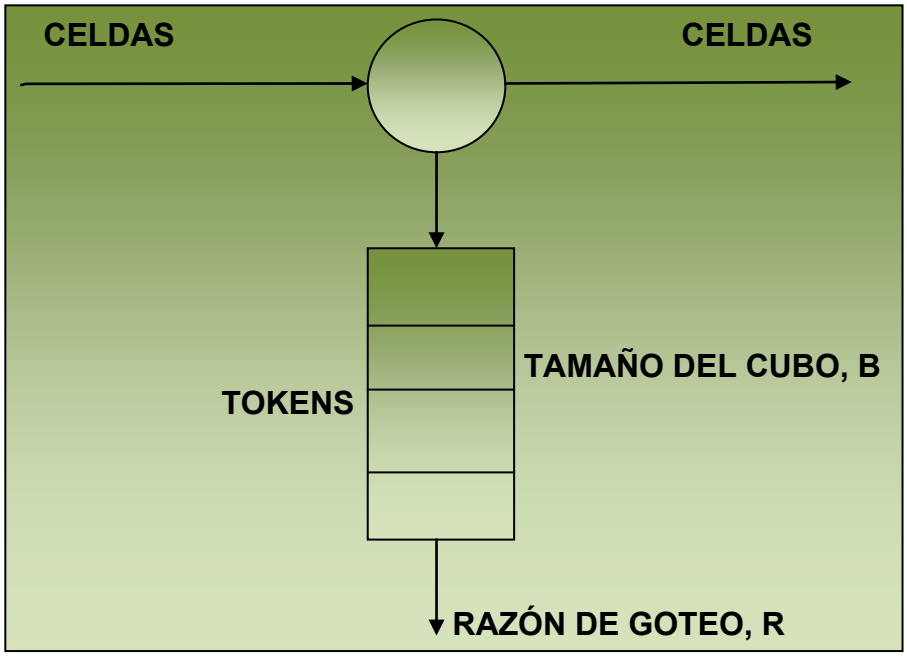


Figura 191

Algoritmo básico de leaky-bucket

Este algoritmo ha sufrido cambios para dar lugar a nuevas versiones. Por ejemplo, en vez de eliminar las celdas cuando el recipiente se llena, se llevan a otro buffer de entrada. También, se pueden etiquetar y dejarlas pasar con alta posibilidad de ser descartadas. Un espaciador de celdas en la salida puede servir para dar forma al tráfico y de esta manera suavizar los tiempos de salida de las celdas. Se ha propuesto utilizar múltiples leaky-buckets para poder reforzar los diferentes parámetros. Por ejemplo, el leaky-bucket doble. El tamaño de los recipientes puede ajustarse para las tolerancias que se tengan pensadas para la variación del retraso de celdas y las explosiones. El UPC puede utilizar esta ventaja cuando el control de tráfico comprende valor pico de celdas, tolerancia de la variación del retraso de celdas, valor de celda sostenido y tolerancia de explosión. La efectividad del método del leaky-bucket ha aumentado. Si B es pequeña, se tiene entonces poca tolerancia a las variaciones en los tiempos de llegadas de las celdas, y algunas celdas conformes pueden ser eliminadas por error. Por otro lado, si B es muy grande, se tiende a caer en un mecanismo poco efectivo debido a que causa una desviación mayor de R, figura 192

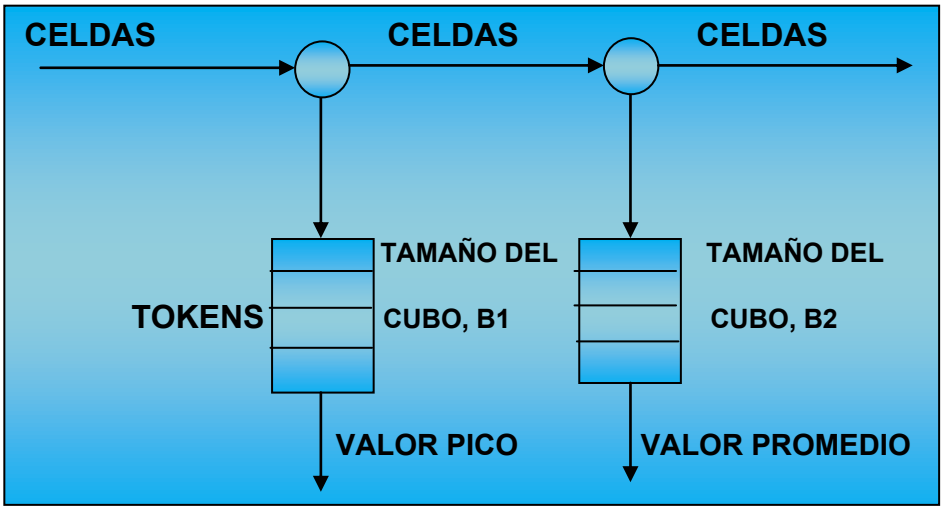


Figura 192

Leaky-buckey doble

El GCRA es equivalente, funcionalmente hablando, a un leaky-bucket de estado continuo. El recipiente drena a razón de 1 por unidad de tiempo y se llena a una velocidad **I** por cada llegada de celda conforme. Cuando llega una celda, esta se considera conforme en caso de que el recipiente se encuentre por debajo del límite L a la llegada; la capacidad del recipiente es de L+I.

Congestionamiento

El Control de Admisión de Conexión y el Control del Parámetro de Uso, CAC y UPC respectivamente, son funciones que sirven para prevenir el congestionamiento, sin embargo existe una probabilidad pequeña de que suceda un congestionamiento causado por la sobrecarga temporal de lo buffers dentro de la red. El propósito del control de congestionamiento es detectar su existencia, y así reaccionar mediante el decremento de velocidad, efectos y duración del mismo. Por simplificación y velocidad, el protocolo ATM no incluye controles de flujo convencionales en el nivel de enlace, los cuales son apropiados tan sólo para aquel tipo de tráfico que tolera retrasos. Los controles de congestionamiento en ATM incluyen la eliminación selectiva de celdas y la **Indicación de Congestionamiento Explícita Adelantada (Explicit Forward Congestion Indication, EFCI)**.

Prioridad de Retraso y Pérdida

La eliminación selectiva de celdas depende plenamente de la prioridad de pérdida de las celdas. ATM permite que estas prioridades sean asignadas explícitamente a celdas individuales utilizando el CLP en el header. Cuando se presenta un congestionamiento, la pérdida de una celda es inevitable, las celdas con prioridad de pérdida baja, CLP=1 se eliminan antes que las que tienen una prioridad de pérdida alta; CLP=0. Cuando una celda posee un CLP=1, puede que sea celda no conforme al contrato de tráfico, en caso de que haya sido marcada por la red, o que contenga datos de usuario que pueden ser usados, si fue marcada por el usuario. Las prioridades de pérdida pueden reducir la pérdida de información importante. Existen dos métodos de eliminación. En el primero, el **push-out**, una celda que llega con un CLP=0 puede unirse a una fila llena mediante la eliminación de una celda cuyo CLP sea 1, en tanto que una celda que llegue con un CLP=1 no puede unirse a dicha fila. El segundo método se denomina buffer parcialmente compartido, **partial-buffer-sharing**, en este cuando una sucesión llega a un determinado umbral, aquellas celdas cuya prioridad de pérdida sea alta pueden pasar, no así las que poseen un CLP=1. Se puede ver que el método de push-out tiene un mejor desempeño, sin embargo el de buffer parcialmente compartido puede tener una implementación más sencilla. Las prioridades de retraso son muy útiles en al reducción de retrasos de extremo a extremo y el retraso de tráfico de tiempo crítico. En ATM estas prioridades pueden ser asignadas implícitamente por las VPC/VCC, por ejemplo, las celdas del mismo VPC/VCC tienen asignada la misma prioridad de retraso asociada con su VPI/VCI.

Las prioridades de retraso afectan el orden en el cual las celdas que se encuentran en los buffers se programan en tiempo o catalogan, para la transmisión sobre enlaces compartidos. Esta programación en el tiempo puede hacerse en base a celdas individuales o ciclos. En la programación en tiempo por celdas existe una política de atender primero a las celdas que tengan un tiempo límite, y ha demostrado tener óptimas propiedades. Considérese una fila que contenga celdas con límites de tiempo; entonces aquellas celdas que no sean transmitidas antes del tiempo límite se eliminan. La política de escoger la celda con un límite de tiempo más cercano reduce el número de celdas eliminadas. En la programación en tiempo por ciclos, las decisiones de programación se llevan a cabo únicamente antes de cada ciclo. Un ejemplo es el esquema asíncrono de tiempo compartido. En cada ciclo, se asignan las ranuras de tiempo al número mínimo de celdas en tiempo real alineadas que no pueden esperar hasta el siguiente ciclo para que no se venza su tiempo límite. El resto del ciclo se llena con celdas de tiempo no real. En otro ejemplo de programación por ciclos al inicio de cada ciclo se determina una lista de pesos asignados. Estos especifican la razón relativa de ranuras de tiempo que se asignan con la prioridad

más alta para cada clase de tráfico. Si no hay ninguna celda de mayor prioridad en espera, entonces cualquier otra celda puede utilizar esa ranura.

Indicación de Congestionamiento Explícita Adelantada (EFCI)

Las prioridades, tanto de retraso como de pérdida se utilizan para el control del tráfico dentro de un conmutador, en tanto que el EFCI es un mecanismo de comunicación desde la red al usuario para activar el control de extremo a extremo. Si un nodo de red se sufre un congestionamiento, puede pasar la información a los nodos que se encuentran corriente abajo y al destinatario con sólo cambiar el campo PT en los headers de las celdas. El destinatario está al tanto pues del congestionamiento y de esta forma mandar indicaciones a la fuente apropiada que cambie su velocidad. Obviamente esto depende de la cooperación de los usuarios de terminales para que respondan apropiadamente a la indicación de congestionamiento. Este mecanismo no puede ejecutar acciones de prevención de congestionamiento o el sobre uso, pero es útil para aminorar la pérdida de celdas en periodos persistentes de congestionamiento. El método mediante el cual un nodo de red vigila su propia operación interna y clasifica su congestionamiento se considera de implementación dependiente y no está sujeto a estandarización.

Manejo Inteligente de Red Distribuida

Como principio general se tiene que cada capa del modelo de referencia, así como cada nivel de la red, tiene su propio proceso de manejo independiente. Es decir, cada nivel está equipado con su propio mecanismo OAM. Para poder realizar el monitoreo, cada nivel, de manera implícita, debe ser capaz de llevar a cabo las mediciones pertinentes. Todos los mecanismos descritos en las secciones pasadas son sencillos y aún flexibles en un principio. El problema surge cuando se planea el control de los valores de los parámetros y la optimización del desempeño de los esquemas de control planteados en las secciones previas. Un mecanismo distribuido inteligente puede ser la solución para el monitoreo y los esquemas de control de tráfico y congestionamiento.

Sistemas Multiagentes

Un sistema multiagentes se puede definir como un sistema en el cual varios agentes interactúan. Se considera un agente una entidad, ya sea física o abstracta, que sea capaz de actuar en sí misma y en el medio en el que se encuentre, además de poder manipular una representación parcial de su medio y comunicarse con otros agentes. El comportamiento de un agente viene como consecuencia de su percepción, conocimiento e interacción con otros agentes. Se han desarrollado algunos temas con respecto al estudio de los agentes:
Los agentes pueden considerarse entidades autónomas con las capacidades de percepción, decisión y comunicación. Son capaces de actuar en su propio medio, o bien de forma independiente. Los agentes se consideran módulos especializados que interactúan en grupo de acuerdo a una arquitectura específica. Se puede representar a cada agente como una base de datos o un procedimiento especializado.

Existe un punto intermedio entre estos dos casos extremos, donde se trabaja ya sea con un sistema único, o bien con sistemas independientes; existen pues, sistemas multiagentes. En este caso, los agentes operan de manera síncrona y en grupo en diferentes tareas, con otros agentes y sin conocer del todo el medio. Para el control de tráfico, no es necesario utilizar uno de los tres métodos anteriores. Se puede asumir que cada interfaz y cada switch de celda tienen un agente a cargo de las tareas de control. El primer método habla acerca de que cada agente trabaja con su propio conocimiento. La ventaja que representa es que evita los problemas de comunicación entre los agentes. Como resultado se tiene un esquema simplificado y no hay sobre nivel de tráfico dentro de la red. En el segundo método todos los agentes están coordinados y un panorama global de la red puede ser el camino hacia una decisión. Esto no es posible en un ambiente ATM, donde el retraso de propagación de celdas puede ser aproximadamente del mismo orden que el retraso de propagación de señal.

De acuerdo a lo expuesto anteriormente es posible concluir que la mejor opción son los agentes semiautónomos, para que de esta forma las decisiones locales se hagan instantáneamente cuando los agentes están preparados para hacerlas. Cuando la red no está muy cargada, es posible intercambiar información sobre la vida de la red para mejorar la información que los agentes poseen. Esto supone que los agentes son capaces de tomar mejores decisiones con el uso de datos históricos, lo cual a su vez es parte de un proceso de aprendizaje.

Arquitectura Blackboard

La organización de **Inteligencia Artificial Distribuida (DAI)**, en este caso se implementa de acuerdo al principio de la arquitectura **blackboard**, la cual está constituida por tres componentes:

- Una estructura de base de datos llamada blackboard que contiene el estado actual de la solución a un problema dado. Esta información es análoga al trabajo de una memoria que se accesa mediante varias reglas de producción, pero el blackboard se divide en áreas separadas de abstracción semántica llamadas niveles.
- Un grupo de agentes independientes, los cuales pueden leer o escribir en varios niveles. Estos pueden tomarse como una colección de procesos independientes capaces de cooperar en la solución de un problema.
- Un sistema de control que sirve para asegurar la supervisión de las acciones de los diferentes agentes. Este sistema también es una colección de fuentes de control de información integrado.

Sin embargo esta organización no es suficiente para llevar a cabo un sistema multiagentes. Es necesario describir una arquitectura completa para cada agente. Por lo tanto se ha decidido organizar el agente en los siguientes principios de acuerdo a la arquitectura blackboard con tres componentes:

- Un agente que se encargue de la información usual y el conocimiento del dominio.
- Un módulo de control que defina la estrategia de solución del problema y el mecanismo de control para determinar las acciones que se deben tomar.
- Un módulo de comunicación que modele a los otros agentes en el medio. Este módulo también tiene que ser capaz de proporcionar un intérprete de mensajes y comunicaciones lógicas con los otros agentes.

Cada agente puede ser visto como un procesador de software independiente con sus propios recursos. Los agentes se comunican compartiendo la información, en los niveles altos, por ejemplo un nivel de multiagentes completo. Se comunican a través de un blackboard general que contiene en un principio los hechos de un problema dado. Los agentes leen la información del blackboard y ahí mismo escriben para lograr una solución paso a paso. En una red ATM se asume que un agente está conectado a cada nodo y puede trabajar aislado en caso de que sea necesario. Además, la información procedente del exterior se añade al agente.

Arquitectura del Manejo del Desempeño de la Red

Para lograr una mayor eficiencia, es conveniente agrupar los recursos de acuerdo a ciertos criterios. Estos juegos se denominan dominios. Esto es una manera de poder introducir tres niveles en la solución de un problema distribuido. El primer nivel se encarga de la resolución ejecutada por el agente sólo. El segundo nivel trata de la resolución dentro de un dominio en caso de que el problema sea más grande que la capacidad del agente, y el tercer nivel interviene cuando se utilizan más de un dominio. El dominio se maneja por uno o varios agentes que pueden estar situados en cualquier nodo de la red perteneciente al dominio. Los agentes trabajan de una forma coordinada en una estructura de datos común: el blackboard. Éste se sitúa en el administrador donde se proporcionan todas las funciones de manejo. Los agentes pueden trabajar en grupo con un problema dado, en el blackboard, o bien por su parte o con algunos otros agentes de su medio para la solución de problemas puntuales.

Los esquemas de monitoreo se han desarrollado y normalizado. Dichos esquemas se hacen posibles por la generación de celdas OAM y las funciones de procesamiento que se llevan a cabo por los agentes a lo largo de la conexión virtual ATM que se está monitoreando. Una de las ventajas que se obtiene al utilizar celdas OAM para comunicar la función de la indicación desde cualquier punto de la conexión es que el reporte puede leerse en los puntos intermedios a lo largo de la conexión. Esta información la capturan los agentes. Los esquemas de monitoreo son lo suficientemente flexibles de tal forma que otros parámetros de ejecución se pueden tomar en cuenta. Toda esta información de ejecución la capturan los agentes y la conducen hacia la optimización de los valores de los parámetros a pesar de la capacidad de inteligencia de los agentes.

6.2.3 TIPOS DE CONEXIONES

ATM provee servicios orientados a conexión. Para comunicarse con un nodo remoto, un host debe solicitar a su switch local el establecimiento de una conexión con el destino. Estas conexiones pueden ser de dos naturalezas: **Switched Virtual Circuits (SVC) o Permanent Virtual Circuits (PVC)**

6.2.3.1 SWITCHED VIRTUAL CIRCUITS

Un SVC opera del mismo modo que una llamada telefónica convencional. Un host se comunica con el switch ATM local y requiere del mismo el establecimiento de un SVC. El host especifica la dirección completa del nodo destino y la calidad del servicio requerido. Luego espera que la red establezca el circuito. El sistema de señalización de ATM se encarga de encontrar el path necesario desde el host origen al host destino a lo largo de varios switches. El host remoto debe aceptar el establecimiento de la conexión. Durante el proceso de señalización (toma este nombre por analogía con el usado en sistemas telefónicos de los cuales deriva ATM) cada uno de los switches examina el tipo de servicio solicitado por el host de origen. Si acuerda propagar información de dicho host registra información acerca el circuito solicitado y propaga el requerimiento al siguiente switch de la red. Este tipo de acuerdo reserva determinados recursos el switch para ser usados por el nuevo circuito. Cuando el proceso de señalización concluye el switch local reporta la existencia del SVC al host local y al host remoto. La interfaz UNI identifica a cada uno de los SVC por medio de un número de 24 bits. Cuando un host acepta un nuevo SVC, el switch ATM local asigna al mismo un nuevo identificador. Los paquetes transmitidos por la red no llevan información de nodo origen ni nodo destino. El host marca a cada paquete enviado con el identificador de circuito virtual necesario para llegar al nodo destino. Nótese que se ha evitado hablar de los protocolos usados para el establecimiento de los SVC, para los procesos de señalización y para comunicar a los hosts el establecimiento de un nuevo SVC. Además hay que tener en cuenta que comunicaciones bidireccionales van a necesitar reservar recursos a lo largo del SVC para dos sentidos de comunicación.

6.2.3.2 PERMANET VIRTUAL CIRCUITS

La alternativa al mecanismo de SVC descrito anteriormente es evidente: el administrador de la red puede configurar en forma manual los switches para definir circuitos permanentes. El administrador identifica el nodo origen, el nodo destino, la calidad de servicio y los identificadores de 24 bits para que cada host pueda acceder al circuito.

6.2.3.3 PATHS, CIRCUITOS E IDENTIFICADORES

ATM asigna un entero único como identificador para cada path abierto por un hosts. Este identificador contiene mucha menos información de la que fue necesaria para la creación del circuito. Además el identificador sólo es válido mientras que el circuito permanece abierto.

Otro punto a tener en cuenta es que el identificador es válido para un sólo sentido del circuito. Esto quiere decir que los identificadores de circuito obtenidos por los dos hosts en los extremos del mismo usualmente son diferentes. Los identificadores usados por la interfaz UNI están formados por 24 bits, divididos en dos campos, el primero de 8 bits y el segundo de 16 bits. Los primeros 8 bits forman el llamado «**Virtual Path Identifier**» y los 16 restantes el «**Virtual Circuit Identifier**». Este conjunto de bits suele recibir el nombre de **VPI/VCI pair**. Esta división del identificador en dos campos persigue el mismo fin que la división de las direcciones IP en un campo para identificar la red y un segundo campo para identificar el host. Si un conjunto de VC's sigue el mismo path el administrador puede asignar a todos ellos un mismo VPI. El hardware de ATM usa entonces los VPI para funciones de ruteo de tráfico.

6.2.3.4 ATM CELL TRANSPORT

En cuanto al transporte de información, ATM usa tramas de tamaño fijo que reciben el nombre de celdas. El hecho de que todas las celdas sean del mismo tamaño permite construir equipos de switching de muy alta velocidad. Cada celda de ATM tiene una longitud de 53 bytes, reservándose los 5 primeros para el encabezado y el resto para datos. Dentro del encabezado se coloca el par VPI/VCI que identifica al circuito entre extremos, información de control de flujo y un CRC. La conexión final entre dos nodos recibe el nombre de Virtual Channel Connection o VCC. Una VCC se encuentra formada por un conjunto de pares VPI/VCI.

6.2 GIGABITETHERNET

6.2.1 INTRODUCCION

No hace mucho tiempo, los usuarios se daban por satisfechos con la llegada de los largos tentáculos de Ethernet al ambicioso ámbito de los 100Mbps. La aparición de Fast Ethernet supuso la constatación de que la más tradicional y popular tecnología LAN no sólo no estaba muerta, sino que incluso era capaz de competir en capacidad con las más nuevas propuestas de alta velocidad. Hoy, la promesa de un estándar Ethernet capaz de operar a un nivel teórico de 1Gbps esta creando una gran expectación en la demanda y la industria. Lejos quedan los días en que los entornos Ethernet habían de conformarse con la velocidad de 10Mbps ofrecida por el estándar. Al día de hoy, una vez ya consolidadas las opciones FastEthernet de 100Mbps, estamos asistiendo al surgimiento de una nueva propuesta que promete extender las capacidades del tradicional y difundido Ethernet al rango teórico de 1Gbps. En realidad, el proceso incrementa de velocidades de operación en LAN protagonizado por la industria y los organismos de normalización no es más que una respuesta a las necesidades crecientes de los usuarios. El gran despliegue actual de redes locales y las cada vez más complejas aplicaciones informáticas obligan a los usuarios a disponer de mayores niveles de ancho de banda. Y dada la difusión que están teniendo las soluciones FastEthernet hasta los puestos de trabajo, parece clara la necesidad de instalar conexiones de mayores velocidades, tanto en los servidores como en las redes troncales. GigabitEthernet surge así como una extensión natural de las normas Ethernet 802.3 de 10Mbps y 100Mbps que prometen tanto en modo **half-dúplex** como **full-dúplex**, un ancho de banda de 1Gbps, asegurando además la compatibilidad con la enorme base instalada Ethernet de 10Mbps y 100Mbps.

6.2.2 NORMALIZACION DE GIGABITETHERNET

Los trabajos de normalización están siendo llevados a cabo por el grupo de trabajo 802.3z del IEEE, formado el mes de julio de 1996. Con el objetivo de completar el estándar en los primeros meses del 98, si bien durante el año 97 aparecieron en el mercado conmutadores y tarjetas de red desarrollados de acuerdo a las especificaciones del borrador de la norma, las prioridades del grupo se centran en las áreas del control de flujo, arquitecturas de repetidor, distancias soportadas por los distintos medios físicos y esquemas de codificación 8B/10B. La especificación de control de flujos asegurara la interoperabilidad desatendida entre conmutadores que soporten la futura norma

y los más lentos 10Mbps y 100Mbps actuales. En modo half-dúplex, el estándar GigabitEthernet conservará con mínimos cambios el método de acceso **CSMA/CD (Carrier Sense Multiple Access/colision Detection)** típico de Ethernet. Los protocolos iniciales se basarán en la tecnología de señalización física de Fiber Channel que será adaptada para operar en velocidades de 1Gbps. Y, según la GigabitEthernet Alliance, los avances en silicio y procesamiento de señal digital permitirá posteriormente adaptar GigabitEthernet, sin grandes costos, a cableado UTP de categoría 5. En cuanto a las dimensiones de red, no parece que en principio haya límites respecto a extensión física o número de nodos. Al igual que sus predecesores, GigabitEthernet soportará diferentes medios físicos, con distintos valores máximos de distancia. El IEEE 802.3 Higher Speed Study Group ha identificado tres objetivos específicos de distancia de conexión: conexión de fibra óptica multimodo con una longitud máxima de 500m; conexión de fibra óptica monomodo con una longitud máxima de 2km; y una conexión basada en cobre con una longitud de al menos 25m. Además, se esta trabajando para soportar distancias de al menos 100m en cableado UTP de categoría 5.

Los cambios de CSMA/CD previstos consisten en una característica llamada **extensión del portador (Carrier Extensión)** necesario para permitir dominios de colisión de tamaño práctico a 1,000Mbps, que sólo afecta al modo half-dúplex. Carrier extensión incrementa la longitud de un medio portador sin alargar el tamaño mínimo de la trama Ethernet (64 bytes). Una segunda característica añadida es la llamada **ráfagas de paquetes (packet bursting)**, que permite mejorar la eficiencia en operaciones con paquetes pequeños permitiendo la transmisión de múltiples paquetes sobre un único acceso a la red. Estas dos características sólo afectan a la operación en modo half-dúplex. "Las operaciones en modo full-dúplex requerirán simplemente una versión de FastEthernet de mayor velocidad". La velocidad con que GigabitEthernet esta siendo acogida por la industria es asombrosa. La incorporación de nuevos miembros a la GigabitEthernet Alliance no ha parado de crecer desde su creación en el mes de mayo de 1996, bajo el impulso de firmas como 3Com, Sun Microsystems, Bay Networks, Cisco Systems, UB Networks, Intel y Compaq. El rápido crecimiento de la alianza demuestra que tanto las grandes como las pequeñas compañías creen en GigabitEthernet como una tecnología LAN clave. El gran interés por la nueva propuesta Ethernet se debe a su simplicidad, fiabilidad, compatibilidad hacia atrás y costos. En general, la mayoría de los grandes del mercado ATM están incorporando GigabitEthernet a sus planes de desarrollo diversificando sus estrategias de banda ancha.

6.2.3 EL MEDIO FISICO

En GigabitEthernet existen cuatro especificaciones de medios físicos: 1000BASE-T (IEEE 802.3ae), 1000BASE-SX, 1000BASE-LX y 1000BASE-CX (las tres son IEEE 802.3z), tabla 28. Estos emplean código 8B/10B que ya se utilizaba en Fiber Channel, de donde deriva toda la capa física de 1000BASE-X. La transmisión de GigabitEthernet por cable UTP categoría 5 1000BASE-T se realiza de forma muy similar a 100BASE-T2, se utilizan 4 canales de 250Mbps y se envían los datos en paralelo por los cuatro pares. En las anteriores especificaciones, el alcance de la fibra óptica viene limitado por la atenuación de la señal, pero en GigabitEthernet el alcance está limitado fundamentalmente por el efecto del retardo en modo diferencial. Este fenómeno consiste en que cuando el haz láser llega a la fibra, al ser ésta apreciablemente más ancha que el haz, este genera haces de luz secundarios que van rebotando por las paredes al avanzar por la fibra. Este rebote no ocurre exactamente igual para todos los rayos, por lo que unos realizan un trayecto un poco más largo que otros, con lo que el pulso de luz se ensancha ligeramente. El ensanchamiento es mayor cuanto mayor es la distancia recorrida.

	1000Base-T	1000Base-CX	1000Base-SX	1000Base-LX
Cable	UTP Cat 5	STP	Fibra óptica	Fibra óptica
Pares	4	2	2	2
Full-dúplex	Si	Si	Si	Si

Tipo Conector	RJ-45	9 pin D sub	SC	SC
Topología	Estrella	Estrella	Estrella	Estrella
Dist. Seg.	100 m	25 m	275, máx 500 m	550, máx 5,000 m

Tabla 28 Medios Físicos Especificados en IEEE 802.3z.

6.2.4 SUBCAPA MAC

La longitud mínima de una trama Ethernet fija el diámetro de la red, debido al funcionamiento de CSMA/CD. De haber mantenido la trama mínima de 64 bytes en GigabitEthernet el diámetro máximo habría sido de unos 45 m, inaceptables en la mayoría de situaciones. Para evitar esto, la trama GigabitEthernet incorpora un segundo relleno denominado **extensión de portadora** que se añade al final de la trama para garantizar que la longitud mínima nunca sea inferior a 512 bytes. De esta forma, el **Round Trip Time** máximo es de 4.096ms y el diámetro puede ser de unos 330m. Este segundo relleno no es formalmente parte de la trama Ethernet, por lo que sólo existirá mientras viaje por GigabitEthernet. De esta forma, se respetará la compatibilidad con los tipos anteriores de Ethernet. En el caso de que una trama con extensión de portadora sea transmitida a una red de 10Mbps o 100Mbps, ésta se eliminará. Inversamente, si una trama menor de 512 bytes llega a una red GigabitEthernet desde otra, el switch correspondiente añadirá la extensión de portadora necesaria para que la longitud sea de 512 bytes.

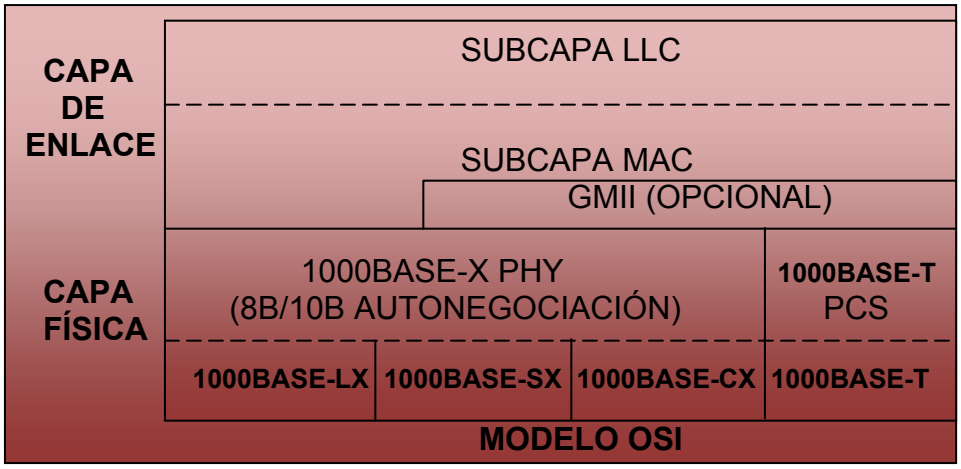


Figure 193 Arquitectura GigabitEthernet

6.3 xDSL

6.3.1 INTRODUCCION

xDSL es un grupo de tecnologías de comunicación que permiten transportar información multimedia a mayores velocidades, que las que se obtienen actualmente vía módem, simplemente utilizando las líneas telefónicas convencionales. Puesto que la red telefónica también tiene grandes limitaciones, tales como la de que su ancho de banda tan sólo llega a los 4Khz, no permite el transporte de aplicaciones que requieran mayor amplitud de banda, nace la tecnología **DSL (Digital Subscriber Line)**, que soporta un gran ancho de banda con unos costos de inversión relativamente bajos y que trabaja sobre la red telefónica ya existente, y que convierte la línea analógica convencional en una línea digital de alta velocidad. xDSL provee configuraciones asimétricas o simétricas para soportar requerimientos de ancho de banda en uno o dos sentidos. Esto se refiere a configuraciones simétricas si el canal de ancho de banda necesario o provisto es el mismo en las dos direcciones **(upstream: sentido cliente-red, y downstream: sentido red-cliente)**. Las aplicaciones asimétricas implican necesidades de ancho de banda mucho mayores tanto en una dirección como en la otra. Por ejemplo, para navegar en el web se requiere de un ancho de banda muy pequeño desde el usuario hasta su proveedor, dado que solamente se exige

lo necesario para transferir cantidades pequeñas de información. En el otro sentido (desde el proveedor hasta el cliente), el ancho de banda necesario se podría expresar en varios Mbps.

Son unas tecnologías de acceso punto a punto a través de la red telefónica pública (circuitos locales de cable de cobre) sin amplificadores ni repetidores de señal a lo largo de la ruta del cableado, que soportan un gran ancho de banda entre la conexión del cliente y el primer nodo de la red, que permiten un flujo de información tanto simétrico como asimétrico y de alta velocidad sobre el bucle de abonado. xDSL es una tecnología en la que se necesita un dispositivo módem xDSL terminal en cada extremo del circuito de cobre, que acepte flujo de datos en formato digital y lo superponga a una señal analógica de alta velocidad. El factor común de todas las tecnologías xDSL es que funcionan sobre líneas de cobre simples, y aunque cada una tiene sus propias características, todas utilizan la modulación para alcanzar elevadas velocidades de transmisión. Esta tecnología ofrece servicios de banda ancha sobre conexiones que no superen los 6km de distancia entre la central telefónica y el lugar de conexión del abonado; dependiendo de:

- Velocidad alcanzada.
- Calidad de las líneas.
- Distancia.
- Calibre del cable.
- Esquema de modulación utilizado.

La ventaja de las técnicas consiste en soportar varios canales sobre un único par de cables. Basándonos en esto, los operadores telefónicos proporcionan habitualmente tres canales: dos para datos (bajada y subida) y uno para voz. Los servicios envío y recepción de datos se establecen a través de un módem xDSL. Estos datos pasan por un dispositivo, llamado **splitter**, que permite la utilización simultánea del servicio telefónico básico y del servicio xDSL. El splitter se coloca delante de los módems del usuario y de la central; está formado por dos filtros, uno paso bajas y otro paso altas cuya finalidad es la de separar las señales transmitidas por el canal en señales de alta frecuencia (datos) y señales de baja frecuencia (telefónicas).
Canal Downstream (de bajada).-Desde la central telefónica hasta el usuario, con el que se pueden alcanzar velocidades entre 1.544Mbps y 6.3Mbps. Este canal se puede presentar al usuario como uno sólo, o múltiples subcanales, siempre dependiendo de la función a realizar. Las transmisiones de recepción residen en la banda de espectro más alta.
Canal Upstream (o subida).-Desde el usuario hasta la central telefónica, con velocidades que varían entre 16Kbps y 640kbps. Las transmisiones de envío residen en la banda de espectro más alta.
Canal telefónico.-Puede ser usado para el servicio tradicional telefónico (RTB) o bien para ISDN. Este canal es separado de los dos anteriores mediante el uso de filtros externos, y es alimentado por la central telefónica, para mantenerlo operativo aún en el caso de una caída de tensión en la oficina o casa del abonado. Las transmisiones de envío y recepción de voz, se realizan en la banda base, de hasta 4KHz. Las modalidades más comunes son mostradas en la tabla 29.

xDSL	Descripción	Velocidad máxima Usuario-red	Velocidad máxima Red-usuario	Comentarios
ADSL	Assymetric DSL	1 Mbps	8 Mbps	Asimétrico
HDSL	High Speed DSL	2 Mbps	2 Mbps	Interferente
SDSL	Symetric DSL	2.3 Mbps	2.3 Mbps	Estándar internacional
VDSL	Very High Speed DSL	53 Mbps	53 Mbps	No estándar

Tabla 29

Las técnicas de modulación usadas actualmente para xDSL son **2B1Q (2 Bit, 1 Quaternary), Carrier-Less Amplitude Phase Modulation" (CAP)** y **Discrete Multitone Modulation (DMT)**.

6.3.2 SERVICIOS QUE PUEDEN OFRECER CON UN SISTEMA DE COMUNICACION xDSL

- Navegación Internet.
- Intranet.
- Videoconferencia.
- Servicios Transparentes LAN para Clientes Corporativos.
- Acceso Remoto LAN para Clientes Corporativos.
- Educación a Distancia.
- Video en Demanda/Televisión Interactiva.
- Juegos Interactivos

Considerando la necesidad de soportar el incremento en la demanda para el acceso a Internet combinada con telecomunicación e interconectividad de las Redes LAN, podemos ver que xDSL ofrece a los carriers, **Proveedores de Servicios Internet (ISP)** y proveedores de acceso competitivo, una oportunidad excelente y maravillosa de ampliar sus recursos. Enfrentados al reto de desarrollar soluciones que cumplan con las necesidades crecientes de un mercado en expansión, los proveedores de servicios están concluyendo rápidamente que xDSL se les presenta con una serie de opciones invaluables. Dado que la tecnología xDSL ha madurado rápidamente y ha establecido una segura y muy fuerte penetración en la industria de las comunicaciones, las aplicaciones que requieren gran ancho de banda pueden ser soportadas en una plataforma altamente competitiva y costo-efectiva. Acceso a Internet y acceso a Redes LAN, pueden ser soportadas como nunca antes dada la compatibilidad de xDSL con los estándares tradicionales de comunicación. Dados esos desarrollos importantes y difíciles de alcanzar, esta claro que la tecnología xDSL será el mayor componente de la infraestructura del proveedor de servicios. Usando estas capacidades, los proveedores podrán ofrecer un rango completo de servicios, organizándolos rápidamente, y asegurándose de un servicio excelente. Las soluciones xDSL también ofrecen a los proveedores de servicios la habilidad de maximizar los recursos de personal, utilizando empleados y habilidades existentes con gran eficiencia. Consecuentemente, sus clientes tendrán alto nivel de satisfacción y los proveedores podrán potencialmente experimentar una ganancia saludable sobre su inversión.

6.3.3 TIPOS DE xDSL

	Modulación	Downstream	Upstream	Dist.màx	Voz
IDSL	2B1Q	56,64,128,144kbps	56,64,128,144kbps	1 km	No
HDSL	2B1Q	2Mbps	2Mbps	2 km	No
SDSL	2B1Q	160kbps-1'1Mbps	160kbps-1'1Mbps	3 km	No
ADSL	CAP	1'5Mbps-8Mbps	64-800kbps	3 km	Pasiva
R-ADSL	DMT	1'5Mbps-8Mbps	64-800kbps	2 km	Pasiva
VDSL	TBD	13Mbps-52Mbps	1'5Mbps-3Mbps	1km	Pasiva

6.3.3.1 ADSL

ADSL (Assymetric Digital Subscriber Line, Línea de Abonado Digital Asimétrica) es una tecnología que nos permite, usando el mismo cable telefónico que llega a nuestros hogares o empresas (par de cobre), acceder a servicios de datos (Internet) a alta velocidad sin interferir en el uso tradicional del teléfono usando la capacidad espectral del par de cobre hasta el momento desperdiciada. Permite velocidades de hasta 8Mbps en el sentido red-usuario y de hasta 1Mbps en el sentido usuario-red. Actualmente. Es una tecnología asimétrica, lo que significa que las características de la transmisión no son iguales en ambos sentidos: la velocidad de recepción de datos es mucho mayor que la de envío, lo cual hace de esta tecnología el instrumento idóneo para acceso a los denominados servicios de información, y en particular la navegación por Internet. Ello es debido a que, cuando se accede a Internet, el volumen de información recibido es muy grande, especialmente al recuperar contenidos multimedia (imágenes, video, audio) siendo la información

enviada, en general, muy inferior. Fue diseñado con el fin de satisfacer la demanda de un mayor rate de datos de la red al cliente en comparación con el rate de datos del cliente a la red.
Los siguientes tres canales pueden ser creados en el par trenzado para interconectar los módems ADSL a cada extremo terminal de la red local:

- Un canal de alta velocidad (de la red al cliente).
- Un canal de velocidad media (incluye ambas direcciones: del cliente a la red y de la red al cliente).
- Un canal **POTS (Plain Old Telephone System)**, el cual es separado de la red digital ADSL mediante filtros.

Estos tres canales son creados dividiendo la línea telefónica con la ayuda de los siguientes métodos: Multiplexaje por División de Frecuencia (FDM) y Cancelación de Eco. Las velocidades de la red al cliente dependen principalmente de la distancia y de la capacidad del cable de cobre. Un rate de datos por encima de 9Mbps puede ser alcanzada con un cable con una longitud menor a los 2,743 metros y de calibre 24 AWG. Si se duplica la distancia la velocidad puede caer a 1.544Mbps.

6.3.3.2 HDSL

HDSL (High Data Rate Digital Subscriber Line, Línea de abonado digital de Alta Velocidad) es una tecnología que permite aprovechar los pares de cobre que conforman la planta externa telefónica para la transmisión de señales digitales con velocidades de hasta 2.048Mbps. Esta tecnología transmite en full-dúplex por dos pares telefónicos una igual cantidad de tráfico de bits por medio de líneas privadas. Es un módem completo el cual trabaja con ETSI ETR 152 para dos pares de transmisión a 5Km y un sólo par de transmisión a 3.5Km. Ha sido diseñado para cubrir los requerimientos de los clientes ofreciéndoles flexibilidad de transmisión digital proveyendo transmisión de 2Mbps sobre una o dos pares trenzados de cobre. El módem HDSL se puede clasificar en varios productos como: Hiperlink E1, Hiperlink T1, Hiperlink 784, Hiperlink Rack y la Interlink. Esta tecnología es aplicable a: redes privadas, extensión E1, conexión LAN a LAN, conexión PABX a PABX, videoconferencia, redes de distribución PBX, aprendizaje a distancia, enlaces CAD/CAM y acceso remoto a datos. HDSL es la más difundida de las tecnologías xDSL y ha sido estandarizada por ANSI y **ETSI (European Technical Standards Institute)**. Esta tecnología requiere dos pares de líneas trenzadas para transportar datos a 1.544Mbps desde de la red al cliente y del cliente a la red. HDSL se utiliza también con tres pares trenzados de líneas de cobre para transportar 2.048Mbps. La distancia de operación de la tecnología HDSL es de 3,657 metros. La aplicación de HDSL es principalmente permitir el acceso a los siguientes sistemas: red PBX, estaciones de antenas para celulares, servicios de Internet y redes privadas de datos. HDSL es la más antigua de las variantes de xDSL. Se usa para transmisión digital de banda ancha dentro de instalaciones de empresas y compañías telefónicas que requieren dos cables entrelazados y que usan líneas T1. La principal característica de HDSL es que es simétrica: está disponible una cantidad igual de ancho de banda en ambas direcciones. Por esta razón, su máxima tasa de transferencia de datos es menor que la de ADSL.

6.3.3.3 VDSL

VDSL (Very High Speed Digital Subscriber Line, Líneas Digitales de Muy Alta Velocidad para el Abonado) ha sido desarrollado con la idea que pueda ser utilizado como método de transmisión entre el hogar (o negocio) y el punto de acceso a la red de fibra óptica que pueda ser localizada en el vecindario. Esto es, VDSL está destinado a ser utilizado en conjunción con **FTTC (Fiber To The Curb)** o **FTTB (Fiber To The Basement)**. La conexión local a la columna vertebral (backbone) de datos a grandes velocidades es hecha con la fibra óptica. VDSL puede suministrar rangos de datos entre 13Mbps y 60Mbps. El rango de datos a que puede ser realizado depende de la longitud de la línea. La conexión local a la columna vertebral (backbone) de datos a grandes velocidades es hecha con la fibra. Existe un punto de acceso en la vecindad (FTTC) o en el sótano del edificio (FTTB) que es propiedad del operador de telecomunicaciones. Este centro utiliza entonces VDSL para alcanzar el hogar o negocio utilizando el lazo local existente de par trenzado.

Las operadoras de telecomunicaciones podrían utilizar VDSL para enviar demanda de video a los hogares, usando **televisión de alta definición (HDTV)**, dado el largo ancho de banda que VDSL permite sobre un simple par de par trenzado. Otra aplicación potencial de VDSL es la de ser utilizada para realizar tráfico sobre ATM. Una alternativa para alcanzar altas velocidades de transmisión de datos, es la combinación de cables de fibra óptica alimentando a las **Unidades Opticas de la Red (ONU, Optical Network Units)** en los sectores residenciales y la conexión final a través de la red telefónica de cobre. Esta topología es denominada **Fiber to the Neighborhood (FTTN)**. Una de las tecnologías FTTN disponibles es VDSL, la cual transmite datos a alta velocidad sobre distancias cortas de pares trenzados de líneas de cobre con un rango de velocidad que depende de la longitud de la línea. El máximo rate de transmisión de la red al cliente está entre 51Mbps y 55Mbps sobre líneas de 300 metros de longitud. Las velocidades del cliente a la red son similares a las obtenidas con ADSL, desde 1.6Mbps a 2.3Mbps. En la Figura 194 se presenta una gráfica que permite visualizar la idea básica de la tecnología VDSL.

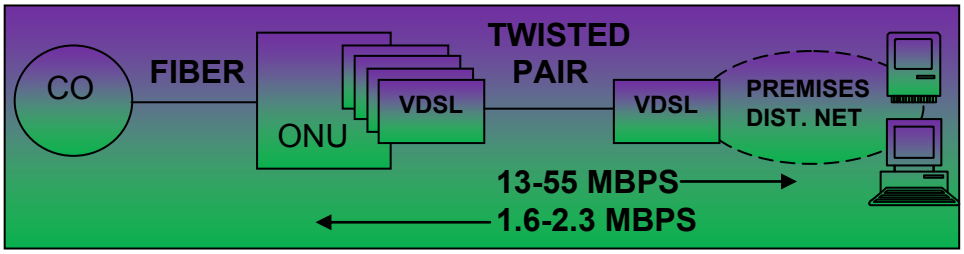


Figura 194

Aunque el estándar VDSL aún no ha sido concluido, se estima que esta tecnología proporcionará **la última milla** en las conexiones desde la red de fibra óptica y los clientes. Las velocidades (desde la red al cliente) proyectadas alcanzarán 1/12, 1/6 y 1/3 de la velocidad de Sonet (155.52Mbps). En la tabla 30 se pueden observar las velocidades (de la red al cliente) que alcanza VDSL de acuerdo con la distancia de las líneas.

LONGITUD (mts)	VELOCIDAD (Mbps)
1500	12,96 – 13,8
1000	25,92 – 27,6
300	51,84 – 55,2

Tabla 30

Al igual que ADSL, VDSL puede transmitir video comprimido, una señal en tiempo real nada común en los esquemas de retransmisión de error usados en las comunicaciones de los datos. Para lograr una tasa de error compatible con video comprimido, VDSL tendrá que incorporar la **Corrección de Errores hacia delante (FEC: Forward Error Correction)** lo suficientemente intercalado para corregir todos los errores creados debido al ruido con alguna duración especifica. Los datos en la dirección de la red al cliente serán emitidos a cada **Equipo Local del Cliente (CPE, Customer Premises Equipment)** y transmitidos a puertos lógicamente separados que distribuyen los datos a la dirección CPE que se desea acceder utilizando Multiplexaje por División de Tiempo (TDM). El multiplexaje en la dirección del cliente a la red es más difícil. Los sistemas que utilizan **Terminaciones de Red pasivas (NT, Network Termination)** deben insertar datos al medio compartido mediante TDMA o por FDM. Los sistemas que utilizan terminaciones de red activas transfieren los datos (del cliente a la red) a un puerto lógicamente separado que usaría protocolos Ethernet o ATM para realizar el multiplexaje.

La migración y las consideraciones del inventario dictadas por las unidades de VDSL establece que pueden operar a varias velocidades con el reconocimiento automático de un dispositivo recientemente conectado a una línea o un cambio en velocidad. Las interfaces de la red pasivas necesitan tener inserción caliente, donde un nuevo VDSL establece como premisas que la unidad puede ponerse en la línea sin interferir con el funcionamiento de otros módems. La tecnología VDSL tiene un grado alto de parecido con ADSL, aunque esta última debe enfrentar rangos dinámicos mucho más grandes y es considerablemente más compleja como resultado. VDSL es más bajo en costo y en poder, y las unidades de VDSL locales pueden llegar a implementar un control de acceso al medio en un nivel físico, mediante el multiplexaje de los datos en la dirección del cliente a la red. Es importante considerar los siguientes aspectos para relacionarlos con la tecnología VDSL: los posibles códigos de línea, el control del error FEC, la separación de canal y el multiplexaje en la dirección del cliente a la red.

Aspectos Pendientes en el Desarrollo de VDSL

Como ya se ha mencionado, La tecnología VDSL aún no está completa ya que existen ciertos aspectos que aún requieren de una definición clara. Estos aspectos se mencionan a continuación.

TDD (Time Division Duplexing) vs. FDD (Frequency Division Duplexing)

El tipo de división dúplex que se usará en VDSL está discutiéndose en los actuales momentos. FDD parece ser una mejor opción ya que los servicios existentes son típicamente canceladores de eco o FDD. La sincronización de los canales (en la dirección de la red al cliente y viceversa) es más fácil con FDD, porque todos los sistemas necesitan tener las mismas frecuencias del **bandsplit**. Por el contrario, con TDD la sincronización puede ser más compleja.

Modelo de Referencia

La característica del ruido en la línea no sólo variará con el tipo de línea, sino también con la base instalada de la red local. No hay ningún acuerdo hasta la fecha, aunque es necesario que se propongan varios modelos antes de que la tecnología sea masivamente comercializada. El Comité Europeo (TM6) está a favor de esperar por los resultados de los estudios de los operadores de la red y separar el modelo del ruido de los códigos de línea.

Interferencia del Sistema de Radio de Onda Corta

En el caso de antena de área local, la señal VDSL sobre el cable generará un campo eléctrico capaz de interferir con bandas de la radio de onda corta. Por otra parte, las bandas de frecuencia de radio de onda corta que coinciden con la frecuencia de VDSL dañarán la señal VDSL.

Radiación Producida por Cables Aéreos

Utilizando TDD, un transmisor de VDSL produce una emisión de radiación no deseada que interfiere con los receptores de radio-aficionados. Se determinó que el máximo PSD de 60 dBm/Hz, permitido para la tecnología VDSL puede generar interferencia potencial en algunas bandas de alta frecuencia del espectro de radio.

Operación Simétrica o Asimétrica.

Es posible que VDSL soporte tanto sistemas simétricos como asimétricos. VDSL simétrico es adecuado para distancias cortas ya que puede simplificar la interfaz con la red conjuntamente con las redes LAN. Para distancias largas VDSL asimétrico es apropiado, ya que simplifica los equipos electrónicos requeridos por los usuarios residenciales.

La tecnología VDSL permitirá en un futuro la transmisión de datos a altas velocidades utilizando una combinación de cables de fibra óptica y la red telefónica de cobre existente. Esta tecnología

proporcionará un acceso a Internet más rápido, así como la transmisión de video interactivo y mayor velocidad para los servicios de comunicación de datos. Sin embargo, aún es necesario definir ciertos aspectos como lo son, el modelo adecuado del ruido, la interferencia con señales de radio y cables aéreos y los códigos de línea que serán utilizados. VDSL (Very-High-Speed DSL): es el prospecto para ofrecer mayor velocidad en rangos de 3Mbps de subida y arriba de 52Mbps en bajada. Probablemente VDSL será una tecnología con preferencia de uso en aplicaciones con mayor ancho de banda, como manejo de imágenes en medicina, video en tiempo real o televisión de alta definición.

6.3.3.4 RADSL

RADSL (Rate-Adaptative/Assymetric Digital Subscriber Line) esta nueva tecnología va a ir suplantando a las anteriores, ofreciendo velocidades de acceso mayores y una configuración de canales que se adapta mejor a los requerimientos de las aplicaciones dirigidas a los usuarios privados como video simple (o TV en modo distribución), video bajo demanda o acceso a Internet. Son estas las típicas aplicaciones donde se necesitan unos anchos de banda elevados para recibir la información multimedia y sólo unos pocos Kbps para seleccionarla.

6.3.3.5 SDSL

SDSL (Single Line Digital Subscriber Line) es prácticamente la misma tecnología que HDSL pero utiliza únicamente un par, por lo que se sitúa estratégicamente en el segmento de los usuarios residenciales que sólo disponen de una línea telefónica. SDSL tiene la habilidad de transferir datos a la misma velocidad que HDSL, con la diferencia de que requiere solamente un par trenzado de cable de cobre. Adicionalmente, la red local telefónica existente y la transferencia digital de datos pueden ser soportadas simultáneamente por SDSL. La distancia de operación de la tecnología SDSL es de 3,048 metros. La aplicación típica de SDSL es la misma de HDSL, con la diferencia de que SDSL tiene una importante ventaja sobre HDSL: es apropiada para usuarios residenciales aunque estos usualmente tienen solamente un par trenzado de cobre. SDSL transmite señales T1 o E1 sobre un par trenzado. Puede soportar estándares de transmisión de la línea telefónica y simultáneamente sobre T1/E1. La tecnología SDSL es recomendable para pequeños suscriptores (como usuarios en el hogar) equipados con una línea telefónica individual. Utiliza un sólo par obteniendo velocidades de 760Kbps en ambas direcciones. Se está tratando de hacerla llegar a los 2Mbps de la norma E1. De toda la familia, SDSL es la opción idónea para las empresas ya que permite ofrecer una gama amplia de servicios:

- Telefonía (líneas analógicas/accesos básicos ISDN/primarios ISDN).
- Acceso a Internet de banda ancha simétrica.
- Circuitos punto a punto.
- Interconexión de LAN's.
- Empaquetamiento de servicios sobre la misma línea: Voz + Internet + Datos.
- Limitaciones tecnológicas.

La tecnología SDSL está limitada en cuanto al ancho de banda en función de la longitud del par de cobre. La tabla 31 muestra a título orientativo la velocidad máxima alcanzable según la longitud del bucle:

Longitud nominal (Km)	Payload bitrate (kbits/s)
1,38	2304 (s)
1,56	2048 (s)
1,82	1536
2,11	1280
2,44	1024
2,77	768
3,54	512
4,11	384

Tabla 31

6.4 MPLS

6.4.1 INTRODUCCION

El crecimiento imparable de Internet, así como la demanda sostenida de nuevos y más sofisticados servicios, supone cambios tecnológicos fundamentales respecto a las prácticas habituales desarrolladas a en los años 90. Nuevas tecnologías de transmisión sobre fibra óptica, tales como Dense Wavelength Division Multiplexing (DWDM), proporcionan una eficaz alternativa a ATM para multiplexar múltiples servicios sobre circuitos individuales. Además, los tradicionales conmutadores ATM están siendo desplazados por una nueva generación de routers con funciones especializadas en el transporte de paquetes en el núcleo de las redes. Esta situación se complementa con la arquitectura de red, conocida como Multi-Prototocol Label Switching (MPLS). MPLS se considera fundamental en la construcción de los nuevos cimientos para Internet del siglo. MPLS es hoy día una solución clásica y estándar al transporte de información en las redes. Aceptado por toda la comunidad de Internet, ha sido hasta hoy una solución aceptable para el envío de información, utilizando Routing de paquetes con ciertas garantías de entrega. A su vez, los avances en el hardware y una nueva visión a la hora de manejar las redes, están dando lugar al empleo creciente de las tecnologías de Conmutación, encabezadas por la tecnología ATM. Aportando velocidad, calidad de servicio y facilitando la gestión de los recursos en la red. De aquí derivan los siguientes problemas: el paradigma del Routing está muy extendido en todos los entornos, tanto empresariales como académicos, etc. El rediseño total del software existente hacia la Conmutación supondría un enorme gasto de tiempo y dinero. Igualmente sucede con el hardware que está funcionando hoy en día. En la primera parte de la se analiza la evolución del routing en Internet desde mitad de los 90's y las motivaciones que han llevado a la adopción del estándar MPLS. Se aprovecha esta introducción para avanzar un aspecto fundamental de MPLS, que consiste en la clara separación entre las funciones de routing (es decir el control de la información sobre la topología y tráfico en la red), de las funciones de forwarding (es decir el envío en sí de datos entre elementos de la red).

La segunda parte se centra en la descripción funcional de MPLS, de los principales componentes que intervienen en esta arquitectura y de la actuación conjunta de los mismos. A continuación se pasa a discutir las ventajas de MPLS para el soporte de procedimientos de encaminamiento y envío de paquetes en backbones IP, y la posibilidad de proporcionar nuevas aplicaciones y servicios, en redes IP y en Internet en general. En concreto, se presenta la utilidad de MPLS para el soporte de aplicaciones de: ingeniería de tráfico, de diferenciación de servicios en distintas clases (CoS) y de establecimiento de redes privadas virtuales (VPN's) sobre una topología "inteligente", muy superior en prestaciones a las soluciones tradicionales de túneles y circuitos virtuales. Uno de los factores de éxito de Internet está en la acepción de los protocolos TCP/IP como estándar de facto para todo tipo de servicios y aplicaciones. Internet ha desplazado a las tradicionales redes de datos y ha llegado a ser el modelo de red pública del siglo XXI. Pero si bien es cierto que Internet puede llegar a consolidarse como el modelo de red pública de datos a gran escala, también lo es que no llega a satisfacer ahora todos los requisitos de los usuarios, principalmente los de aquellos de entornos corporativos, que necesitan la red para el soporte de aplicaciones críticas. Una carencia fundamental de Internet es la imposibilidad de seleccionar diferentes niveles de servicio para los distintos tipos de aplicaciones de usuario. Internet se valora más por el servicio de acceso y distribución de contenidos que por el servicio de transporte de datos, conocido como **"best-effort"**. Si el modelo Internet ha de consolidarse como la red de datos, se necesita introducir cambios tecnológicos fundamentales, que permitan ir más allá del nivel best-effort y puedan proporcionar una respuesta más determinística y menos aleatoria.

Junto a los últimos avances tecnológicos en transmisión por fibra óptica (principalmente DWDM), que lleva a conseguir anchos de banda de magnitudes muy superiores, y en tecnología de integración de circuitos ASIC (Application Specific Integrated Circuits), que permite aumentar enormemente la velocidad de proceso de información en la red, hemos de considerar la arquitectura MPLS, sustrato para la inclusión en la red de nuevas aplicaciones y para poder ofrecer diferentes niveles de servicio, en un entorno de mayor fiabilidad y con las necesarias garantías.

MPLS es un estándar emergente del IETF que surgió para consensuar diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes a mitad de los 90. Como concepto, MPLS es a veces un tanto difícil de explicar. Como protocolo es bastante sencillo, pero las implicaciones que supone su implementación real son enormemente complejas. Según el énfasis (o interés) que se ponga a la hora de explicar sus características y utilidad, MPLS se puede presentar como un sustituto de la conocida arquitectura IP sobre ATM. También como un protocolo para hacer túneles (sustituyendo a las técnicas habituales de "tunneling"). O bien, como una técnica para acelerar el encaminamiento de paquetes... incluso, ¿para eliminar por completo el routing? En realidad, MPLS hace un poco de todo eso, ya que integra sin discontinuidades los niveles de transporte y de red, combinando eficazmente las funciones de control del routing con la simplicidad y rapidez de la conmutación del nivel transporte. Pero, ante todo y sobre todo, debemos considerar MPLS como el avance más reciente en la evolución de las tecnologías de routing y forwarding en las redes IP, lo que implica una evolución en la manera de construir y gestionar estas redes. Los problemas que presentan las soluciones de IP sobre ATM, tales como la expansión sobre una topología virtual superpuesta, así como la complejidad de gestión de dos redes separadas y tecnológicamente diferentes, quedan resueltos con MPLS. Al combinar en uno sólo lo mejor de cada nivel (la inteligencia del routing con la rapidez del switching), MPLS ofrece nuevas posibilidades en la gestión de backbones, así como en la provisión de nuevos servicios de valor añadido. Para poder entender mejor las ventajas de la solución MPLS, vale la pena revisar antes los esfuerzos anteriores de integración de los niveles de transporte y de red que han llevado finalmente a la adopción del estándar MPLS.

6.4.2 MARCO TEORICO

MPLS (Multi-Protocol Label Switching) es una red privada IP que combina la flexibilidad de las comunicaciones punto a punto o Internet y la fiabilidad, calidad y seguridad de los servicios de Prívate Line, Frame Relay o ATM. Ofrece niveles de rendimiento diferenciados y priorización del tráfico, así como aplicaciones de voz y multimedia. Y todo ello en una única red. Contamos con distintas soluciones, una completamente gestionada que incluye el suministro y la gestión de los equipos en sus instalaciones (CPE). O bien, que sea el administrador quien los gestione.

- MPLS (Multiprotocol Label Switching) **intenta conseguir las ventajas de ATM, pero sin sus inconvenientes.**
- Asigna a los datagramas de cada flujo una etiqueta única que permite una conmutación rápida en los routers intermedios (sólo se mira la etiqueta, no la dirección de destino).
- **Las principales aplicaciones de MPLS** son:
  - Funciones de ingeniería de tráfico (a los flujos de cada usuario se les asocia una etiqueta diferente).
  - Policy Routing.
  - Servicios de VPN.
  - Servicios que requieren QoS.
- MPLS se basa en el etiquetado de los paquetes en base a criterios de prioridad y/o calidad (QoS).
- La idea de MPLS es realizar la conmutación de los paquetes o datagramas en función de las etiquetas añadidas en capa 2 y etiquetar dichos paquetes según la clasificación establecida por la QoS en la SLA.
- Por tanto MPLS es una tecnología que permite ofrecer QoS, independientemente de la red sobre la que se implemente.
- El etiquetado en capa 2 permite ofrecer servicio multiprotocolo y ser portable sobre multitud de tecnologías de capa de enlace: ATM, Frame Relay, líneas dedicadas, LAN's.

6.4.2.1 ORIGENES DE MPLS

Para poder crear los circuitos virtuales como en ATM, se pensó en la utilización de etiquetas añadidas a los paquetes. Estas etiquetas definen el circuito virtual por toda la red.

- Estos circuitos virtuales están asociados con una QoS determinada, según el SLA.

- Inicialmente se plantearon dos métodos diferentes de etiquetamiento, en capa 3 o en capa 2.
- La opción de capa 2 es más interesante, porque es independiente de la capa de red o capa 3 y además permite una conmutación más rápida, dado que la cabecera de capa 2 está antes de capa 3.

Ejemplo de arquitectura

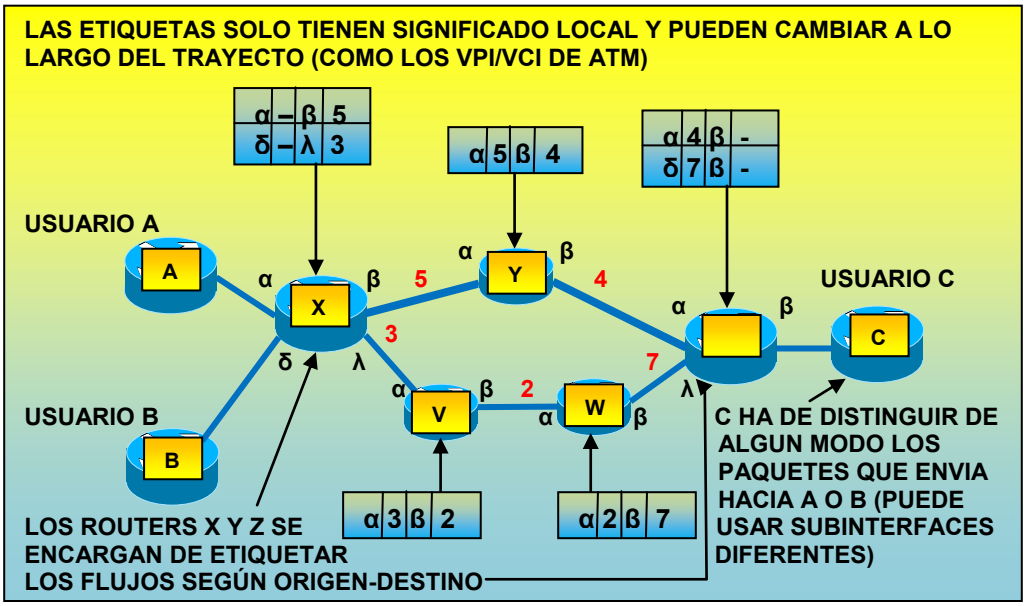


Figura 195 Conmutación MPLS

Conmutación de etiquetas en un LSR a la llegada de un paquete:

- Examina la etiqueta del paquete entrante y la interfaz por donde llega.
- Consulta la tabla de etiquetas.
- Determina la nueva etiqueta y la interfaz de salida para el paquete.

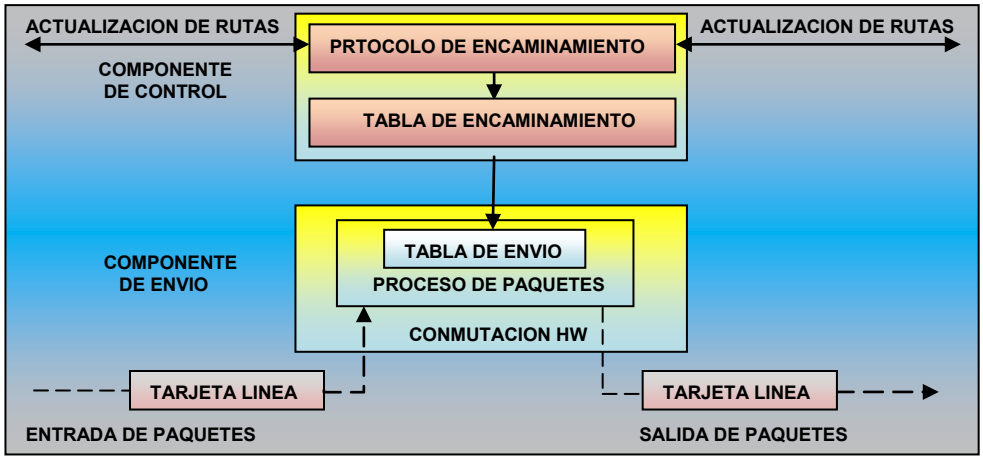


Figura 196 MPLS y pila de etiquetas

6.4.2.2 FUNCIONAMIENTO DE MPLS

Jerarquía MPLS

- MPLS funciona sobre multitud de tecnologías de nivel de enlace.
- La etiqueta MPLS se coloca delante del paquete de red y detrás de la cabecera de nivel de enlace.

- Las etiquetas pueden anidarse, formando una pila con funcionamiento LIFO (Last In, First Out). Esto permite ir agregando (o segregando) flujos. El mecanismo es escalable.
- Cada nivel de la pila de etiquetas define un nivel de LSP Túneles MPLS.
- Así dentro de una red MPLS se establece una jerarquía de LSP's.
- En ATM y Frame Relay la etiqueta MPLS ocupa el lugar del campo VPI/VCI o en el DLCI, para aprovechar el mecanismo de conmutación inherente.

Etiquetas MPLS

- Las etiquetas MPLS identifican a la FEC asociada a cada paquete.
- Etiqueta MPLS genérica:

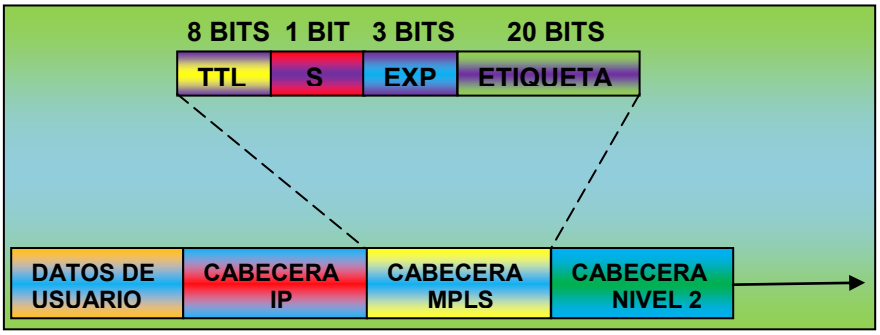


Figura 197 Formato de la etiqueta MPLS: 32 bits

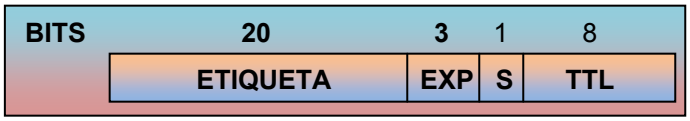


Figura 198 Situación de la etiqueta MPLS

ETIQUETA: La etiqueta propiamente dicha que identifica una FEC (con significado local).
EXP: Bits para uso experimental; una propuesta es transmitir en ellos información de DiffServ.
S: Vale 1 para la primera entrada en la pila (la más antigua), cero para el resto. Esta es la primera etiqueta introducida.
TTL: Contador del número de saltos. Este campo reemplaza al TTL de la cabecera IP durante el viaje del datagrama por la red MPLS.

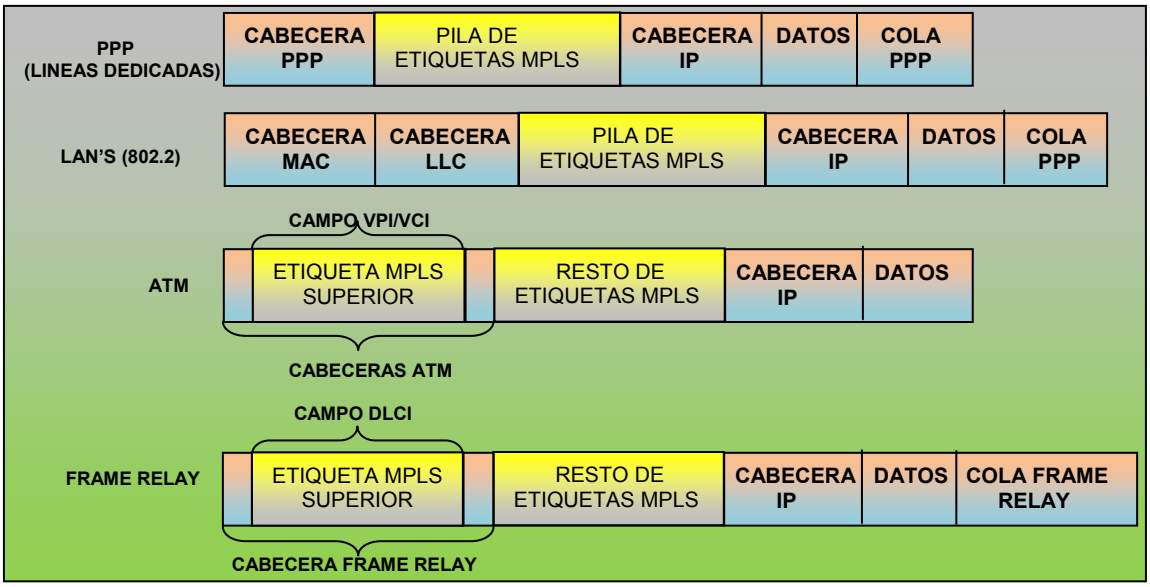


Figura 199

Routing MPLS

- Los paquetes se envían en función de las etiquetas.
- No se examina la cabecera de red completa.
- El direccionamiento es más rápido.
- Cada paquete es clasificado en unas clases de tráfico denominadas FEC *(Forwarding Equivalence Class).*
- Los LSP's por tanto definen las asociaciones FEC-etiqueta.

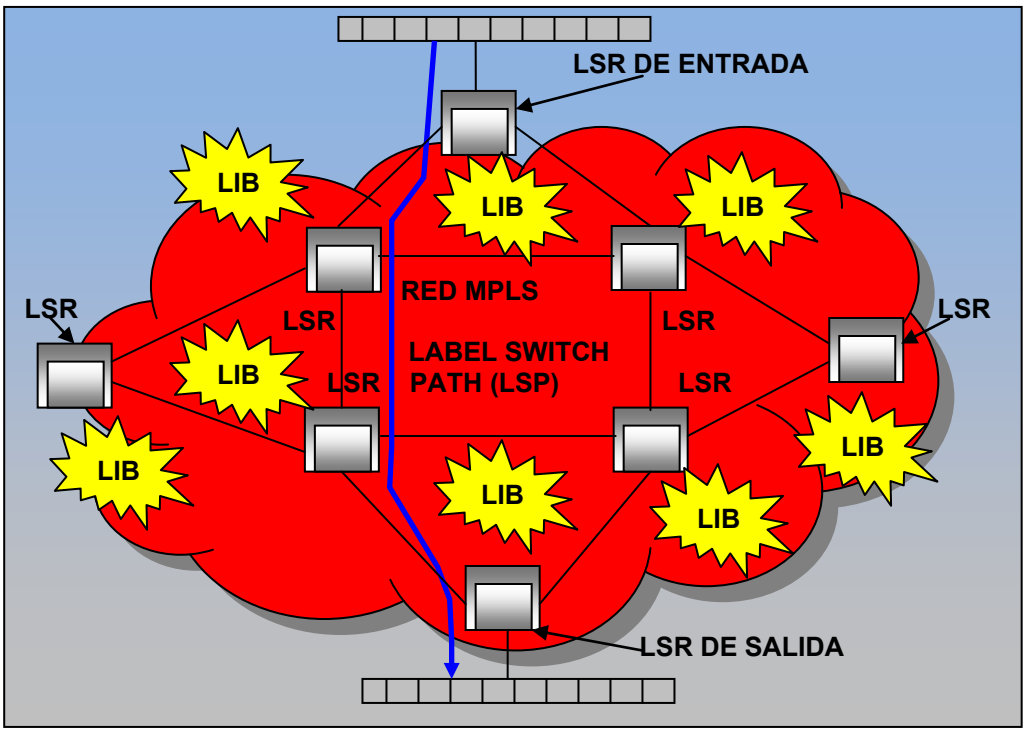


Figura 200 Ejemplo de MPLS

- Esta es una red MPLS en la cual se ven todos sus componentes.
- La línea azul representa el LDP entre el LSR de entrada y el LSR de salida.

6.4.3 EL CAMINO HACIA LA CONVERGENCIAS DE NIVELES: IP/ATM

A mediados de los 90 IP fue ganando terreno como protocolo de red a otras arquitecturas en uso (SNA, IPX, AppleTalk, OSI). Por otro lado, hay que recordar que los backbones IP que los proveedores de servicio (NSP) habían empezado a desplegar en esos años estaban construidos a base de routers conectados por líneas dedicadas T1/E1 y T3/E3. El crecimiento explosivo de Internet había generado un déficit de ancho de banda en aquel esquema de enlaces individuales. La respuesta de los NSP's fue el incremento del número de enlaces y de la capacidad de los mismos. Del mismo modo, los NSP's se plantearon la necesidad de aprovechar mejor los recursos de red existentes, sobre todo la utilización eficaz del ancho de banda de todos los enlaces. Con los protocolos habituales de encaminamiento (basados en métricas del menor número de saltos), ese aprovechamiento del ancho de banda global no resultaba efectivo. Había que idear otras alternativas de ingeniería de tráfico. Como consecuencia, se impulsaron los esfuerzos para poder aumentar el rendimiento de los routers tradicionales. Estos esfuerzos trataban de combinar, de diversas maneras, la eficacia y la rentabilidad de los conmutadores ATM con las capacidades de control de los routers IP. A favor de integrar los niveles de transporte y de red estaba el hecho de las infraestructuras de redes ATM que estaban desplegando los operadores de telecomunicación. Estas redes ofrecían entonces (1995-97) una buena solución a los problemas de crecimiento de los NSP's. Por un lado, proporcionaba mayores velocidades (155Mpbs) y, por otro, las características

de respuesta determinística de los circuitos virtuales ATM posibilitaban la implementación de soluciones de ingeniería de tráfico. El modelo de red "IP sobre ATM" (IP/ATM) pronto ganó adeptos entre la comunidad de NSP's, a la vez que facilitó la entrada de los operadores telefónicos en la provisión de servicios IP y de conexión a Internet al por mayor.

El funcionamiento IP/ATM supone la superposición de una topología virtual de routers IP sobre una topología real de conmutadores ATM. El backbone ATM se presenta como una nube central (el núcleo) rodeada por los routers de la periferia. Cada router comunica con el resto mediante los circuitos virtuales permanentes (PVC's) que se establecen sobre la topología física de la red ATM. Los PVC's actúan como circuitos lógicos y proporcionan la conectividad necesaria entre los routers de la periferia. Estos, sin embargo, desconocen la topología real de la infraestructura ATM que sustenta los PVC's. Los routers ven los PVC's como enlaces punto a punto entre cada par. En la figura 201 se representa un ejemplo en el que se puede comparar la diferencia entre la topología física de una red ATM con la de la topología lógica IP superpuesta sobre la anterior.

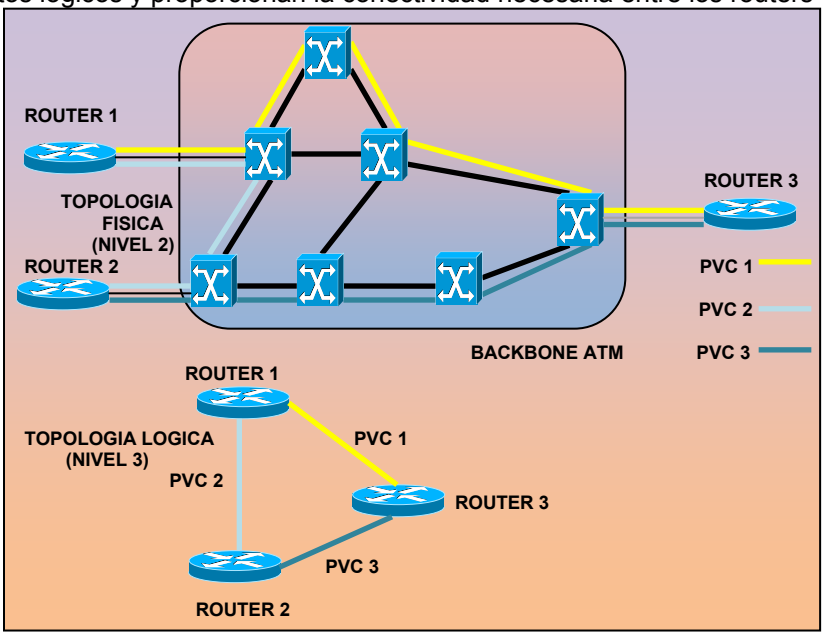


Figura 201

La base del modelo IP/ATM está en la funcionalidad proporcionada por el nivel ATM, es decir, los controles de software (señalización y routing) y el envío de las celdas por hardware (conmutación). En realidad, los PVC's se establecen a base de intercambiar etiquetas en cada conmutador de la red, de modo que la asociación de etiquetas entre todos los elementos ATM determina los correspondientes PVC's. (Más adelante se verá que el intercambio de etiquetas es uno de los componentes fundamentales en la arquitectura MPLS). Las etiquetas tienen solamente significado local en los conmutadores y son la base de la rapidez en la conmutación de celdas. La potencia de esta solución de topologías superpuestas está en la infraestructura ATM del backbone; el papel de los routers IP queda relegado a la periferia, que, a mitad de los 90, tenían una calidad cuestionable, al estar basados en funcionamiento por software. En la figura 202 se representa el modelo IP/ATM con la separación de funciones entre lo que es routing IP en el nivel de red (control y envío de paquetes) y lo que es conmutación en el nivel de transporte (control/señalización y envío de celdas). Aunque se trata de una misma infraestructura física, en realidad existen dos redes separadas, con diferentes tecnologías, con diferente funcionamiento y, lo que quizás es más sorprendente, concebidas para dos finalidades totalmente distintas. La solución de superponer IP sobre ATM permite aprovechar la infraestructura ATM existente. Las ventajas inmediatas son el ancho de banda disponible a precios competitivos y la rapidez de transporte de datos que proporcionan los conmutadores. En los casos de NSP's de primer nivel ellos poseen y operan el backbone ATM al servicio de sus redes IP. Los caminos físicos de los PVC's se calculan a partir de la necesidades del tráfico IP, utilizando la clase de servicio ATM UBR (Unspecified Bit Rate), ya que en este caso el ATM se utiliza solamente como infraestructura de transporte de alta velocidad (no hay necesidad de apoyarse en los mecanismos inherentes de ATM para control de la congestión y clases de servicio). La ingeniería de tráfico se hace a base de proporcionar a los

routers los PVC's necesarios, con una topología lógica entre routers totalmente mallada. El "punto de encuentro" entre la red IP y la ATM está en el acoplamiento de las subinterfaces en los routers con los PVC's, a través de los cuales se intercambian los routers la información de encaminamiento correspondiente al protocolo interno IGP. Lo habitual es que, entre cada par de routers, haya un PVC principal y otro de respaldo, que entra automáticamente en funcionamiento cuando falla el principal.

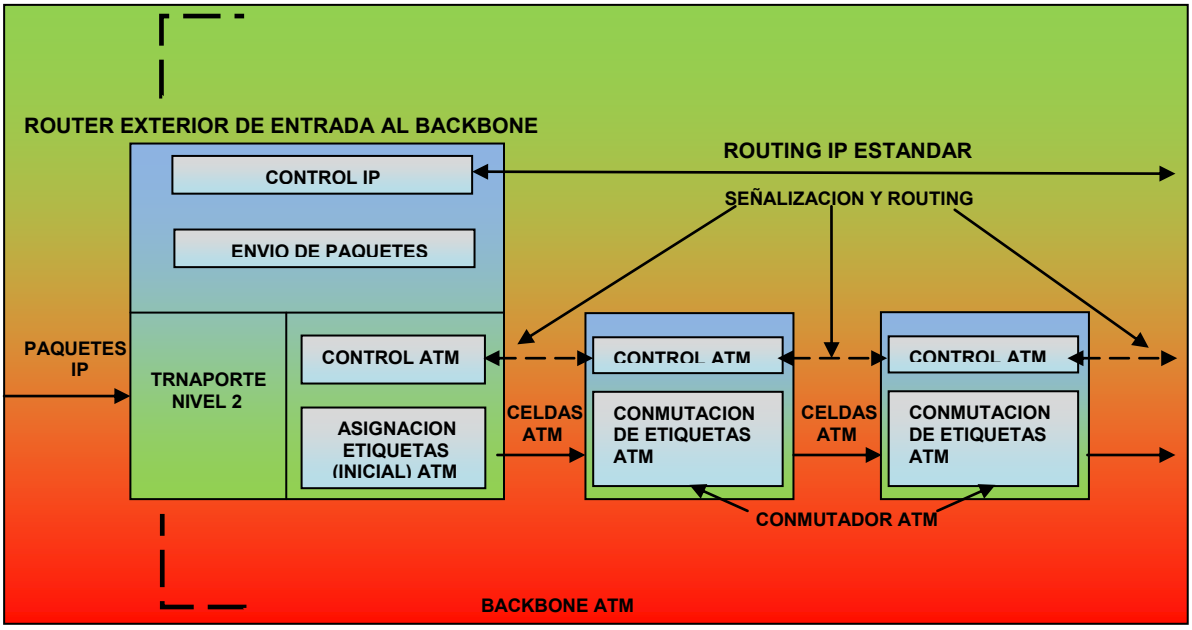


Figura 202

Sin embargo, el modelo IP/ATM tiene también sus inconvenientes: hay que gestionar dos redes diferentes, una infraestructura ATM y una red lógica IP superpuesta, lo que supone a los proveedores de servicio mayores costos de gestión global de sus redes. Existe, además, lo que se llama la **"tasa impuesta por la celda"**, un overhead aproximado del 20% que causa el transporte de datagramas IP sobre las celdas ATM y que reduce en ese mismo porcentaje el ancho de banda disponible. Por otro lado, la solución IP/ATM presenta los típicos problemas de crecimiento exponencial n x (n-1) al aumentar el número de nodos IP sobre una topología completamente mallada. Piénsese, por ejemplo, en una red con 5 routers externos con una topología virtual totalmente mallada sobre una red ATM. Son necesarios 5 x 4 =20 PVC's (uno en cada sentido de transmisión). Si se añade un sexto router se necesitan 10 PVC's más para mantener la misma estructura (6 x 5=30). Una paga adicional del crecimiento exponencial de rutas es el mayor esfuerzo que tiene que hacer el correspondiente protocolo IGP. Como conclusión, podemos decir que el modelo IP/ATM, si bien presenta ventajas evidentes en la integración de los niveles de transporte y de red, lo hace de modo discontinuo, a base de mantener dos redes separadas. MPLS logra esa integración de niveles sin discontinuidades.

6.4.4 UN PASO MÁS EN LA CONVERGENCIA HACIA IP: CONMUTACIÓN IP

La convergencia continuada hacia IP de todas las aplicaciones existentes, junto a los problemas de rendimiento derivados de la solución IP/ATM, llevaron posteriormente (1997-98) a que varios fabricantes desarrollasen técnicas para realizar la integración de niveles de forma efectiva, sin las discontinuidades señalas anteriormente. Esas técnicas se conocieron como **"conmutación IP"** (IP switching) o "conmutación multinivel" (multilayer switching). Una serie de tecnologías privadas (entre las que merecen citarse: IP Switching de Ipsilon Networks, Tag Switching de Cisco, Aggregate Route-Base IP Switching (ARIS) de IBM, IP Navigator de Cascade/Ascend/Lucent y Cell Switching Router (CSR) de Toshiba condujeron finalmente a la adopción del actual estándar MPLS del IETF. El problema que presentaban tales soluciones era la falta de interoperatividad, ya que

usaban diferentes tecnologías privadas para combinar la conmutación del nivel de transporte con el encaminamiento IP (nivel de red). Se resume a continuación los fundamentos de esas soluciones integradoras, ya que permitirá luego comprender mejor la esencia de la solución MPLS.

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

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

En la figura 196 se representa la separación funcional de esas dos componentes, una de control y la otra de envío. La componente de control utiliza los protocolos estándar de encaminamiento (OSPF, IS-IS y BGP-4) para el intercambio de información con los otros routers para la construcción y el mantenimiento de las tablas de encaminamiento. Al llegar los paquetes, la componente de envío busca en la tabla de envío, que mantiene la componente de control, para tomar la decisión de encaminamiento para cada paquete. En concreto, la componente de envío examina la información de la cabecera del paquete, busca en la tabla de envío la entrada correspondiente y dirige el paquete desde la interfaz de entrada a la de salida a través del correspondiente hardware de conmutación. Al separar la componente de control (encaminamiento) de la componente de envío, cada una de ellas se puede implementar y modificar independientemente. El único requisito es que la componente de encaminamiento mantenga la comunicación con la de envío mediante la tabla de envío de paquetes y actualice la información. El mecanismo de envío se implementa mediante el intercambio de etiquetas, similar a lo visto para ATM. La diferencia está en que ahora lo que se envía por la interfaz física de salida son paquetes "etiquetados". De este modo, se está integrando realmente en el mismo sistema las funciones de conmutación y de encaminamiento.

En cuanto a la etiqueta que marca cada paquete, decir que es un campo de unos pocos bits, de longitud fija, que se añade a la cabecera del mismo y que identifica una "clase equivalente de envío" (Forwarding Equivalence Class, FEC). Una FEC es un conjunto de paquetes que se envían sobre el mismo camino a través de una red, aún cuando sus destinos finales sean diferentes. Por ejemplo, en el encaminamiento convencional IP por prefijos de red (longest-match) una FEC serían todos los paquetes unicast cuyas direcciones de destino tengan el mismo prefijo. Realmente, una etiqueta es similar a un identificador de conexión (como el VPI/VCI de ATM o el DLCI de Frame Relay). Tiene solamente significado local y, por consiguiente, no modifica la información de la cabecera de los paquetes; tan sólo los encapsula, asignando el tráfico a los correspondientes FEC. El algoritmo de intercambio de etiquetas permite así la creación de "caminos virtuales" conocidos como LSP (Label-Switched Paths), funcionalmente equivalentes a los PVC's de ATM y Frame Relay. En el fondo, lo que hace es imponer una conectividad entre extremos a una red no conectiva por naturaleza, como son las redes IP, pero todo ello sin perder la visibilidad del nivel de red (de aquí los nombres de conmutación IP o conmutación multinivel). Esta es la diferencia básica con el modelo IP/ATM.

6.4.5 IDEAS PRECONCEBIDAS SOBRE MPLS

Durante el tiempo en que se ha desarrollado el estándar, se han extendido algunas ideas falsas o inexactas sobre el alcance y objetivos de MPLS. Hay quien piensa que MPLS se ha desarrollado para ofrecer un estándar a los vendedores que les permitiese evolucionar los conmutadores ATM a routers de backbone de altas prestaciones. Aunque esta puede haber sido la finalidad original de los desarrollos de conmutación multinivel, los recientes avances en tecnologías de silicio ASIC permite a los routers funcionar con una rapidez similar para la consulta de tablas a las de los conmutadores ATM. Si bien es cierto que MPLS mejora notablemente el rendimiento del mecanismo de envío de paquetes, éste no era el principal objetivo del grupo del IETF. Los objetivos establecidos por ese grupo en la elaboración del estándar eran:

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

- MPLS debía permitir el crecimiento constante de Internet.
- MPLS debía ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

También ha habido quien pensó que MPLS perseguía eliminar totalmente el encaminamiento convencional por prefijos de red. Esta es otra idea falsa y nunca se planteó como objetivo del grupo, ya que el encaminamiento tradicional de nivel 3 siempre sería un requisito en Internet por los siguientes motivos:

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

6.4.6 DESCRIPCION FUNCIONAL DE MPLS

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

- **Funcionamiento del envío de paquetes en MPLS**.-La base del MPLS está en la asignación e intercambio de etiquetas ya expuesto, que permiten el establecimiento de los caminos LSP por la red. Los LSP's son simplex por naturaleza (se establecen para un sentido del tráfico en cada punto de entrada a la red); el tráfico dúplex requiere dos LSP's, uno en cada sentido. Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un "conmutador de etiquetas" (Label-Switching Router) a otro, a través del dominio MPLS. Un LSR no es sino un router especializado en el envío de paquetes etiquetados por MPLS.
  Al igual que en las soluciones de conmutación multinivel, MPLS separa las dos componentes funcionales de control (routing) y de envío (forwarding). Del mismo modo, el envío se implementa mediante el intercambio de etiquetas en los LSP's. Sin embargo, MPLS no utiliza ninguno de los protocolos de señalización ni de encaminamiento definidos por el ATM Forum; en lugar de ello, en MPLS o bien se utiliza el protocolo RSVP o bien un nuevo estándar de señalización (el Label Distribution Protocol, LDP, del que se tratará más adelante). Pero, de acuerdo con los requisitos del IETF, el transporte de datos puede ser cualquiera. Si éste fuera ATM, una red IP habilitada para MPLS es ahora mucho más sencilla de gestionar que la solución clásica IP/ATM. Ahora ya no hay que administrar dos arquitecturas diferentes a base de transformar las direcciones IP y las tablas de encaminamiento en las direcciones y el encaminamiento ATM: esto lo resuelve el procedimiento de intercambio de etiquetas MPLS. El papel de ATM queda restringido al mero transporte de datos a base de celdas. Para MPLS esto es indiferente, ya que puede utilizar otros transportes como Frame Relay, o directamente sobre líneas punto a punto.

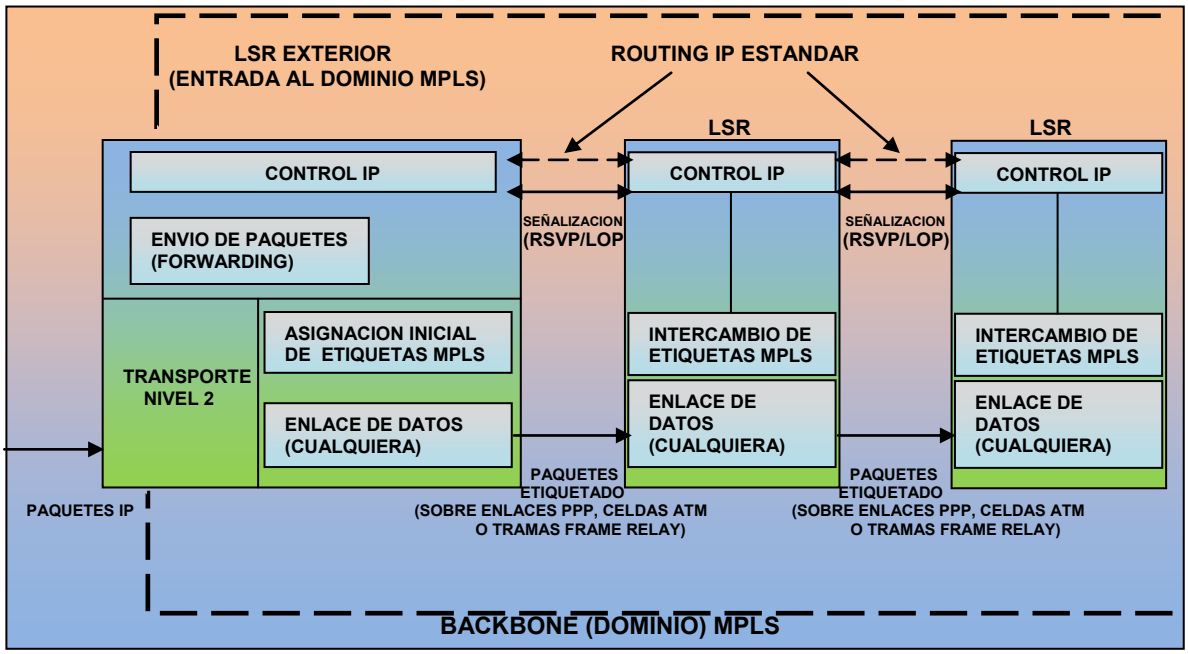
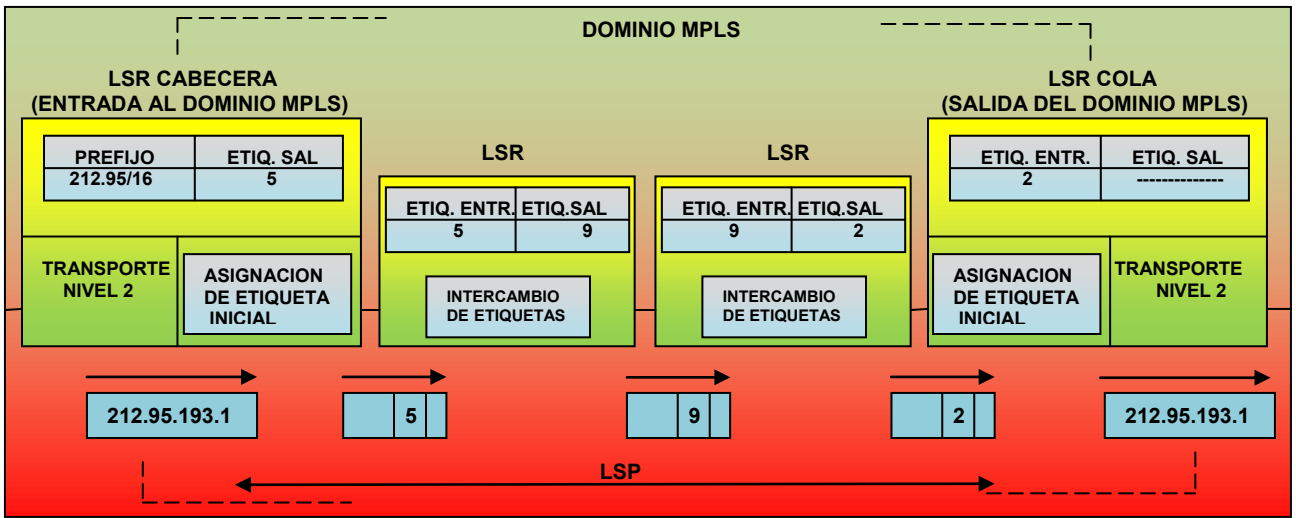


Figura 203

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

Figura 204

El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera. En la figura 205 el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LSR consulta la tabla de encaminamiento y asigna el paquete a la clase FEC definida por el grupo 212.95/16. Asimismo, este LSR le asigna una etiqueta y envía el paquete al siguiente LSR del LSP. Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente



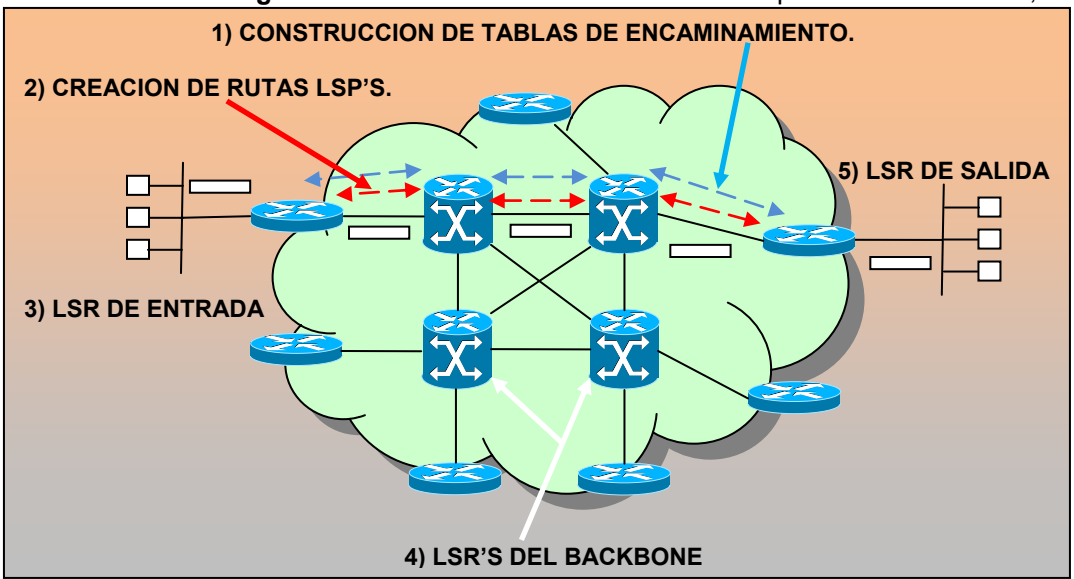
(tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas. Al llegar el paquete al LSR de cola (salida), ve que el siguiente salto lo saca de la red MPLS; al consultar ahora la tabla de conmutación de etiquetas quita ésta y envía el paquete por routing convencional.

Figura 205

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

- **Control de la información en MPLS**.-Hasta ahora se ha visto el mecanismo básico de envío de paquetes a través de los LSP's mediante el procedimiento de intercambio de etiquetas según las tablas de los LSR's. Pero queda por ver dos aspectos fundamentales:
  - Cómo se generan las tablas de envío que establecen los LSP's.
  - Cómo se distribuye la información sobre las etiquetas a los LSR's.

  El primero de ellos está relacionado con la información que se tiene sobre la red: topología, patrón de tráfico, características de los enlaces, etc. Es la información de control típica de los algoritmos de encaminamiento. MPLS necesita esta información de routing para establecer los caminos virtuales LSP's. Lo más lógico es utilizar la propia información de encaminamiento que manejan los protocolos internos IGP (OSPF, IS-IS, RIP...) para construir las tablas de encaminamiento (recuérdese que los LSR son routers con funcionalidad añadida). Esto es lo que hace MPLS precisamente: para cada "ruta IP" en la red se crea un "camino de etiquetas" a base de concatenar las de entrada/salida en cada tabla de los LSR's; el protocolo interno correspondiente se encarga de pasar la información necesaria. El segundo aspecto se refiere a la información de "señalización". Pero siempre que se quiera establecer un circuito virtual se necesita algún tipo de señalización para marcar el camino, es decir, para la distribución de etiquetas entre los nodos. Sin embargo, la arquitectura MPLS no asume un único protocolo de distribución de etiquetas; de hecho se están estandarizando algunos existentes con las correspondientes extensiones; unos de ellos es el protocolo RSVP del Modelo de Servicios Integrados del IETF. Pero, además, en el IETF se están definiendo otros nuevos, específicos para la distribución de etiquetas, cual es el caso del Label Distribution Protocol (LDP).
- **Funcionamiento global MPLS**.-Una vez vistos todos los componentes funcionales, el



esquema global de funcionamiento es el que se muestra en la figura 206, donde quedan reflejadas las diversas funciones en cada uno de los elementos que integran la red MPLS. Es importante destacar que en el borde de la nube MPLS tenemos una red convencional de routers IP. El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de routers a una distancia de un sólo salto. Funcionalmente es como si estuvieran unidos todos en una topología mallada (directamente o por PVC's ATM). Ahora, esa unión a un sólo salto se realiza por MPLS mediante los correspondientes LSP's (puede haber más de uno para cada par de routers). La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y que no se pierde la visibilidad sobre los paquetes IP. Todo ello abre enormes posibilidades a la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario, tal como se explica en la sección siguiente.

Figura 206

6.4.7 APLICACIONES DE MPLS

- **Redes de alto rendimiento**: las decisiones de encaminamiento que han de tomar los routers MPLS en base a la LIB son mucho más sencillas y rápidas que las que toma un router IP ordinario (la LIB es mucho más pequeña que una tabla de rutas normal). La anidación de etiquetas permite agregar flujos con mucha facilidad, por lo que el mecanismo es escalable.
- **Ingeniería de Tráfico**: se conoce con este nombre la planificación de rutas en una red en base a previsiones y estimaciones a largo plazo con el fin de optimizar los recursos y reducir congestión.
- **QoS**: es posible asignar a un cliente o a un tipo de tráfico una FEC a la que se asocie un LSP que discurra por enlaces con bajo nivel de carga.
- **VPN**: la posibilidad de crear y anidar LSP's da gran versatilidad a MPLS y hace muy sencilla la creación de VPN's.
- **Soporte multiprotocolo**: los LSP's son válidos para múltiples protocolos, ya que el encaminamiento de los paquetes se realiza en base a la etiqueta MPLS estándar, no a la cabecera de nivel de red.

6.4.7.1.-INGENIERÍA DE TRÁFICO

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén suprautilizados, con posibles puntos calientes y cuellos de botella, mientras otros puedan estar infrautilizados. A comienzos de los 90 los esquemas para adaptar de forma efectiva los flujos de tráfico a la topología física de las redes IP eran bastante rudimentarios. Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente. En casos de congestión de algunos enlaces, el problema se resolvía a base de añadir más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos). En el esquema de la figura 207 se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino. El camino más corto entre A y B según la métrica normal IGP es el que tiene sólo dos saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los routers correspondientes haga aconsejable la utilización del camino alternativo indicado con un salto más. MPLS es una herramienta efectiva para esta aplicación en grandes backbones, ya que:

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.
- Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.
- Permite hacer "encaminamiento restringido" (Constraint-based Routing, CBR), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios

especiales (distintos niveles de calidad). Por ejemplo, con garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.

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

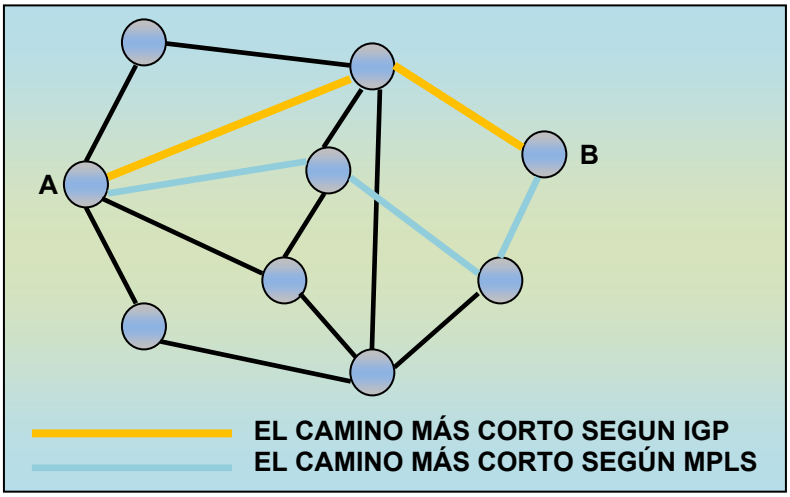


Figura 207

6.4.7.2 CLASE DE SERVICIO (CoS)

MPLS está diseñado para poder cursar servicios diferenciados, según el Modelo DiffServ del IETF. Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de vídeo y voz interactiva. Para ello se emplea el campo ToS (Type of Service), rebautizado en DiffServ como el octeto DS. Esta es la técnica QoS de marcar los paquetes que se envían a la red. MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP. De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que:

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

6.4.7.3 REDES PRIVADAS VIRTUALES (VPN'S)

Una red privada virtual (VPN) se construye a base de conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPN's es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y vídeo sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces. Las IP/VPN's son soluciones de comunicación VPN basada en el protocolo de red IP de Internet. En esta sección se va a describir brevemente las ventajas que MPLS ofrece para este tipo de redes frente a otras soluciones tradicionales. Las VPN's tradicionales se han

venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada. Tal es el caso de las redes de datos Frame Relay, que permiten establecer PVC's entre los diversos nodos que conforman la VPN. La seguridad y las garantías las proporcionan la separación de tráficos por PVC y el caudal asegurado (CIR). Algo similar se puede hacer con ATM, con diversas clases de garantías. Los inconvenientes de este tipo de solución es que la configuración de las rutas se basa en procedimientos más bien artesanales, al tener que establecer cada PVC entre nodos, con la complejidad que esto supone al proveedor en la gestión (y los mayores costos asociados). Si se quiere tener conectados a todos con todos, en una topología lógica totalmente mallada, añadir un nuevo emplazamiento supone retocar todos los CPE's del cliente y restablecer todos los PVC's.

Además, la popularización de las aplicaciones TCP/IP así como la expansión de las redes de los NSP's, ha llevado a tratar de utilizar estas infraestructuras IP para el soporte de VPN's, tratando de conseguir una mayor flexibilidad en el diseño e implantación y unos menores costos de gestión y provisión de servicio. La forma de utilizar las infraestructuras IP para servicio VPN (IP/VPN) ha sido la de construir túneles IP de diversos modos. El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados. Lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de tuberías privadas por las que no puede entrar nadie que no sea miembro de esa IP/VPN. Los túneles IP en conexiones dedicadas se pueden establecer de dos maneras:

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

En las VPN's basadas en túneles IPSec, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte por la red del proveedor. Es relativamente sencillo de implementar, bien sea en dispositivos especializados, tales como cortafuegos, como en los propios routers de acceso del NSP. Además, como es un estándar, IPSec permite crear VPN's a través de redes de distintos NSP's que sigan el estándar IPSec. Pero como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS son bastante limitadas, ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles de servicio. Además, sólo vale para paquetes IP nativos, IPSec no admite otros protocolos. En los túneles de nivel 2 se encapsulan paquetes multiprotocolo (no necesariamente IP), sobre los datagramas IP de la red del NSP. De este modo, la red del proveedor no pierde la visibilidad IP, por lo que hay mayores posibilidades de QoS para priorizar el tráfico por tipo de aplicación IP. Los clientes VPN pueden mantener su esquema privado de direcciones, estableciendo grupos cerrados de usuarios, si así lo desean. (Además de encapsular los paquetes, se puede cifrar la información por mayor seguridad, pero en este caso limitando las opciones QoS). A diferencia de la opción anterior, la operación de túneles de nivel 2 está condicionada a un único proveedor. A pesar de las ventajas de los túneles IP sobre los PVC's, ambos enfoques tienen unas características comunes que las hacen menos eficientes frente a la solución MPLS:

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

Realmente, el problema que plantean estas IP/VPN's es que están basadas en un modelo topológico superpuesto sobre la topología física existente, a base de túneles extremo a extremo (o circuitos virtuales) entre cada par de routers de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos. Con una arquitectura MPLS se obvian estos

inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPN's se implementan mediante los caminos LSP's creados por el mecanismo de intercambio de etiquetas MPLS. Los LSP's son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo. Aquí está la diferencia: en los túneles se utiliza el encaminamiento convencional IP para transportar la información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de routing IP. Sin embargo, sí se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada de rutas MPLS sino que ve una Internet privada (intranet) entre los miembros de su VPN. De este modo, se pueden aplicar técnicas QoS basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hasta el destino, pudiendo así reservar ancho de banda, priorizar aplicaciones, establecer CoS y optimizar los recursos de la red con técnicas de ingeniería de tráfico. La diferencia entre los túneles IP convencionales (o los circuitos virtuales) y los "túneles MPLS" (LSP's) está en que éstos se crean dentro de la red, a base de LSP's, y no de extremo a extremo a través de la red.

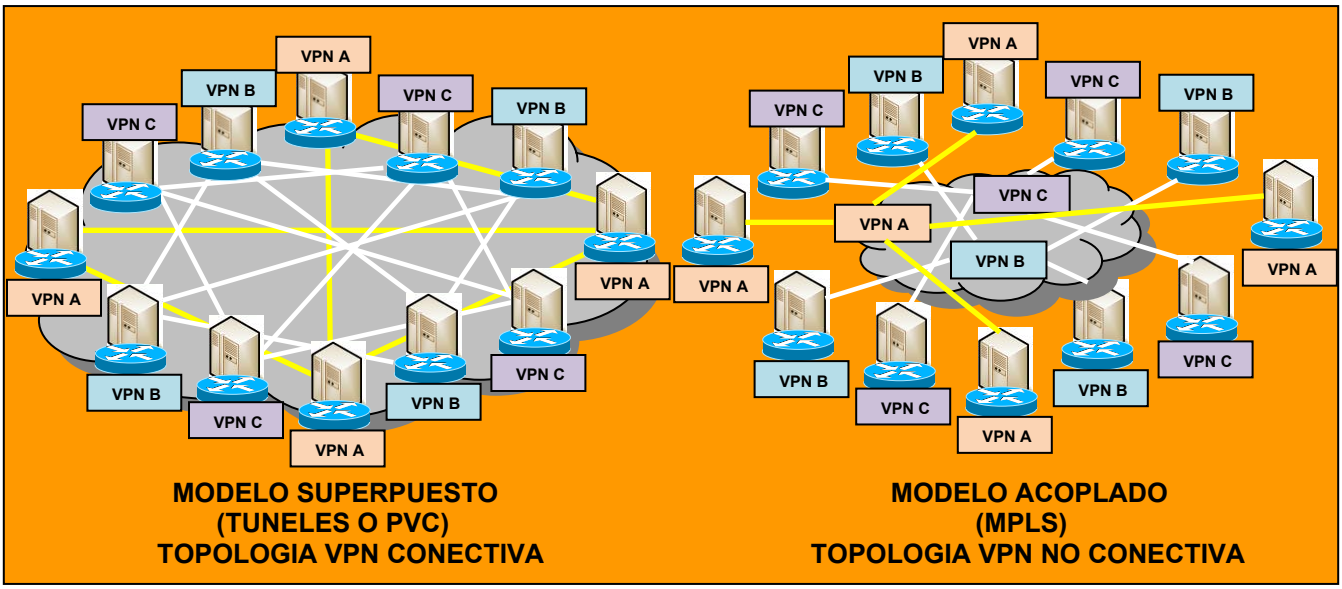


Figura 208

Como resumen, las ventajas que MPLS ofrece para IP/VPN's son:

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

6.4.7.4 DIEZ RAZONES PARA MIGRAR A MPLS/VPN

En los últimos tiempos, no sólo se viene hablando de la famosa convergencia de Voz, Video y Datos sobre una misma plataforma, sino también de la necesidad de la migración de servicios "Legacy" (heredados) como ATM o Frame Relay a una nueva generación de "IPbased VPN's" (Redes Privadas Virtuales basadas en protocolo IP) como los son las "MPLS/VPN's" (Redes Privadas Virtuales basadas en Multiprotocol Label Switching). Sin embargo, resistencia sigue siendo la primera palabra que se asocia cuando se habla de "cambios", mucho más aún, cuando se trata de migraciones de servicios de comunicaciones, críticos para una empresa. A continuación, encontraremos 10 razones claves para hacer frente a la mencionada "resistencia" a los cambios cuando una empresa, corporación u organismo este pensando en migrar su infraestructura Legacy actual a una IP-Based MPLS/VPN

1 - Flexibilidad.

Cada empresa, corporación u organismo tiene desarrollada su propia estructura interna, tanto en infraestructura como en recursos humanos, generadas en base a sus necesidades y recursos disponibles. En base a ésta estructura, muchas veces única, se montan los servicios de comunicaciones para acomodar de la mejor manera posible y al menor costo, el transporte de la información interna, así como también externa, con sus clientes y proveedores. La topología de una MPLS/VPN puede acomodarse acorde a cada necesidad, dada su naturaleza que brinda conexiones "Any-to-Any" (cualquiera con cualquiera) entre los distintos puntos que comprenden la VPN, contando así con el mejor camino o ruta entre cada punto. A su vez se puede obtener mayor flexibilidad realizando configuraciones híbridas con Hub-and-Spoke (estrella), por ejemplo en las conexiones con clientes.

2 - Escalabilidad.

Con un nuevo concepto de aprovisionamiento, llamado "Point-to-Cloud" (punto a la nube), se implementan los nuevos puntos de la VPN. Este concepto proviene del hecho de que cada vez que sea necesario "subir" un nuevo punto a la VPN, sólo habrá que configurar el equipamiento del Service Provider que conecte este nuevo punto. De esta forma, evitamos tareas complejas y riesgosas, como las que se producen cuando se activa un nuevo punto en una red basada en circuitos virtuales de Frame Relay o ATM, en donde es necesario re-configurar TODOS los puntos involucrados.

3 - Accesibilidad.

La arquitectura de MPLS/VPN permite utilizar prácticamente todas las tecnologías de acceso para interconectar las oficinas del cliente con su "Service Provider" (Proveedor de Servicios). Por dicho motivo, la versatilidad que nos permite utilizar xDSL o un enlace Wireless Ethernet en las oficinas más pequeñas y hasta incluso en usuarios móviles, mientras que en el headquarter utilizamos leased lines (TDM) en altas capacidades como E3/T3, nos permite dimensionar cada punto de la VPN acorde a sus necesidades sin limitar o restringir la de otros puntos.

4 - Eficiencia.

En una infraestructura 100% IP, es decir, aquellas empresas en donde todo el equipamiento involucrado y las aplicaciones utilizadas son IP-based, el uso de servicios de transporte ATM o Frame Relay someten al cliente a incurrir en un costo adicional por el overhead que los protocolos de transporte introducen. Mediante IFX MPLS/VPN - un servicio IP-Based VPN - este costo extra desaparece.

5 - Calidad de servicio (QoS) y Clases de servicio (CoS).

Las necesidades de comunicación entre dos lugares remotos, hoy en día van mucho más allá de la simple transferencia de datos vía e-mail, web u otras aplicaciones. Siendo incluso insuficiente muchas veces, la interesante combinación de voz y datos bajo una misma plataforma. Es por esto, que la ya mencionada Convergencia de datos con aplicaciones real-time y/o interactivas, voz y también video de alta calidad, necesitan de una eficiente plataforma de transporte. Mediante la utilización de técnicas y herramientas de Calidad de Servicio (QoS), se ofrecen distintas Clases de Servicio (CoS) dentro de una MPLS/VPN para complementar los requerimientos de cada servicio o aplicación.

6 - Administración.

Las MPLS/VPN son denominadas Network-Based, ésta característica proviene del hecho en que el servicio es implementado sobre la infraestructura del Service Provider; implicando, entre otras

cosas, que la administración de enrutamiento es llevada a cabo por el Service Provider; quien por su naturaleza, es especialista en dicha tarea desligando así al cliente de llevarla a cabo.

7 - Monitoreo y SLA's.

Las MPLS/VPN son monitoreadas, controladas y con un constante seguimiento en forma permanente, las 24 horas los 7 días de la semana, por parte del Service Provider. Además, se extienden "Service Level Agreements" (acuerdos de nivel de servicio) para garantizar y asegurar la estabilidad y performance que el cliente necesite.

8 - Fácil Migración.

La simplicidad de la tecnología determina que las tareas de aprovisionamiento, administración y mantenimiento sean actividades sencillas para el Service Provider; lo cual se traslada directamente al cliente, obteniendo una migración del servicio actual sin complicaciones.

9 - Seguridad.

Análisis y estudios realizados por los distintos fabricantes y entidades especializadas en el área, determinaron que los niveles de seguridad entregados por una MPLS/VPN son comparables con los entregados por los circuitos virtuales de Frame Relay y ATM. Sin embargo, en escenarios donde estos niveles no son suficientes, como por ejemplo en las necesidades de entidades financieras, una MPLS/VPN puede también ser combinada con la encriptación y autenticación que IPSec brinda, elevando aún más la seguridad de la VPN.

10 -Bajo Costo.

Son varios los motivos que permiten afirmar que un servicio MPLS/VPN ofrece "más por menos", entre ellos podemos destacar:

Independencia de equipos de cliente (CPE): al ser un servicio Network-based, la implementación de la VPN no requiere un hardware específico ni costoso para ser instalado en las oficinas del cliente.

Convergencia: por ser una VPN CoS-Aware (Soporte de Clases de Servicio) se puede integrar distintos servicios y aplicaciones sobre una misma plataforma. De este modo, empresas que al día de hoy mantienen distintos y costosos servicios para soportar sus necesidades de voz, datos y video; pueden unificar estos requerimientos concluyendo en un ahorro significativo y manteniendo relación con un único proveedor de servicios.

6.5 TCP/IP

6.5.1 INTRODUCCIÓN

Las redes se han convertido en una parte fundamental, sino la más importante, de los actuales sistemas de información. Constituyen el pilar en el uso compartido de la información en empresas así como en grupos gubernamentales y científicos. Esta información puede adoptar distintas formas, sea como documentos, datos a ser procesados por otra computadora, ficheros enviados a colegas, e incluso formas más exóticas de datos.

La mayoría de estas redes se instalaron a finales de los años 60 y 70, cuando el diseño de redes se consideraba como la piedra filosofal de la investigación informática y la tecnología punta. Dio lugar a numerosos modelos de redes como la tecnología de conmutación de paquetes, redes de área local con detección de colisión, redes jerárquicas en empresas, y muchas otras de elevada calidad. Desde comienzos de los '70, otro aspecto de la tecnología de redes cobró importancia: el modelo de pila de protocolo, que permite la interoperabilidad entre aplicaciones. Toda una gama de arquitecturas fue propuesta e implementada por diversos equipos de investigación y fabricantes de computadoras. El resultado de todos estos conocimientos tan prácticos es que hoy en día cualquier grupo de usuarios puede hallar una red física y una arquitectura adecuada a sus necesidades específicas, desde líneas asíncronas de bajo costo, sin otro método de recuperación de errores que una función de paridad bit a bit, pasando por funciones completas de redes de área extensa (pública o privada) con protocolos fiables como redes públicas de conmutación de paquetes o redes privadas SNA, hasta las redes de área local, de alta velocidad pero distancia limitada. El lado negativo de esta explosión de la información es la penosa situación que se produce cuando un grupo de usuarios desea extender su sistema informático a otro grupo de usuarios, que resulta que

tiene una tecnología y unos protocolos de red diferentes. En consecuencia, aunque pudieran ponerse de acuerdo en el tipo de tecnología de red para conectar físicamente sus instalaciones, las aplicaciones (como por ejemplo sistemas de correo) serían aún incapaces de comunicarse entre sí debido a los diferentes protocolos.

Se tomó conciencia de esta situación bastante temprano (a comienzo de los '70), gracias a un grupo de investigadores en los Estados Unidos, que fueron artífices de un nuevo paradigma: **la interconexión de redes**. Otras organizaciones oficiales se implicaron en la interconexión de redes, tales como ITU-T e ISO. Todas trataban de definir un conjunto de protocolos, distribuidos en un conjunto bien definido de capas, de modo que las aplicaciones pudieran comunicarse entre sí, con independencia de la tecnología de red subyacente y del sistema operativo sobre el que se ejecutaba cada aplicación. Los diseñadores originales de la pila de protocolos ARPANET, subvencionados por DARPA **(Defense Advanced Research Projects Agency)** introdujeron conceptos fundamentales tales como la **estructura de capas** y el de **virtualidad** en el mundo de las redes, bastante antes de que ISO se interesase en las redes. El organismo oficial de esos investigadores fue el **Grupo de Trabajo en Red (Network Working Group)** llamado **ARPANET**, que tuvo su última reunión general en octubre de 1971. DARPA ha continuado su investigación en busca de una pila de protocolos de red, desde el protocolo host-a-host **NCP (Network Control Program)** a la pila de protocolos TCP/IP, que adoptó la forma que tiene en la actualidad alrededor de 1978. En esa época, DARPA era un organismo famoso por ser pionero en la conmutación de paquetes a través de redes de radio y canales de satélite. La primera implementación real de **Internet** fue se produjo sobre 1980, cuando DARPA comenzó a convertir las máquinas de su red de trabajo (ARPANET) a los nuevos protocolos de TCP/IP. En 1983 la transición fue completa y DARPA exigió que todas las estaciones que quisieran conectarse a ARPANET usaran TCP/IP.

DARPA contrató además a **Bolt, Beranek y Newman (BNN)** para desarrollar una implementación de los protocolos TCP/IP para el UNIX de Berkeley sobre el VAX y dotaron a la Universidad de California en Berkeley para que distribuyese ese código de modo gratuito con su sistema operativo UNIX. El primer lanzamiento de la distribución del sistema de Berkeley que incluyó el protocolo TCP/IP estuvo disponible en 1983 (BSD 4.2). Desde ese momento, TCP/IP se ha difundido rápidamente entre universidades y centros de investigación y se ha convertido en el estándar de subsistemas de comunicación basados en UNIX. El segundo lanzamiento (BSD 4.3) se distribuyó en 1986, que es actualizado en 1988 (BSD 4.3 Tahoe) y en 1990 (BSD 4.3 Reno). BSD 4.4 fue distribuido en 1993. Debido a limitaciones de fondos, el BSD 4.4 será la última distribución que hará el **Grupo de Investigación de Sistemas Informáticos (Computer Systems Research Group)** de la Universidad de California en Berkeley. A medida que TCP/IP se extendía rápidamente, nuevas WAN's se fueron creando y uniendo a ARPANET en los Estados Unidos. Por otro lado, redes de otros tipos, no necesariamente basadas en TCP/IP, se añadieron al conjunto de redes interconectadas. El resultado fue lo que hoy se conoce como **INTERNET**.

La palabra **Internet** es simplemente una contracción de la frase **red interconectada**. Sin embargo, escrita con mayúscula hace referencia a un conjunto mundial de redes interconectadas, de tal forma que Internet es una red interconectada, aunque no a la inversa. A Internet se le llama a veces **Interred Conectada (Connected Internet)**. Internet está constituida por los siguientes grupos de redes:

- **Troncales**: grandes redes que existen principalmente para interconectar otras redes. Actualmente las redes troncales son NSFNET en US, EBONE en Europa y las grandes redes troncales comerciales.
- **Redes regionales** que conectan, por ejemplo, universidades y colegios.
- **Redes comerciales** que suministran acceso a troncales y suscriptores, y redes propiedad de organizaciones comerciales para uso interno que también tienen conexión con Internet.
- **Redes locales**, como por ejemplo, redes a nivel de campus universitario.

En muchos casos, particularmente en redes de tipo comercial, militar y gubernamental, el tráfico entre estas y el resto de Internet está restringido. El **Ping**, es un programa usado para determinar si un host de una red es alcanzable; está implementado en cualquier plataforma TCP/IP. Si la respuesta es no, entonces no estás conectado. Esta definición no implica necesariamente que uno

esté totalmente aislado de Internet: muchos sistemas que fallarían en este test tienen, por ejemplo, pasarelas de correo electrónico a Internet.

El protocolo TCP/IP es uno de los protocolos más ampliamente usados en todo el mundo, y por esta razón merece la pena profundizar en este protocolo en particular. OSI y TCP/IP son pilas de protocolos distintos. En el caso de TCP/IP es mejor utilizar OSI sólo como modelo de referencia teórico y estudiar en profundidad el verdadero modelo TCP/IP. Los protocolos que se utilizan en las comunicaciones son una serie de normas que deben aportar las siguientes funcionalidades:

- Permitir localizar un ordenador de forma inequívoca.
- Permitir realizar una conexión con otro ordenador.
- Permitir intercambiar información entre ordenadores de forma segura, independiente del tipo de maquinas que estén conectadas (PC, Mac, AS-400).
- Abstraer a los usuarios de los enlaces utilizados (red telefónica, radioenlaces, satélite...) para el intercambio de información.
- Permitir liberar la conexión de forma ordenada.

Debido a la gran complejidad que conlleva la interconexión de computadoras, se ha tenido que dividir todos los procesos necesarios para realizar las conexiones en diferentes niveles. Cada nivel se ha creado para dar una solución a un tipo de problema particular dentro de la conexión. Cada nivel tendrá asociado un protocolo, el cual entenderán todas las partes que formen parte de la conexión. Diferentes empresas han dado diferentes soluciones a la conexión entre computadoras, implementando diferentes familias de protocolos, y dándole diferentes nombres (DECnet, TCP/IP, IPX/SPX, NETBEUI, etc.). Cuando se habla de TCP/IP, se relaciona automáticamente como el protocolo sobre el que funciona Internet. Esto, en cierta forma es cierto, ya que se le llama TCP/IP, a la familia de protocolos que nos permite estar conectados Internet. Este nombre viene dado por los dos protocolos estrella de esta familia:

- **El protocolo TCP**, funciona en el nivel de transporte del modelo de referencia OSI, proporcionando un transporte fiable de datos.
- **El protocolo IP**, funciona en el nivel de red del modelo OSI, que nos permite encaminar nuestros datos hacia otras maquinas.

Pero un protocolo de comunicaciones debe solucionar una serie de problemas relacionados con la comunicación entre computadoras, además de los que proporciona los protocolos TCP e IP.

6.5.2 ARQUITECTURA DE PROTOCOLOS TCP/IP

Para poder solucionar los problemas que van ligados a la comunicación de computadoras dentro de la red Internet, se tienen que tener en cuenta una serie de particularidades sobre las que ha sido diseñada TCP/IP:

- Los programas de aplicación no tienen conocimiento del hardware que se utilizara para realizar la comunicación (módem, tarjeta de red)
- La comunicación no esta orientada a conexión, eso quiere decir que cada paquete de información es independiente, y puede viajar por caminos diferentes entre dos estaciones.
- La interfaz de usuario debe ser independiente del sistema, así los programas no necesitan saber sobre que tipo de red trabajan.
- El uso de la red no impone ninguna topología en especial (distribución de las distintas computadoras).

De esta forma, podremos decir, que dos redes están interconectadas, si hay una estación común que pase información de una red a otra. Además, también podremos decir que una Internet virtual realizara conexiones entre redes, que ha cambio de pertenecer a la gran red, colaboraran en el trafico de información procedente de una red cualquiera, que necesite de ella para acceder a una red remota. Todo esto independiente de las estaciones que implementen estas funciones, y de los sistemas operativos que estas utilicen. Toda arquitectura de protocolos se descompone en una serie de niveles, usando como referencia el modelo OSI. Esto se hace para poder dividir el problema global en subproblemas de más fácil solución. A diferencia de OSI, formado por una torre de siete niveles, TCP/IP se descompone en cinco niveles, cuatro niveles software y un nivel hardware. TCP/IP más que un protocolo es un conjunto de protocolos. Se ha convertido en el

estándar de intercomunicación de redes de área extensa y es el único protocolo de enlace y transporte permitido en Internet. La idea general de conectar una red con computadoras diferentes partió de las investigaciones llevadas a cabo en la **Defense Advanced Research Projects Agency (DARPA)**. En el ámbito de esta investigación, DARPA desarrollo el conjunto de protocolos TCP/IP para establecer comunicaciones entre redes e implantó una red que recibió el nombre de ARPAnet, que más tarde se convirtió en Internet. El conjunto de protocolos TCP/IP define los formatos y normas utilizados en la transmisión y recepción de información con independencia de cualquier tipo de hardware determinado u organización de red. A pesar de los protocolos se desarrollaron para Internet, TCP/IP se ha convertido en el estándar de hecho ya que muchas organizaciones públicas y privadas lo utilizan para su conectividad. El éxito inicial de TCP/IP fue debido a su inclusión en las diferentes variedades del sistema operativo UNIX y fue impulsado porque su implantación resulta más cómoda y económica que los protocolos equivalentes. TCP/IP emplea un modelo de enrutamiento basado en **datagramas** (paquetes) en lugar de circuitos virtuales. TCP/IP brinda a los arquitectos de sistemas e ingenieros de comunicaciones una independencia del hardware utilizado.

6.5.3 CONJUNTO DE PROTOCOLOS TCP/IP

En líneas generales, el conjunto de protocolos TCP/IP se corresponde con el modelo ISO. El modelo OSI describe un sistema de redes ideal que permite establecer una comunicación entre procesos de capas distintas y fáciles de identificar. En el host, las capas prestan servicios a capas superiores y reciben servicios de capas inferiores. La figura 209 muestra las siete capas del modelo de referencia OSI y su correspondencia general con las capas del conjunto de protocolos TCP/IP.

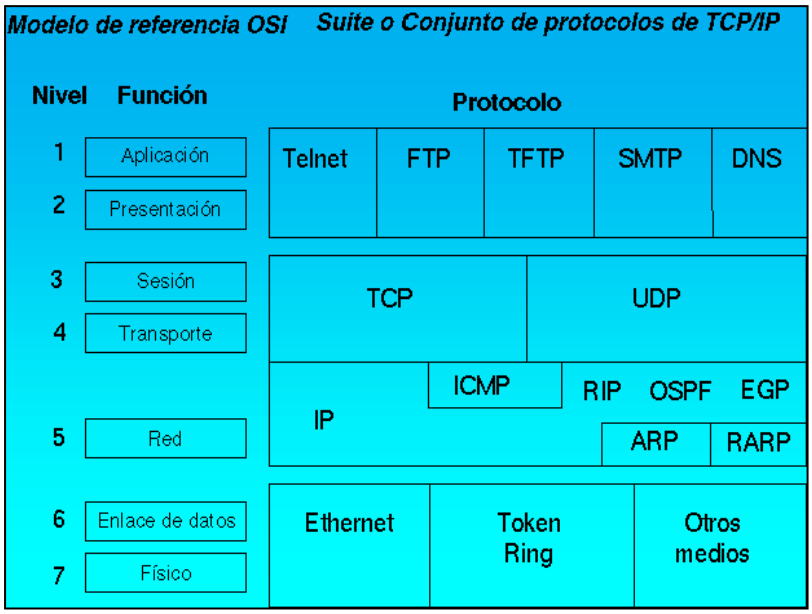


Figura 209 Modelo de referencia OSI y las capas de TCP/IP correspondientes

El sistema para determinar capas permite a los programadores concentrar sus esfuerzos en las funciones de una capa determinada. No es necesario que creen todo los mecanismos para enviar información a lo largo de la red. Sólo tienen que saber los servicios que el software debe proporcionar a la capa superior, los servicios que las capas inferiores pueden proporcionar al software y que protocolos del conjunto proporcionan estos servicios. A continuación se enumeran los protocolos más comunes del conjunto de protocolos TCP/IP, los servicios que proporcionan.

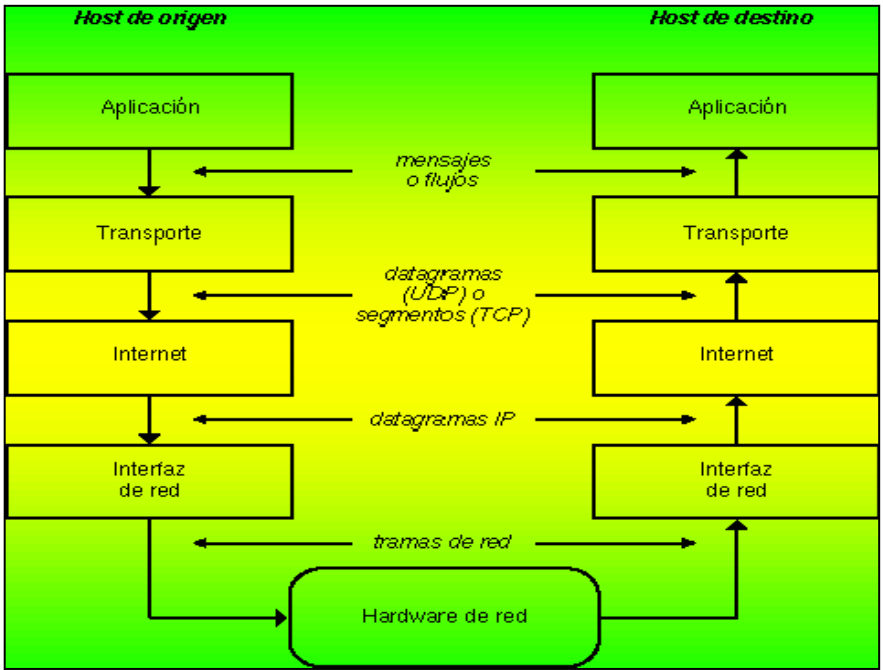
Protocolos TCP/IP	Servicio
Protocolo Internet (IP)	Proporciona servicios para la entrega de paquetes

	(encaminamiento) entre nodos.
Protocolo de Control de Mensaje Internet (ICMP)	Regula la transmisión de mensajes de error y control entre los host y los gateways.
Protocolo de Resolución de Direcciones (ARP)	Asigna direcciones Internet a direcciones físicas.
Protocolo de Resolución de Direcciones Invertidas (RARP)	Asigna direcciones físicas a direcciones Internet.
Protocolo de Control de Transmisión (TCP)	Proporciona servicios de envío de flujos fiables entre los clientes.
Protocolo de Datagrama de Usuario (UDP)	Proporciona servicio de entrega de datagramas no fiable entre clientes.
Protocolo de Transferencia de Archivos (FTP)	Proporciona servicios de nivel de aplicación para la transferencia de archivos.
TELNET	Proporciona un método de emulación de terminal.
Protocolo de Información de Encaminamiento (RIP)	Permite el intercambio de información de encaminamiento de vectores de distancia entre routers.
Protocolo Abrir la Vía Más Corta Primero (OPSF)	Permite el intercambio de información de encaminamiento de estado del enlace entre routers.
Protocolo Gateway Externo (EGP)	Permite el intercambio de información de encaminamiento entre routers externos.

6.5.4 DESCRIPCIÓN GENERAL DEL USO DE TCP/IP

Las aplicaciones que se desarrollan con TCP/IP, normalmente, usan varios protocolos del conjunto. La suma de las capas del conjunto de protocolos se conoce también como el stack de protocolo. Las aplicaciones definidas por el usuario se comunican con la capa superior del conjunto de protocolos. La capa de nivel superior del protocolo de la estación de origen traspasa la información a las capas inferiores del stack, que a su vez la pasan a la red física. La red física traspasa la información a la estación destino. Las capas inferiores del stack de protocolo de la estación destino pasan la información a las capas superiores, que a su vez la pasan a la aplicación del destino.

Cada capa del conjunto de protocolos TCP/IP tiene varias funciones; estas funciones son independientes de las otras capas. No obstante, cada capa espera recibir determinados servicios de la capa inferior y cada capa proporciona ciertos servicios a la capa superior. La figura 210 muestra las



diferentes capas del conjunto TCP/IP. Cada capa del stack de protocolo de la estación de origen se comunica con la misma capa de la estación destino. Las capas que se encuentran al mismo nivel de la estación origen y de destino son pares. Asimismo, la aplicación de la estación de origen y la del de destino también son pares. Desde el punto de vista del usuario o programador, la transferencia de paquetes se efectúa directamente de una capa par a otra.

Figura 210 Capas de los protocolos TCP/IP

El proceso que utiliza una aplicación para transferir el contenido de un archivo es el siguiente:
1. La capa de la aplicación envía un flujo de bytes a la capa de transporte de la estación de origen.
2. La capa de transporte divide el flujo en segmentos TCP, asigna un encabezado con un número de secuencia al segmento en cuestión y transmite este segmento a la capa de Internet (IP). Se calcula la suma de comprobación.
3. La capa de IP crea un paquete con parte de los datos que contiene el segmento TCP. La capa de IP añade al paquete un encabezado que indica las direcciones IP de origen y de destino. Esta capa también determina la dirección física de la estación destino o las estaciones que actúan como intermediarios hasta el host de destino. Entonces, envía el paquete y la dirección física a la capa de enlace de datos. Se vuelve a calcular la suma de comprobación.
4. La capa de enlace de datos transmite el paquete IP en la sección de datos de una trama de enlace de datos a la estación destino. Si la estación destino actúa como intermediario, el paso 3 volverá a repetirse hasta que se alcance el destino final.
5. Cuando se alcanza la estación destino, la capa de enlace de datos descarta el encabezado del enlace y envía el paquete IP a la capa de IP.
6. La capa de IP verifica el encabezado del paquete. Si la suma de comprobación del encabezado no coincide con la calculada por dicha capa, el paquete se ignora.
7. Si las sumas coinciden, la capa IP descarta el encabezado y envía el segmento TCP a la capa TCP correspondiente. Esta capa comprueba el número de secuencia para determinar si el segmento, es el segmento correcto de la secuencia.
8. La capa TCP calcula una suma de comprobación para los datos y el encabezado TCP. Si la suma no coincide con la suma transmitida con el encabezado, la capa TCP descarta el segmento. Si la suma coincide y el segmento está en la secuencia correcta, la capa TCP envía un reconocimiento al ordenador de destino.
9. La capa TCP descarta el encabezado TCP y transfiere los bytes del segmento que acaba de recibir a la aplicación.
10. La aplicación que se encuentra en la estación destino recibe un flujo de bytes como si estuviera conectado directamente a la aplicación del ordenador de origen.

6.5.5 PRICIPALES PROTOCOLOS DE INTERNET

Para dar una idea de la importancia de los principales protocolos, listamos algunos de ellos junto con su estado actual, status y STD donde es aplicable en Tabla 32 - Estado, status y números STD actuales de protocolos importantes de Internet. La lista completa se puede encontrar en RFC 1780 - Estándares de protocolos oficiales en Internet. **Leyenda:**
Estado: Std. = Estándar; Draft = Estándar provisional; Prop. = Propuesto como estándar; Info. = Informativo; Hist. = Histórico
Status: Req. = Requerido; Rec. = Recomendado; Ele. = Electivo; Not = No Recomendado

PRTOCOLO	NOMBRE	ESTADO	ESTATUS	STD
IP	Internet Protocol	Std	Req	5
ICMP	Internet Control Message Protocol	Std	Req	5
UDP	User Datagram Protocol	Std	Rec	6

TCP	Transmission Control Protocol	Std	Rec	7
TELNET	Telnet Protocol	Std	Rec	8
FTP	File Transfer Protocol	Std	Rec	9
SMTP	Simple Mail Transfer Protocol	Std	Rec	10
MAIL	Format of electronic Mail Message	Std	Rec	11
DOMAIN	Domain Name System	Std	Rec	13
DNS-MX	Mail Routing and the Domain System	Std	Rec	14
MIME	Multipurpose Internet Mail Extensions	Draft	Ele	
SNMP	Simple Network Management Protocol	Std	Rec	15
SMI	Structure of Management Information	Std	Rec	16
MIB-I	Management Information Base	Hist	Not	
MIB-II	Management Information Base-II	Std	Rec	17
NETBIOS	NetBios Services Protocol	Std	Ele	19
TFTP	Trivial File Transfer Protocol	Std	Ele	33
RIP	Routing Information Protocol	Std	Ele	34
ARP	Address Resolution Protocol	Std	Ele	37
RARP	Reverse Address Resolution Protocol	Std	Ele	38
GGP	Gateway To Gateway Protocol	Hist	Not	
BGP3	Border Gateway Protocol 3	Draft	Ele	
OSPF2	Open Shortest Path First Protocol V2	Draft	Ele	
IS-IS	OSI IS-IS for TCP/IP Dual Enviroments	Prop	Ele	
BOOTP	Bootstrap Protocol	Draft	Rec	
GOOPHER	The Internet Goopher Protocol	Info		
SUN-NFS	Network File System	Info		
SUN-RFC	Remote Procedure Call Protocol Version2	Info		

Tabla 32: Estado, status y números STD actuales de protocolos importantes de Internet

En el momento de escribir este documento, no hay ningún RFC asociado al protocolo de transferencia de hipertexto **HyperText Transfer Protocol (HTTP)** usado en implementaciones de la **World Wide Web**. Adicionalmente, los siguientes RFC's describen el **URL (Uniform Resource Locator)** y conceptos asociados a él:
RFC 1630 - Identificadores universales de recursos en WWW
RFC 1737 - Requerimientos funcionales para los **URN (Uniform Resource Names)**
RFC 1738 – URL (Uniform Resource Locators)

6.5.6 DIRECCIONES IP

El principal beneficio de IP es que es capaz de convertir un conjunto de redes físicamente distintas en una sola red aparentemente homogénea. Una Internet es una red IP aparentemente homogénea. Internet es la red de redes. La característica de Internet es que cada uno de los nodos tiene una dirección IP única y distinta a la de cualquier otro nodo. Las direcciones IP son cadenas de treinta y dos bits organizadas como una secuencia de cuatro bytes que se representa como 4 enteros entre 0 y 255. El número 0 se reserva para el número de la red y el número 255 es la dirección de difusión de la red, cualquier datagrama enviado a la dirección de difusión será recibido y procesado por todos los hosts de la red. Cada dirección IP de 4 bytes se divide en dos partes:

- Una porción de la red, que identifica la red.
- Una porción del Host, que identifica el nodo.

Las direcciones IP se dividen en tres clases según los dos bits más importantes de los cuatro primeros bytes. Esto se hace para que los routers puedan extraer la porción de la red de la dirección de manera eficiente. Todas las tramas (paquetes) IP llevan una dirección de origen (donde se origino la trama) y una dirección destino (a donde va la misma). Básicamente esto es todo lo que hay que saber cuando se conecta uno a la red y la dirección IP te la asigna un administrador de red.

Estas direcciones tienen una representación como cuatro números enteros separados por puntos y en notación decimal. Las direcciones representan la interfaz de conexión de un equipo con la red. Así, un host que está conectado a varias redes como regla general, no tendrá una única dirección de red, sino varias (normalmente una por cada red a la que esta conectado). Pero internamente, Esto no es del todo cierto. Las direcciones IP se dividen en dos partes (cada una con un cierto número de bits) cuyo significado tiene que ver con el sistema de enrutado de tramas. La primera parte (cuya longitud no es fija y depende de una serie de factores) representa la red, y debe ser igual para todos los hosts que estén conectados a una misma red física. La segunda parte representa el host, y debe ser diferente para todos los hosts que están conectados a la misma red física. El mecanismo de decisión de IP que hace que todas las tramas lleguen a su destino es el siguiente: Cuando la dirección origen y la dirección destino están ambas en la misma red (esto se sabe por que su dirección de red es igual en ambas, la dirección de red será la consecuencia de sustituir por ceros toda la parte de host en la dirección considerada) IP supone que existe un mecanismo de nivel inferior (en este caso Ethernet, Token Ring, etc.) que sabe como hacer llegar la trama hasta el host destino. Cuando la dirección de red origen y la de destino no coinciden, entonces hay que enrutar. Para enrutar, se dispone de una tabla que contiene entradas para cada una de las redes a las que se quieren hacer llegar tramas, que no sean locales a este host (un host, en general, esta conectado a varias redes, de las que hace de gateway (pasarela), si la dirección destino de la trama tiene una dirección de red que coincide con alguna de las direcciones de red propias (las que resultan de sustituir por ceros la parte de host en cada una de las interfaces, entonces no hace falta enrutar). Esta tabla tiene más o menos entradas en función de la complejidad de una Internet y la dirección del siguiente host en el camino hasta la red de destino. Por otro lado, la parte que corresponde a red y la parte que corresponde al host, se realiza usando este modelo (salvo para el subnetting, que añade algo de complejidad).

6.5.6.1 CLASES DE REDES

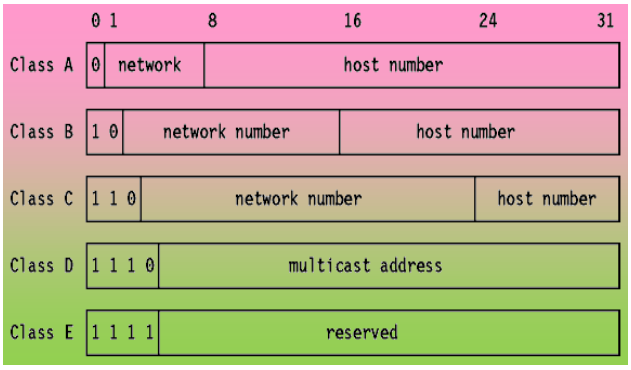
Existen unas clases de redes predeterminadas:

Red de Clase A	10.0.0.0	16, 777, 214 Hosts
Red de Clase B	10.88.0.0.	65, 534 Hosts
Red de Clase C	10.88.221.0.	254 Hosts

Cada dirección tiene una máscara que se determina en función de la dirección de la red. Para conocer, con exactitud, que parte de la dirección corresponde a la dirección de la red y que parte pertenece a la dirección del host, es necesario ver la máscara.

	Dirección Red	Máscara	Rango Hosts
Red de Clase A	10.0.0.0	255.0.0.0	16.777.214 Hosts
Red de Clase B	144.102.0.0.	255.255.0.0	65.534 Hosts
Red de Clase C	194.224.78.0.	255.255.255.0	254 Hosts

Los términos **dirección de red** y **netID** se usan a veces en vez de número de red, pero el término formal, utilizado en RFC 1166, es número de red. Análogamente, los términos **dirección de host** y **hostID** se usan ocasionalmente en vez de número de host. Hay cinco clases de direcciones



IP. Se muestran en la figura 211

Figura 211 Clases asignadas de direcciones de Internet.

Nota: Dos de los números de red de cada una de las clases A, B y C, y dos de los números de host de cada red están preasignados: los que tienen todos los bits a 0 y los que tienen todos los bits a 1.

Las direcciones de clase A usan 7 bits para el número de red permitiendo 126 posibles redes (veremos posteriormente que de cada par de direcciones de red y de host, dos tienen un significado especial). Los restantes 24 bits se emplean para el número de host, de modo que cada red tener hasta 16, 777, 214 hosts.
Las direcciones de clase B usan 14 bits para el número de red, y 16 bits para el de host, lo que supone 16,382 redes de hasta 65,534 hosts cada una.
Las direcciones de clase C usan 21 bits para el número de red y 8 para el de host, lo que supone 2, 097, 150 redes de hasta 254 hosts cada una.
Las direcciones de clase D se reservan para multicasting o multidifusión, usada para direccionar grupos de hosts en un área limitada.
Las direcciones de clase E se reservan para usos en el futuro

Es obvio que una dirección de clase A sólo se asignará a redes con un elevado número de hosts, y que las direcciones de clase C son adecuadas para redes con pocos hosts. Sin embargo, esto significa que las redes de tamaño medio (aquellas con más de 254 hosts o en las que se espera que en el futuro haya más de 254 hosts) deben usar direcciones de clase C. El número de redes de tamaño pequeño y medio ha ido creciendo muy rápidamente en los últimos años y se temía que, de haber permitido que se mantuviera este crecimiento, todas las direcciones de clase B se habrían usado para mediados de los '90. Esto es lo que se conoce como el problema del agotamiento de las direcciones IP. Un hecho a señalar en la división de la dirección IP en dos partes es que esta división a su vez divide en dos partes la responsabilidad de elegir una dirección IP. El número de red es asignado por el InterNIC y el de host por la autoridad que controla la red. El número de host puede dividirse aún más: esta división también es controlada por la autoridad propietaria de la red, y no por el InterNIC.

6.5.6.2 SUBREDES

Debido al crecimiento explosivo de Internet, el uso de direcciones IP asignadas se volvió demasiado rígido para permitir cambiar con facilidad la configuración de redes locales. Estos cambios podían ser necesarios cuando:

- Se instala una nueva red física.
- El crecimiento del número de hosts requiere dividir la red local en dos o más redes.
- Para evitar tener que solicitar direcciones IP adicionales en estos casos, se introdujo el concepto de **subred**.
- El número de host de la dirección IP se subdivide de nuevo en un número de red y uno de host. Esta segunda red se denomina subred. La red principal consiste ahora en un conjunto de subredes y la dirección IP se interpreta como <número de red<número de subred<número de host La combinación del número de subred y del host suele denominarse **dirección local** o **parte local**. La creación de subredes se implementa de forma que es transparente a redes remotas. Un host dentro de una red con subredes es consciente de la existencia de estas, pero un host de una red distinta no lo es; sigue considerando la parte local de la dirección IP como un número de host. La división de la parte local de la dirección IP en números de subred y de host queda a libre elección del administrador local; cualquier serie de bits de la parte local se puede tomar para la subred requerida. La división se efectúa empleando una **máscara de subred** que es un número de 32 bits. Los bits a cero en esta máscara indican posiciones de bits correspondientes al número de host, y los que están a uno, posiciones de bits correspondientes al número de subred. Las posiciones de la máscara pertenecientes al número de red se ponen a uno

pero no se usan. Al igual que las direcciones IP, las máscaras de red suelen expresarse en formato decimal.

El tratamiento especial de **todos los bits a cero** y **todos los bits a uno** se aplica a cada una de las tres partes de dirección IP con subredes del mismo modo que a una dirección IP que no las tiene. Por ejemplo, una red de clase B con subredes, que tiene un parte local de 16 bits, podría hacer uso de uno de los siguientes esquemas:
El primer byte es el número de subred, el segundo el de host. Esto proporciona 254 (256 menos dos, al estar los valores 0 y 255 reservados) posibles subredes, de 254 hosts cada una. La máscara de subred es 255.255.255.0.
Los primeros 12 bits se usan para el número de subred, y los 4 últimos para el de host. Esto proporciona 4,094 posibles subredes (4,096 menos 2), pero sólo 14 host por subred. La máscara de subred es 255.25.255.240. Hay muchas otras posibilidades. Mientras el administrador es totalmente libre de asignar la parte de subred a la dirección local de cualquier forma legal, el objetivo es asignar un **número** de bits al número de subred y el resto a la dirección local. Por tanto, es corriente usar un bloque de bits contiguos al comienzo de la parte local para el número de subred ya que así las direcciones son más legibles (esto es particularmente cierto cuando la subred ocupa 8 o 16 bits). Con este enfoque, cualquiera de las máscaras anteriores es buena, pero no máscaras como 255.255.252.252 o 255.255.255.15.

6.5.6.3 TIPOS DE SUBNETTING

Hay dos tipos de **subnetting**: **estático** y **de longitud variable**. El de longitud variable es el más flexible de los dos. El tipo de "subnetting" disponible depende del protocolo de encaminamiento en uso; el IP nativo sólo soporta "subnetting" estático, al igual que el ampliamente utilizado RIP. Sin embargo, la versión 2 del protocolo RIP soporta además "subnetting" de longitud variable.

6.5.6.3.1 SUBNETTING ESTÁTICO

El "subnetting" estático consiste en que todas las subredes de la red dividida empleen la misma máscara de red. Esto es simple de implementar y de fácil mantenimiento, pero implica el desperdicio de direcciones para redes pequeñas. Por ejemplo, una red de cuatro hosts que use una máscara de subred de 255.255.255.0 desperdicia 250 direcciones IP. Además, hace más difícil reorganizar la red con una máscara nueva. Hoy en día, casi todos los hosts y "routers" soportan "subnetting" estático.

6.5.6.3.1.1 EJEMPLO DE SUBNETTING ESTÁTICO

Asumamos que a nuestra red se le ha asignado el número de red IP de clase B 129.112. Tenemos que implementar múltiples redes físicas en nuestra red, y algunos de los "routers" que usaremos no admiten "subnetting" de longitud variable. Por tanto tendremos que elegir una máscara de subred para la totalidad de la red. Tenemos una dirección local de 16 bits para la red y debemos dividirla correctamente en dos partes. Por el momento, no preveremos tener más de 254 redes físicas, ni más de 254 hosts por red, de tal forma que una máscara de subred aceptable sería 255.255.255.0 (que además tiene la ventaja de ser legible). Esta decisión debe tomarse cuidadosamente, ya que será difícil cambiarla posteriormente. Si el número de redes o de hosts crece por encima de nuestras previsiones, puede que tengamos que implementar "subnetting" de longitud variable para usar al máximo las 65,534 direcciones locales de las que disponemos figura 212.

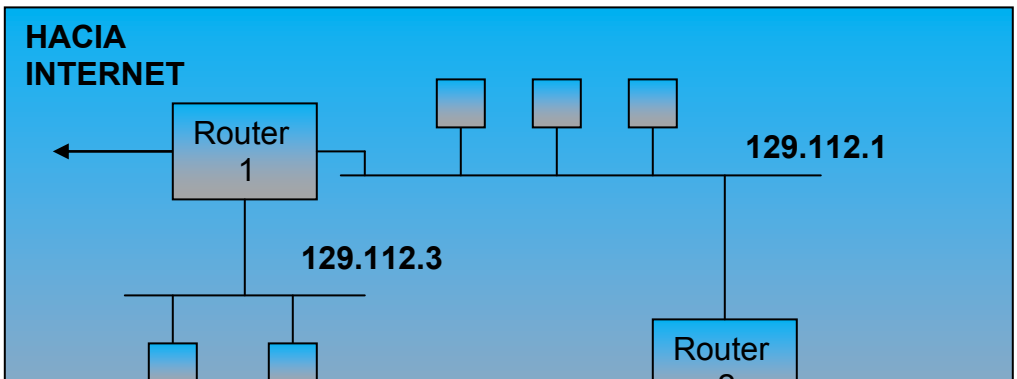


Figura 212: Una configuración de subred

Tres redes físicas forman una sola red IP. Los dos "routers" realizan tareas ligeramente diferentes. El "router" 1 actúa como "router" entre las subredes 1 y 3 así como para toda nuestra red y el resto de Internet. El "router" 2 actúa sólo como "router" entre las redes 1 y 2. Consideremos ahora una máscara de subred diferente: 255.255.255.240. El cuarto octeto se ha dividido por tanto en dos partes figura 213:

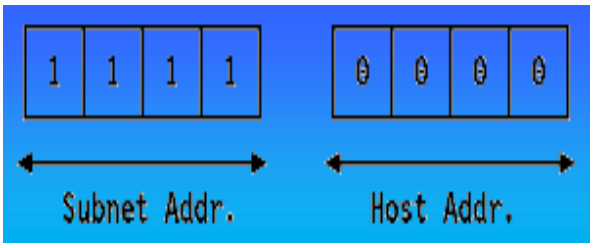


Figura 213

Para cada uno de estos valores de subred, sólo 14 direcciones (de la 1 a la 14) de hosts están disponibles, ya que sólo la parte derecha del octeto se puede usar y porque las direcciones 0 y 15 tienen un significado especial. De este modo, el número de subred 9.67.32.16 contendrá a los hosts cuyas direcciones IP estén en el rango de 9.67.32.17 a 9.67.32.30, y el número de subred 9.67.32.32 a los hosts cuyas direcciones IP estén en el rango de 9.67.32.33 a 9.67.32.46, etc. La siguiente tabla 33 contiene las posibles subredes que usarían esta máscara:

VALOR HEXADECIMAL	SUBRED
0000	0
0001	16
0010	32
0011	48
0100	64
0101	80
0110	96
0111	112
1000	128
1001	144
1010	160
1011	176

1100	192
1101	208
1110	224
1111	240

Tabla 33: Valores de subredes para la máscara de subred 255.255.255.240

6.5.6.3.2 SUBNETTING DE LONGITUD VARIABLE

Cuando se utiliza "subnetting" de longitud variable, las subredes que constituyen la red pueden hacer uso de diferentes máscaras de subred. Una subred pequeña con sólo unos pocos hosts necesita una máscara que permita acomodar sólo a esos hosts. Una subred con muchos puede requerir una máscara distinta para direccionar esa elevada cantidad de hosts. La posibilidad de asignar máscaras de subred de acuerdo a las necesidades individuales de cada subred ayuda a conservar las direcciones de red. Además, una subred se puede dividir en dos añadiendo un bit a la máscara. El resto de las subredes no se verán afectadas por el cambio. No todos los hosts y "routers" soportan "subnetting" de longitud variable. Sólo se dispondrán redes del tamaño requerido y los problemas de encaminamiento se resolverán aislando las redes que soporten "subnetting" de longitud variable. Un host que no soporte este tipo de "subnetting" debería disponer de una ruta de encaminamiento a un "router" que sí lo haga.

6.5.6.3.3 MEZCLANDO SUBNETTING ESTÁTICO Y DE LONGITU VARIABLE

A primera vista, parece que la presencia de un host que sólo puede manejar "subnetting" estático impediría utilizar "subnetting" de longitud variable en cualquier punto de la red. Afortunadamente no es este el caso. Siempre que los "routers" entre las subredes que tengan distintas máscaras usen "subnetting" de longitud variable, los protocolos de encaminamiento son capaces de ocultar la diferencia entre máscaras de subred a cada host de una subred. Los hosts pueden seguir usando encaminamiento IP básico y desentenderse de las complejidades del "subnetting", que quedan a cargo de "routers" dedicados a tal efecto.

6.5.6.4 ENCAMINAMIENTO IP CON SUBREDES

Para encaminar un datagrama IP en la red, el algoritmo general de encaminamiento IP tiene la forma siguiente:

Figura 214 Encaminamiento IP con subredes

Para ser capaz de distinguir entre subredes, el algoritmo de encaminamiento IP cambia y adopta la siguiente forma:

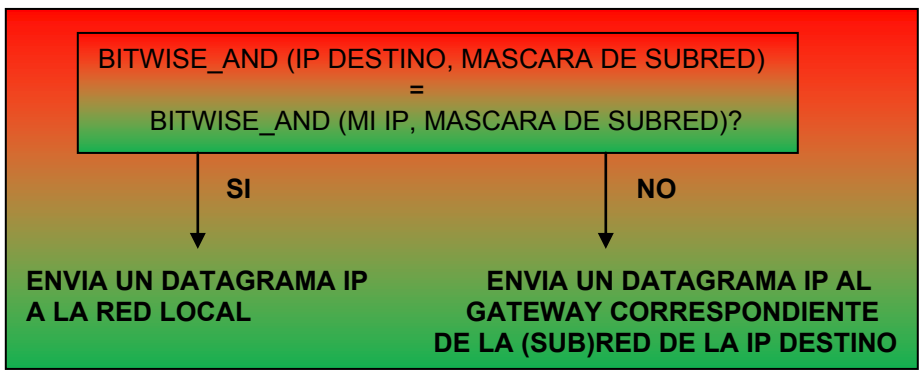


Figura 215 Encaminamiento IP con subredes

Algunas consecuencias de este algoritmo son:
Es un cambio a algoritmo general. Por tanto, para poder operar de este modo, el correspondiente gateway debe contener también el nuevo algoritmo. Algunas implementaciones pueden seguir usando el algoritmo general, y no funcionarán dentro de una red con subredes, aunque todavía podrán comunicarse con hosts en otras redes que no empleen "subnetting". Ya que el encaminamiento IP se usa en todos los hosts (aunque no en todos los "routers"), todos los hosts en la subred deben:

- Tener un algoritmo IP que soporte "subnetting".
- Tener la misma máscara de subred (a menos que existan subredes dentro de la subred).

Si la implementación de algún host no soporta "subnetting", dicho host sólo podrá comunicarse con hosts de la propia subred, pero no con máquinas que se hallen en otra subred dentro de su misma red. Esto se debe a que el host sólo ve la red IP y su encaminamiento no puede distinguir entre un datagrama IP dirigido a un host de su subred y que se debería enviar a través de un "router" a una subred diferente. En caso de que uno o más hosts no soporten "subnetting", una forma alternativa de lograr el mismo objetivo es hacer uso del **proxy-*ARP***, que no requiere cambios al algoritmo de encaminamiento IP para un host con una sola interfaz ("single-homed"), pero requiere cambios en los "routers" entre subredes.

6.5.6.5 OBTENIENDO UNA MÁSCARA DE SUBRED

La máscara de red no es más que una dirección IP donde se ha sustituido todos los bits de la parte de red de la dirección por unos y los bits correspondientes a la parte de host por ceros. Así, la máscara de red de una red de clase A será 255.0.0.0, la de una red de clase B será 255.255.0.0 y la de una clase C será 255.255.255.0. Habitualmente, los hosts almacenan su máscara de subred en un fichero de configuración. Sin embargo, a veces esto no se puede hacer, como es el caso de estaciones de trabajo sin disco. El protocolo ICMP incluye dos mensajes, solicitud de máscara de direcciones y respuesta de máscara de direcciones, que permitirá a los hosts obtener la máscara de subred correcta de un servidor.

6.5.6.6 DIRECCIONANDO ROUTERS Y HOTS MULTI-HOMED

Un host se denomina **multi-homed** cuando tiene conexión física con múltiples redes o subredes. Todos los "routers" han de ser multi-homed ya que su trabajo es unir redes o subredes distintas. Un host multi-homed tiene siempre una dirección IP diferente para cada adaptador de red, puesto que cada adaptador se halla en una red distinta. Hay una excepción aparente a esta regla: con algunos sistemas (por ejemplo VM y VMS) es posible especificar la misma dirección IP para múltiples enlaces punto a punto (como es el caso de los adaptadores de canal a canal) si el protocolo de encaminamiento se limita al algoritmo básico de encaminamiento IP.

6.5.6.7 DIRECIONES IP ESPECIALES

Como se ha señalado anteriormente, cualquier componente de una dirección IP con todos sus bits a 1 o a 0 tiene un significado especial

Todos los bits a 0.-Significa "este": "este" host (direcciones IP con <número de host=0) o "esta" red (direcciones IP con <número de red=0) y sólo se usa cuando el valor real no se conoce. Esta forma de expresar direcciones se utiliza con direcciones IP fuente, cuando el host trata de determinar sus direcciones IP por medio de un servidor remoto. El host puede incluir su número de host, si lo conoce, pero no su número de red o subred.
Todos los bits a 1.-Significa "todos": "todas" las redes o "todos" los hosts. Por ejemplo, 128.2.255.255 (una dirección de clase B con número de host 255.255) significa "todos los host de la red 128.2". Esta forma de expresar direcciones se emplea en mensajes de broadcast.
Hay otra dirección de especial importancia: el número de red de clase A con todos los bits a 1, 127, se reserva para la **dirección de loopback**. Todo lo que se envíe a una dirección con 127 como valor del byte de mayor orden, por ejemplo 127.0.0.1, no debe encaminarse a través de la red, sino directamente del controlador de salida al de entrada.

6.5.6.8 UNICASTING, BROADCASTING Y MULTICASTING

La mayoría de las direcciones IP se refieren a un sólo destinatario: se denomina direcciones de **unicast**. Sin embargo, como se ha señalado anteriormente, hay dos tipos especiales de direcciones IP que se utilizan para direccionar a múltiples destinatarios: las direcciones de broadcast y de multicast. Cualquier protocolo **no orientado a conexión** puede enviar mensajes de broadcast o de multicast, además de los unicast. Un protocolo **orientado a conexión** sólo puede usar direcciones de unicast porque la conexión existe entre un par específico de hosts.

6.5.6.8.1 BROADCASTING

Hay una serie de direcciones que usan para el broadcast en IP: todas manejan el convenio de que "todos los bits a 1" indica "todos". Las direcciones de broadcast nunca son válidas como direcciones fuente, sólo como direcciones de destino. Los diferentes tipos de broadcast se listan aquí:
Direcciones de broadcast limitado.-La dirección 255.255.255.255 (todos los bits a 1 en toda la dirección IP) se usa en redes que soportan broadcast, como por ejemplo redes en anillo, y se refiere a todos los host de la subred. No requiere que el host tenga conocimiento alguno de la configuración IP. Todos los host de la red local reconocerán la dirección, pero los "router" nunca enviarán el mensaje. Esta regla tiene una excepción, llamada **retransmisión BOOTP**. El protocolo BOOTP emplea el broadcast limitado para permitir a estaciones de trabajo sin disco contactar con un servidor BOOTP. La retransmisión BOOTP es una opción de configuración disponible en algunos "routers". Sin esta posibilidad, haría falta un servidor BOOTP en cada subred. Sin embargo, no se trata de una simple retransmisión, ya que el "router" también interviene en el desarrollo del protocolo BOOTP.
Direcciones de broadcast dirigidas a red.-Si el número de red es válido, la red no se subdivide en subredes y el número de host referencia todos los hosts de la red especificada, (por ejemplo, 128.2.255.255). Los "router" deberían enviar estos mensajes de broadcast a menos que están configurados para no hacerlo. Este tipo de broadcast se utiliza en solicitudes ARP (Address Resolution) en redes que contienen subredes.
Direcciones de broadcast dirigidas a subred.-Si el número de red y el de subred son válidos, y el de host tiene todos sus bits a 1, entonces la dirección referencia a todos los host de la subred especificada. Ya que la subred fuente y la de destino pueden tener distintas máscaras de subred, la fuente debe resolver de algún modo la máscara usada en la subred de destino. El broadcast lo efectúa realmente el "router" de subred que recibe el datagrama.
Direcciones de broadcast dirigidas a todas las subredes.-Si el número de red es válido, la red se subdivide en subredes y la parte local de la dirección tiene todos los bits a 1 (por ejemplo, 128.2.255.255), y la dirección se refiere a todos los hosts en todas las subredes de la red especificada. En principio, los "router" pueden propagar broadcasts por todas las subredes, aunque no están obligados a hacerlo. En la práctica, no lo hacen; hay pocas circunstancias en las que un broadcast sea deseable, y puede causar problemas, particularmente si un host se ha configurado incorrectamente sin su máscara de subred. Considerar el derroche de recursos que se produciría si el host 9.180.214.114 en la red local clase A con subredes no fuera consciente de la existencia de

esas subredes y usara 9.255.255.255 como dirección de broadcast "local" en vez de 9.180.214.255 y todos los "router" aceptaran la solicitud de enviar mensajes a todos los clientes.

Si los "router" respetan todos los mensajes de broadcast dirigidos a subredes, utilizan un algoritmo llamado **Retransmisión Inversa (Reverse Path Forwarding")** para evitar que los mensajes de broadcast se multipliquen descontroladamente.

6.5.6.8.2 MULTICASTING

El broadcast tiene una gran desventaja: su falta de selectividad. Si un datagrama IP se difunde por broadcast a una subred, cada host de la misma lo recibirá, y tendrá que procesarlo para determinar si el destinatario está activo. Si no lo está, el datagrama IP se elimina. El multicast elimina este overhead al usar grupos de direcciones IP. Cada grupo está representado por un número de 28 bits, incluido en una dirección de clase D. Recordar que una dirección de clase D tiene el formato:

Figura 216

De este modo, **las direcciones de grupos de multicast** 224.0.0.0 a 239.255.255.255. Para cada dirección multicast hay un conjunto de cero o más hosts a la escucha. Es lo que se denomina el grupo de hosts. Para que un host envíe un mensaje a ese grupo no se requiere que pertenezca a él. Hay dos clases de grupos de hosts:
Permanentes.-La dirección IP tiene una asignación permanente a través de IANA. La pertenencia a un grupo no es permanente: un host puede unirse a un grupo o dejarlo a voluntad. Los grupos asignados con carácter permanente se incluyen en STD 2 - Números asignados de Internet.
Algunos importantes son:
224.0.0.0
Dirección base reservada
224.0.0.1
Todos los sistemas en esta subred
224.0.0.2
Todos los "routers" en esta subred
Algunos otros ejemplos usados por el protocolo de encaminamiento OSPF son:
224.0.0.5
Todos los "router" OSPF
224.0.0.6
"Routers" OSPF designados
Una aplicación puede además determinar la dirección IP permanente de un grupo por medio del DNS (Domain Name System) usando el dominio mcast.net, o determinar el grupo permanente para una dirección a través de una consulta por punteros en el dominio 224.in-addr.arpa. Un grupo permanente existe aunque no tenga miembros.
Provisionales.-Cualquier grupo que no sea permanente es provisional y está disponible para ser asignado dinámicamente según las necesidades. Los grupos provisionales dejan de existir cuando el número de sus miembros se hace cero. El multicast en una sola red física que lo soporte simple. Para unirse a un grupo, un proceso activo en un host debe informar de algún modo a sus controladores de red que desea ser parte del grupo especificado. El propio software de los controladores debe mapear la dirección de multicast a una dirección física de multicast para permitir la recepción de paquetes en esa dirección. Además, tiene que asegurarse de que el proceso receptor no recibe datagramas espúreos, chequeando la dirección de destino de la cabecera IP antes de pasarlos a la capa IP.

Por ejemplo, Ethernet soporta multicast si el byte de orden superior de la dirección de 48 bytes es X'01' y además IANA posee un bloque de la dirección, consistente en las direcciones entre X'00005E000000' y X'00005EFFFFFF'. IANA ha asignado la mitad inferior de este rango para

direcciones de multicast, de modo que en una LAN Ethernet hay un rango de direcciones físicas entre X'01005E000000' y X'01005E7FFFFF' usado para el multicast IP. Este rango tiene 23 bits utilizables, por lo que las direcciones de multicast de 28 bits se mapean a Ethernet tomando los 23 bits inferiores, es decir, hay 32 direcciones de multicast mapeadas sobre cada dirección Ethernet. Debido a este mapeo no unívoco, hace falta efectuar un filtrado en el controlador. Hay otras dos razones por la que se podría seguir necesitando el filtrado:

- Algunos adaptadores LAN están limitados a un número finito de direcciones multicast concurrentes y si este es excedido tendrán que recibir todos los multicast.
- Otros adaptadores LAN tienden a filtrar de acuerdo con un valor de una tabla de hash, lo que significa que hay una posibilidad de que el filtro tenga fugas, si dos direcciones multicast con el mismo valor de hash se usan al mismo tiempo.

A pesar de la necesidad de filtrar por software de paquetes multicast, el multicast aún causa mucho menos overhead en los hosts no interesados. En particular, aquellos hosts que no estén en ningún grupo no escuchan a los mensajes con direcciones multicast y por tanto todos los mensajes multicast son filtrados por el hardware de la interfaz de red. El multicast no se limita a una sola red física. Hay dos aspectos del multicast en redes físicas a considerar:

- Un mecanismo para decidir la amplitud del multicast (recordar que a diferencia del unicast y el broadcast, las direcciones de multicast cubren toda Internet).
- Un mecanismo para decidir si un datagrama multicast necesita ser enviado a una red concreta.

El primer problema tiene fácil solución: el datagrama multicast tiene un **TTL (tiempo de vida o Time To Live)** como cualquier otro datagrama, que se decrementa con cada salto a una nueva red Cuando el TTL se decrementa a cero, el datagrama no puede ir más lejos. El mecanismo para decidir si un router debe enviar un datagrama multicast se denomina **IGMP (Internet Group Management Protocol** o **Internet Group Multicast Protocol)**. IGMP y el multicast se definen en el RFC 1112 - Extensiones de host para el multicast IP.

6.5.7 PROTOCOL INTERNET (IP)

El protocolo IP es el elemento que permite integrar distintas redes entre si. El protocolo IP enlaza las diferentes redes (FDDI, ISDN, X.25, líneas dedicadas, Token Ring, Ethernet, líneas telefónicas) de Internet. Cada máquina de la red Internet tiene una dirección IP única. Una dirección IP es un número de 32 bits que normalmente se escribe como cuatro enteros entre 0 y 255 separados por puntos (192.112.36.5), la dirección IP permite el encaminamiento de la información a través de Internet. En la terminología de comunicaciones el protocolo IP define una red de conmutación de paquetes. La información se fragmenta en pequeños trozos o paquetes (alrededor de 1,500 caracteres) que se envían independientemente por la red. Cada paquete es enviado con la dirección de la estación donde ha de ser entregado y, de forma similar a como funciona un sistema postal, cada paquete viaja independientemente de los demás por la red hasta alcanzar su destino. Dentro de una red local, el encaminamiento de la información es simple. En Ethernet por ejemplo todas las estaciones **escuchan** la red para detectar los paquetes que se dirigen a ellos. En Internet este procedimiento es inviable. Los routers son los elementos encargados del encaminamiento de los mensajes IP. Los routers conocen las máquinas conectadas a la red y toman la decisión de como encaminar los paquetes de datos a través de unos enlaces u otros. Cada router sólo necesita saber que conexiones están disponibles y cual es el mejor **próximo salto** para conseguir que un paquete este más cerca de su destino (el paquete va **saltando** de router a router hasta llegar a su destino). Las máquinas de Internet, fuera del entorno de la red local, utilizan un router para encaminar los paquetes. La dirección IP de esta máquina es la única información que deben conocer, del resto se encargan los routers.

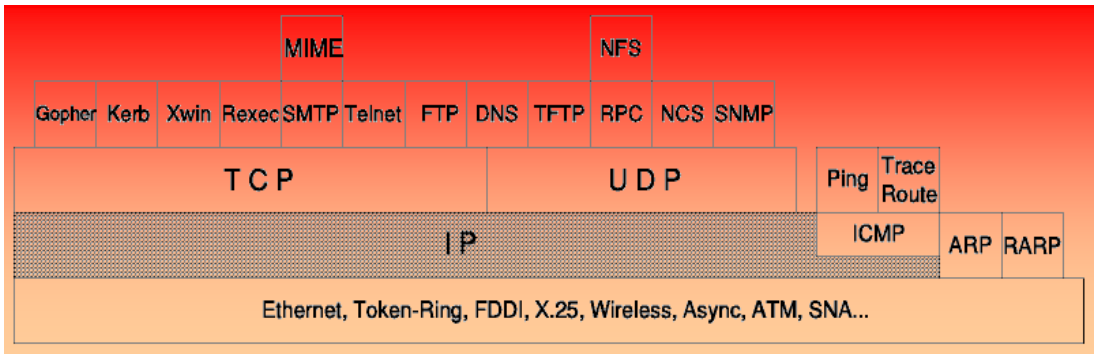


Figura 217 IP (Internet Protocol)

IP es un protocolo estándar con STD 5 que además incluye **ICMP (Internet Control Message Protocol**) e **IGMP (Internet Group Management Protocol**). IP es el protocolo que oculta la red física subyacente creando una vista de **red virtual**. Es un protocolo de entrega de paquetes no fiable y no orientado a conexión, y se puede decir que aplica la ley del mínimo esfuerzo.
No aporta fiabilidad, control de flujo o recuperación de errores a los prots de red inferiores. Los paquetes (datagramas) que envía IP se pueden perder, desordenarse, o incluso duplicarse, e IP no manejará estas situaciones. El proporcionar estos servicios depende de prots superiores. IP asume pocas cosas de las capas inferiores, sólo que los datagramas **probablemente** serán transportados al host de destino.

6.5.7.1 EL DATAGRAMA IP

El datagrama IP es la unidad de transferencia en la pila IP. Tiene una cabecera con información para IP, y los datos relevantes para los prots superiores.

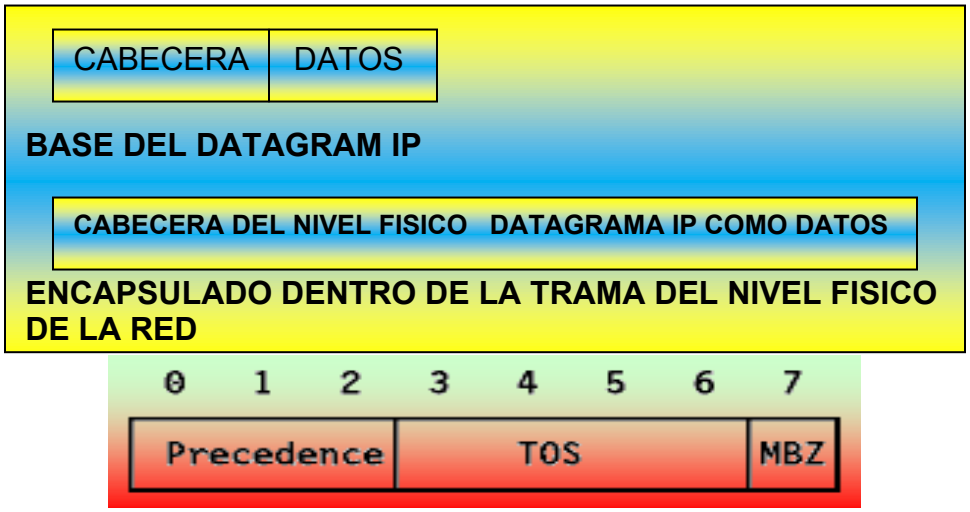


Figura 218 El datagrama IP

El datagrama IP está encapsulado en la trama de red subyacente, que suele tener una longitud máxima, dependiendo del hardware usado. En vez de limitar el datagrama a un tamaño máximo, IP puede tratar la **fragmentación** y el **re-ensamblado** de sus datagramas. En particular, el IP no impone un tamaño máximo, pero establece que todas las redes deberían ser capaces de manejar al menos 576 bytes. Los fragmentos de datagramas tienen todos una cabecera, copiada básicamente del datagrama original, y de los datos que la siguen. Se tratan como datagramas normales mientras son transportados a su destino. Nótese, sin embargo, que si uno de los

fragmentos se pierde, todo el datagrama se considerará perdido, y los restantes fragmentos se considerarán perdidos.

6.5.7.1.1 FORMATO DEL DATAGRAMA IP

La cabecera del datagrama IP es de un mínimo de 20 bytes de longitud:

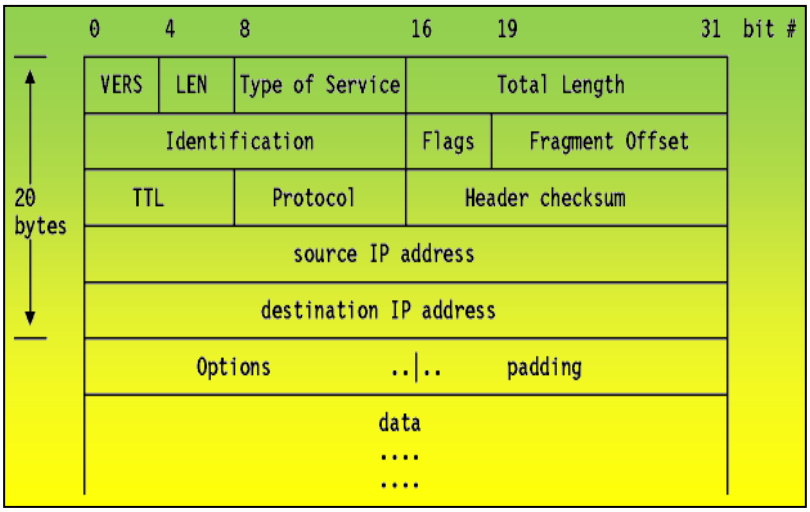


Figura 219 Formato del datagrama IP

- **VERS**.-La versión del protocolo IP. La versión actual es la 4. La 5 es experimental y la 6 es Ipng.
- **LEN**.-La longitud de la cabecera IP contada en cantidades de 32 bits. Esto no incluye el campo de datos.
- **Type of Service**.-El tipo de servicio es una indicación de la calidad del servicio solicitado para este datagrama IP.
    - **Precedencia**.-Es una medida de la naturaleza y prioridad de este datagrama:
      000 Rutina
      001 Prioridad
      010 Inmediato
      011 Flash
      100 Flash override
      101 Crítico
      110 Control de red (Internet work control)
      111 Control de red (Network control)
    - **TOS (type of service):**
      1000 Minimizar retardo
      0100 Maximizar la densidad de flujo
      0010 Maximizar la fiabilidad
      0001 Minimizar el costo monetario
      0000 Servicio normal
    - **MBZ**.-Reservado para uso futuro (debe ser cero, a menos que participe en un experimento con IP que haga uso de este bit)
- **Total Length**.-La longitud total del datagrama, cabecera y datos, especificada en bytes.
- **Identification**.-Un número único que asigna el emisor para ayudar a reensamblar un datagrama fragmentado. Los fragmentos de un datagrama tendrán el mismo número de identificación.

- **Flags**.-Varios flags de control figura 220:

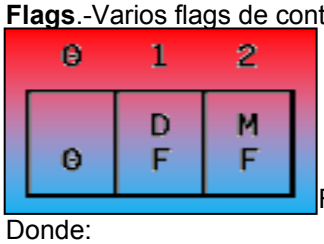


Figura 220

  Donde:
  0 Reservado, debe ser cero
  DF (No fragmentar, Don't Fragment): con 0 se permite la fragmentación, con 1 no.
  MF (Más fragmentos, More Fragments): 0 significa que se trata del último fragmento del datagrama, 1 que no es el último.
- **Fragment OFFSET**.-Usado con datagramas fragmentados, para ayudar al reensamblado de todo el datagrama. El valor es el número de partes de 64 bits (no se cuentan los bytes de la cabecera) contenidas en fragmentos anteriores. En el primer (o único) fragmento el valor es siempre cero.
- **TTL (Time to Live)**.-Especifica el tiempo (en segundos) que se le permite viajar a este datagrama. Cada router por el que pase este datagrama ha de sustraer de este campo el tiempo tardado en procesarlo. En la realidad un router es capaz de procesar un datagrama en menos de 1 segundo; por ello restará uno de este campo y el TTL se convierte más en una cuenta de saltos que en una métrica del tiempo. Cuando el valor alcanza cero, se asume que este datagrama ha estado viajando en un bucle y se desecha. El valor inicial lo debería fijar el protocolo de alto nivel que crea el datagrama.
- **Protocol Number spotipprotn**.-Indica el protocolo de alto nivel al que IP debería entregar los datos del datagrama. Algunos valores importantes son:
  0 Reservado
  1 ICMP (Internet Control Message Protocol)
  2 IGMP (Internet Group Management Protocol)
  3 GGP (Gateway-to-Gateway Protocol)
  4 IP (IP encapsulation)
  5 Flujo (Stream)
  6 TCP (Transmission Control)
  8 EGP (Exterior Gateway Protocol)
  9 PIRP (Private Interior Routing Protocol)
  17 UDP (User Datagram Protocol)
  89 OSPF (Open Shortest Path First)
- **Header Checksum**.-.Es el checksum de la cabecera. Se calcula como el complemento a uno de la suma de los complementos a uno de todas las palabras de 16 bits de la cabecera. Con el fin de este cálculo, el campo checksum se supone cero. Si el checksum de la cabecera no se corresponde con los contenidos, el datagrama se desecha, ya que al menos un bit de la cabecera está corrupto, y el datagrama podría haber llegado al destino equivocado.
- **Source IP Address**.-La dirección IP de 32 bits del host emisor.
- **Destination IP Address**.-La dirección IP de 32 bits del host receptor.
- **Options: Longitud variable**.-No requiere que toda implementación de IP sea capaz de generar opciones en los datagramas que crea, pero sí que sea capaz de procesar datagramas que contengan opciones. El campo Options (opciones) tiene longitud variable. Puede haber cero o más opciones. Hay dos formatos para estas. El formato usado depende del valor del número de opción hallado en el primer byte.
  Un byte de tipo (type byte) sólo, figura 221.

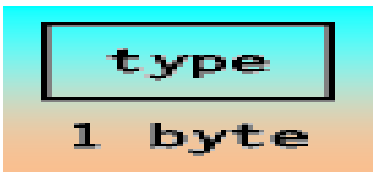


Figura 221

Un byte de tipo, un byte de longitud y uno o más bytes de opciones, figura 222.

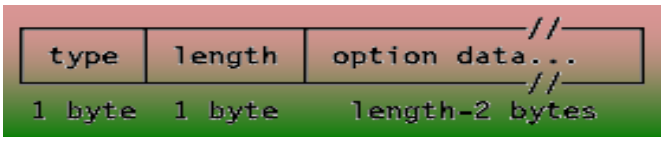


Figura 222

El byte de tipo tiene la misma estructura en ambos casos, figura 223:

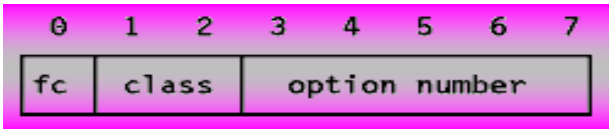


Figura 223

Donde:

- **FC (Flag copy)**.-Que indica si el campo de options se ha de copiar (1) o no (0) cuando el datagrama está fragmentado.
- **Class**.-Un entero sin signo de 2 bits:
  0 control
  1 reservado
  2 depurado y mediciones
  3 reservado
- **Option Number**.-Entero sin signo de 5 bits.
  0 Fin de la Lista de Opciones.-Con class a cero, fc a cero, y sin byte de longitud o de datos. Es decir, la lista termina con el byte X'00'. Sólo se requiere si la longitud de la cabecera IP (que es un múltiplo de 4 bytes) no se corresponde con la longitud real de las opciones.
  1 No Operación.-Tiene class a cero, fc a cero y no hay byte de longitud ni de datagramas. Es decir, un byte X'01' es NOP (no operation). Se puede usar para alinear campos en el datagrama.
  2 Security.-Tiene class a cero, fc a uno y el byte de longitud a 11 y el de datos a 8. Se usa para la información de seguridad que necesitan las especificaciones del departamento de defensa de los Estados Unidos.
  3 LSR (Loose Source Routing).-Tiene class a cero, fc a uno y hay un campo de datos de longitud variable.
  4 IT (Internet Time stamp).-Tiene class a 2, fc a cero y hay un campo de datos de longitud variable.
  7 RR (Record Route).-Tiene class a 0, fc a cero y hay un campo de datos de longitud variable.
  8 SID (Stream ID, o identificador de flujo).-Tiene class a 0, fc a uno y hay un byte de longitud a 4 y un byte de datos. Se usa con el sistema SATNET.
  9 SSS (Strict Source Routing).-Tiene class a 0, fc a uno y hay un campo de datos de longitud variable.
  Length.-Cuenta la longitud (en bytes) de la opción, incluyendo los campos de tipo y longitud.
  Option Data.-No contiene datos relevantes para la opción.

- **Padding**.-Si se usa una opción, el datagrama se rellena con bytes a cero hasta la siguiente palabra de 32 bits.
- **Data**.-Los datos contenidos en el datagrama se pasan a un protocolo de nivel superior, como se especifica en el campo **protocol**.

6.5.7.1.2 FRAGMENTACION

Cuando un datagrama IP viaja de un host a otro puede cruzar distintas redes físicas. Las redes físicas imponen un tamaño máximo de trama, llamado **MTU (Maximum Transmission Unit)**, que limita la longitud de un datagrama. Por ello, existe un mecanismo para fragmentar los datagramas IP grandes en otros más pequeños, y luego reensamblarlos en el host de destino. IP requiere que

cada enlace tenga un MTU de al menos 68 bytes, de forma que si cualquier red proporciona un valor inferior, la fragmentación y el reensamblado tendrán que implementarse en la capa de la interfaz de red de forma transparente a IP. 68 es la suma de la mayor cabecera IP, de 60 bytes, y del tamaño mínimo posible de los datos en un fragmento (8 bytes). Las implementaciones de IP no están obligadas a manejar datagrama sin fragmentar mayores de 576 bytes, pero la mayoría podrá manipular valores más grandes, típicamente ligeramente más de 8,192 bytes, o incluso mayores, y raramente menos de 1,500. Un datagrama sin fragmentar tiene a cero toda la información de fragmentación. Es decir, el flag fc y el fo (fragment offset) están a cero. Cuando se ha de realizar la fragmentación, se ejecutan los siguientes pasos:

- Se chequea el bit de flag DF para ver si se permite fragmentación. Si está a uno, el datagrama se desecha y se devuelve un error al emisor usando ICMP.
- Basándose en el valor MTU, el campo de datos se divide en dos o más partes. Todas las nuevas porciones de datos, excepto la última, se alinean a 8 bytes.
- Todas las porciones de datos se colocan en datagramas IP. Las cabeceras se copian de la cabecera original, con algunas modificaciones:
    - El bit de flag mf (more fragments) se pone a uno en todos los fragmentos, excepto en el último.
    - El campo fo se pone al valor de la localización de la porción de datos correspondiente en el at original, con respecto al comienzo del mismo. Su valor se mide en unidades de 8 bytes.
    - Si se incluyeron opciones en el datagrama original, el bit de orden superior del byte type option determina si se copiaran o no en todos los fragmentos o sólo en el primero. Por ejemplo, las opciones de encaminamiento de la fuente se tendrán que copiar en todos los fragmentos y por tanto tendrán a uno este bit.
- Se inicializa el campo de longitud (length) del nuevo datagrama.
- Se inicializa el campo de longitud (length) total del nuevo datagrama.
- Se recalcula el checksum de la cabecera.1

Cada uno de estos datagramas se envía como un datagrama IP normal. IP maneja cada fragmento de forma independiente, es decir, los fragmento pueden atravesar diversas rutas hacia su destino, y pueden estar sujetos a nuevas fragmentaciones si pasan por redes con MTU's inferiores. En el host de destino, los datos se tienen que reensamblar. El host emisor inicializó el campo ID a un número único (dentro de los límites impuestos por el uso de un número de 16 bits). Como la fragmentación no altera este campo, los fragmentos que le van llegando al destino se pueden identificar, si este ID se usa junto con las direcciones IP fuente y destino (source, destination) del datagrama. También se chequea el campo de protocolo Con el fin de reensamblar los fragmentos, el receptor destina un buffer de almacenamiento en cuanto llega el primer fragmento. Se inicia una rutina para un contador. Cuando el contador a un timeout y no se han recibido todos los datagramas, se desecha el datagrama. El valor inicial el contador es el TTL (time-to-live). Depende de la implementación, y algunas permiten configurarlo. Cuando llegan los fragmentos siguientes, antes de que expire el tiempo, los datagramas se copian al buffer en la localización indicada por el fo (fragment offset). Cuando han llegado todos los datagramas, se restaura el datagrama original y continúa su procesamiento.
Nota: IP no proporciona el contador de reensamblado. Tratará cada datagrama, fragmentado o no, de la misma forma. Depende de una capa superior el implementar un timeout y reconocer la pérdida de fragmentos. Esta capa podría ser TCP para el transporte en una red orientada a conexión o UDP, para el caso contrario.

6.5.7.1.3 OPCIONES DE ENCAMINAMIENTO DEL DATAGRAMA IP

El campo options del datagrama IP admite dos métodos para que el generador del datagrama de explícitamente información de encaminamiento y uno para que el datagrama determine a ruta que va a emplear.

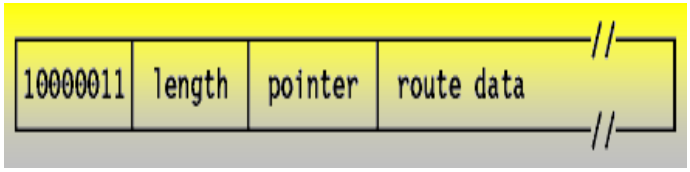
LSR (Loose Source Routing).-Esta opción, conocida también como **LSRR (Loose Source and Record Route)**, proporciona un medio para que la fuente del dar suministre información de encaminamiento explícita que usarán los routers que retransmitan el datagrama, y para grabar la ruta seguida, figura 224.

Figura 224 Opción LSR

- **1000011 (131 decimal)**.-Es el valor del byte option para LSR.
- **Length**.-Contiene la longitud de este campo, incluyendo los campos type y length.
- **Pointer**.-Apunta a los datagramas de la opción en la siguiente dirección IP a procesar. Es relativo al comienzo de la opción, por lo que su valor mínimo es de cuatro. Si su valor supera la longitud de la opción, se alcanza el final de la ruta de la fuente y el resto del encaminamiento se ha de basar en la dirección IP de destino (como en los datagramas que no tienen esta opción).
- **Route Data**.-Es una serie de direcciones IP de 32 bits.

Siempre que un datagrama llega a su destino y la ruta de la fuente no está vacía (pointer < length) el receptor: Tomará la siguiente dirección IP de este campo (el indicado por pointer y lo pondrá en el campo de la dirección IP de destino el datagrama). Pondrá la dirección IP local en la **SL (source list)** en la localización a la que apunte pointer. La dirección IP local es la correspondiente a la red por la que se enviará el datagrama.
Incrementará pointer en 4.
Transmitirá el datagrama a la nueva dirección IP de destino.

Este procedimiento asegura que la ruta de retorno se graba en **route datagram (en orden inverso)** de modo que el receptor use estos datagramas para construir un LSR en el sentido inverso. Se denomina LSR (loose source route) porque al router retransmisor se le permite usar cualquier ruta y cualquier número de host intermedios para alcanzar la siguiente dirección de la ruta.
Nota: El host emisor pone la dirección IP del primer router intermedio en el campo dirección IP de destino y las direcciones de los demás routers de la ruta, incluyendo el destino, en la opción source route. La ruta que hay grabada en el datagrama cuando este llega al objetivo contiene las direcciones IP de cada uno de los routers que retransmitió el datagrama.



SSR (Strict Source Routing).-Esta opción, llamada también **SSRR (Strict Source and Record Route)**, emplea el mismo principio que LSR exceptuando que el router intermedio **debe** enviar el datagrama a la siguiente dirección IP en la ruta especificada por la fuente a través de una red conectada directamente y no por medio de un router intermedio. Si no puede hacerlo, envía un mensaje **ICMP Destination Unreachable**.

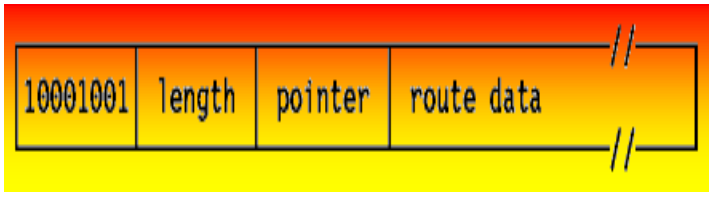
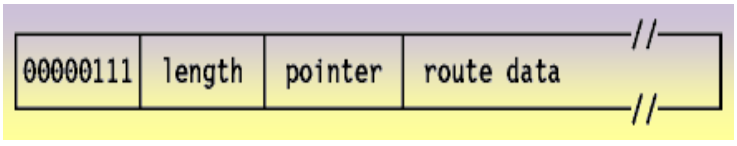


Figura225 Opción SSR

- **1001001 (137 decimal)**.-Es el valor del byte option para el método SSR.
- **Length**.-Tiene el mismo significado que para LSR.
- **Pointer**.-Tiene el mismo significado que para LSR.
- **Route Data**.-Es una serie de direcciones IP.

RR (Record Route).-Esta opción proporciona un medio para grabar la ruta de un datagrama IP. Funciona de modo similar al SSR anterior, pero en este caso el host fuente deja el campo de datos de encaminamiento vacío, que se irá llenando a medida que el datagrama viaja. Nótese que el host fuente debe dejar suficiente espacio para esta información: si el campo se llena antes de que el



datagrama llegue a su destino, el datagrama se retransmitirá, pero se dejará de grabar la ruta, figura 226.

Figura 226 Opción RR

- **0000111 (7 decimal)**.-Es el valor del byte option para el método RR.
- **Length**.-Tiene el mismo significado que para LSR.
- **Pointer**.-Tiene el mismo significado que para LSR.
- **Route Data**.-Su longitud es un múltiplo de cuatro bytes, y lo elige el generador del datagrama.

6.5.7.1.4 IT (INTERNET TIMESTAMP)

El **timestamp o sello de tiempo** es una opción para forzar algunos (o a todos) de los routers de la ruta hacia el destino a poner un timestamp en los datos de la opción. Los timestamps se miden en segundos y se pueden usar para la depuración. No se pueden emplear para medir el rendimiento por dos razones: No son lo bastante preciso porque la mayoría de los datagramas se envían en menos de un segundo. No son lo bastante precisos porque los routers no han de tener relojes sincronizados, figura 227.

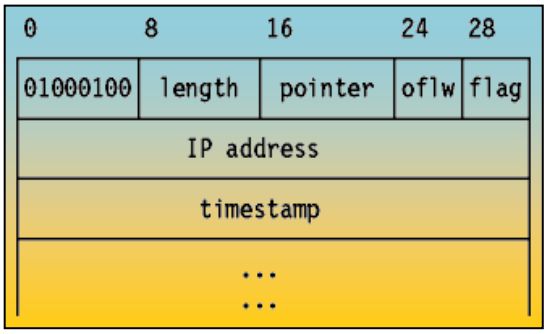


Figura 227 Opción IT

- **1000100 (68 decimal)**.-Es el valor del byte option para IT.
- **Length**.-Contiene la longitud total de esta opción, incluyendo los campos type y length.
- **Pointer**.-Apunta al siguiente timestamp a procesar (el primero que esté disponible).
- **oflw (overflow)**.-Es un entero sin signo de 4 bits que indica el número de módulos IP que no pueden registrar timestamps por falta de espacio en el campo de datos.
- **Flag**.-Es una valor de 4 bits que indica como se han de registrar los timestamps. Los valores posibles son:
  - 0 Sólo timestamps, almacenados en palabras consecutivas de 32 bits.
  - 1 Cada timestamp se precede con la dirección IP del módulo que efectúa el registro.
  - 2 La dirección IP se pre-especifica, y un módulo IP sólo realiza el registro cuando encuentra su propia dirección en la lista.
  - Timestamp.-Un timestamp de 32 bits medido en milisegundos desde la medianoche según UT (GMT). El host emisor debe componer esta opción con un área de datos lo bastante grande para almacenar todos los timestamps. Si el área de los timestamps se llena, no se añaden más.

6.5.7.2 ENCAMINAMIENTO IP

Una función importante de la capa IP es el **encaminamiento**. Proporciona los mecanismos básicos para interconectar distintas redes físicas. Esto significa que un host puede actuar simultáneamente como host normal y como router. Un router básico de este tipo se conoce como **router con información parcial de encaminamiento**, ya que sólo contiene información acerca de cuatro tipos de destino:

- Los hosts conectados directamente a una de las redes físicas a las que está conectado el router.
- Los host o redes para las que se le han dado al router definiciones específicas.
- Los hosts o redes para las que el host ha recibido un mensaje **ICMP redirect**.
- Un destino por defecto para todo lo demás.

Los dos últimos casos permiten a un router básico comenzar con una cantidad muy limitada de información para irla aumentando debido a que un router más avanzado lance un mensaje **ICMP**

redirect cuando reciba un datagrama y conozca un router mejor en la misma red al que dirigir el datagrama. Este proceso se repite cada vez que un router básico se reinicia. Se necesitan protocolos adicionales para implementar un router completamente funcional que pueda intercambiar información con otros routers en redes remotas. Tales routers son esenciales, excepto en redes pequeñas.

6.5.7.3 DESTINOS DIRECTOS E INDIRECTOS

Si el host de destino está conectado a una red a la que también está conectado el host fuente, un datagrama IP puede ser enviado directamente, simplemente encapsulando el datagrama IP en una trama. Es lo que se llama **encaminamiento directo**. El **encaminamiento indirecto** ocurre cuando el host de destino no está en una red conectada directamente al host fuente. La única forma de alcanzar el destino es a través de uno o más routers, figura 228.

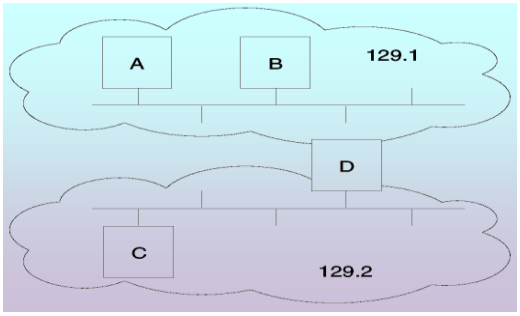


Figura 228 Rutas IP directas e indirectas

La dirección del primero de ellos (el **primer salto**) se llama **ruta indirecta**. La dirección del primer salto es la única información que necesita el host fuente: el router que reciba el datagrama se responsabiliza del segundo salto, y así sucesivamente. El host A tiene una ruta directa con B y D, y una indirecta con C. El host D es un router entre las redes 129.1 y 129.2. Un host puede distinguir si una ruta es directa o indirecta examinando el número de red y de subred de la dirección IP. Si coinciden con una de las direcciones IP del host fuente, la ruta es directa. El host necesita ser capaz de direccionar correctamente el objetivo usando un protocolo inferior a IP. Esto se puede hacer automáticamente, usando un protocolo como **ARP (Address Resolution Protocol)**, que se usan en LAN's con broadcast, o estáticamente y configurando el host, por ejemplo cuando un host MVS tiene una conexión TCP/IP sobre un enlace SNA. Para rutas indirectas, el único conocimiento requerido es la dirección IP de un router que conduzca a la red de destino. Las implementaciones de IP pueden soportar también rutas explícitas, es decir, una ruta a una dirección IP concreta. Esto es habitual en las conexiones que usan **SLIP (Serial Line Internet Protocol)** que no proporciona un mecanismo para que dos hosts se informen mutuamente de sus direcciones IP. Tales rutas pueden tener incluso el mismo número de red que el host, por ejemplo en subredes compuestas de enlaces punto a punto. Sin embargo, la información de encaminamiento se genera sólo mediante los números de red y de subred.

6.5.7.4 TABLA DE ENCAMINAMIENTO IP

Cada host guarda el conjunto de mapeados entre las direcciones IP de destino y las direcciones IP del siguiente salto para ese destino en una tabla llamada **tabla de encaminamiento IP**. En esta tabla se pueden encontrar tres tipos de mapeado:

- **Rutas Directas**.-Para redes conectadas localmente.
- **Rutas Indirectas**.-Para redes accesibles a través de uno o más rotures.
- **Una Ruta por Defecto**.-Que contiene la dirección IP de un router que todas las direcciones IP no contempladas en las rutas directas e indirectas han de usar, figura229. Ejemplo de tabla de encaminamiento IP para un ejemplo.

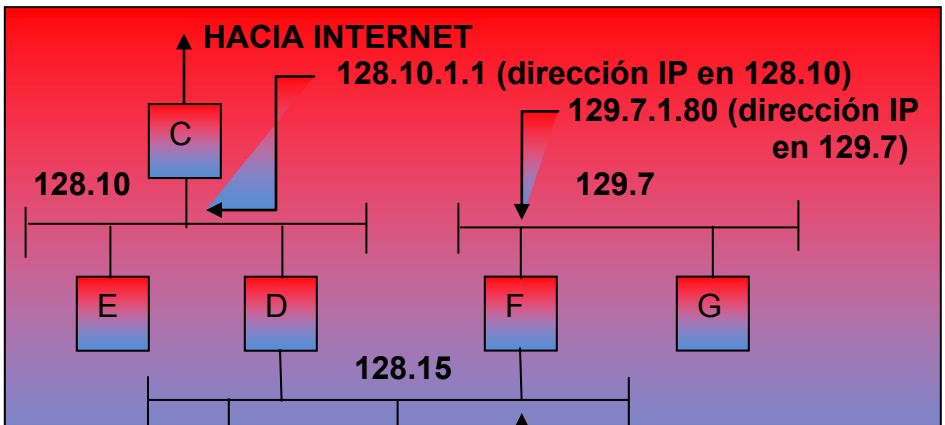


Figura 229 Ejemplo de tabla de encaminamiento IP

La tabla de encaminamiento contiene las siguientes entradas
Destination
route via
128.10
direct attachement
128.15
direct attachement
129.7
128.15.1.2
default
128.10.1.1

6.5.7.5 ALGORITMO DE ENCAMINAMIENTO IP

De los principios ya comentados de IP, es fácil deducir los pasos que IP debe tomar con el fin de determinar la ruta para un datagrama de salida. Es lo que se denomina **algoritmo de encaminamiento IP**, y se muestra esquemáticamente en la figura 230 Algoritmo de encaminamiento IP. Nótese que se trata de un proceso iterativo. Se aplica a todo host que maneje un datagrama, exceptuando al host al que se entrega finalmente el datagrama.

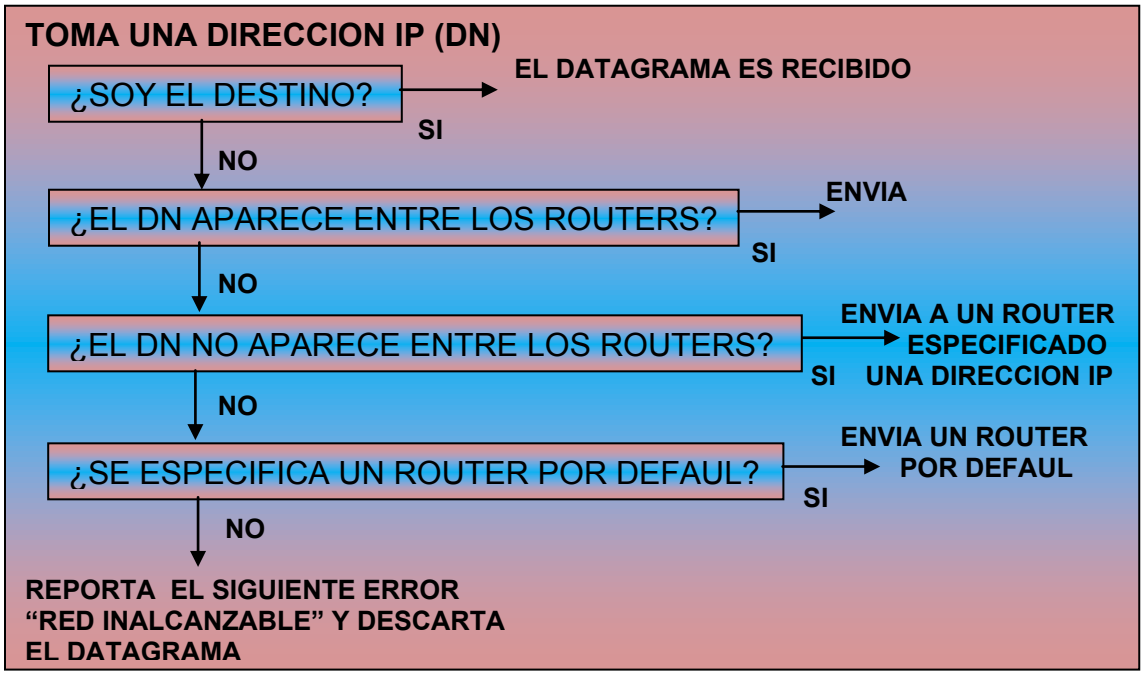


Figura 230 Algoritmo de encaminamiento IP

6.5.8 DNS (DOMAIN NAME SYSTEM)

Las configuraciones iniciales de Internet requerían que los usuarios emplearan sólo direcciones IP numéricas. Esto evolucionó hacia el uso de nombres de host simbólicos muy rápidamente. Por ejemplo, en vez de escribir TELNET 128.12.7.14, se podría escribir TELNET eduvm9, y eduvm9 se traduciría de alguna forma a la dirección IP 128.12.7.14. Esto introduce el problema de mantener la correspondencia entre direcciones IP y nombres de máquina de alto nivel de forma coordinada y centralizada. Inicialmente, el **NIC (Network Information Center)** mantenía el mapeado de nombres a direcciones en un sólo fichero (HOSTS.TXT) que todos los hosts obtenían vía FTP. Se denominó **espacio de nombres plano**. Debido al crecimiento explosivo del número de hosts, este mecanismo se volvió demasiado tosco (considerar el trabajo necesario sólo para añadir un host a Internet) y fue sustituido por un nuevo concepto: **DNS (Domain Name System)**. Los hosts pueden seguir usando un espacio de nombres local plano (el fichero HOSTS.LOCAL) en vez o además del DNS, pero fuera de redes pequeñas, el DNS es prácticamente esencial. El DNS permite que un programa ejecutándose en un host le haga a otro host el mapeo de un nombre simbólico de nivel superior a una dirección IP, sin que sea necesario que cada host tenga una base de datos completa de los nombres simbólicos y las direcciones IP.

6.5.8.1 EL ESPACIO DE NOMBRES JERÁRQUICO

Consideremos la estructura interna de una gran organización. Como el jefe no lo puede hacer todo, la organización tendrá que partirse seguramente en divisiones, cada una de ellas autónoma dentro de ciertos límites. Específicamente, el ejecutivo a cargo de una división tiene autoridad para tomar decisiones sin requerir el permiso de su jefe. Los nombres de dominio se forman de modo similar, y con frecuencia reflejarán la delegación jerárquica de autoridades usada para asignarlos. Por ejemplo, considerar el nombre lcs.mit.edu. Aquí, lcs.mit.edu es el nombre de dominio de nivel inferior, un subdominio de mit.edu, que a su vez es un subdominio de edu (education), conocido como **dominio raíz**. También podemos representar este forma de asignar nombres con un árbol jerárquico, figura 231 Espacio de nombres jerárquico. Esta figura muestra la cadena de autoridades en la asignación de nombres de dominio. Este árbol es sólo una fracción mínima del espacio de nombres real.

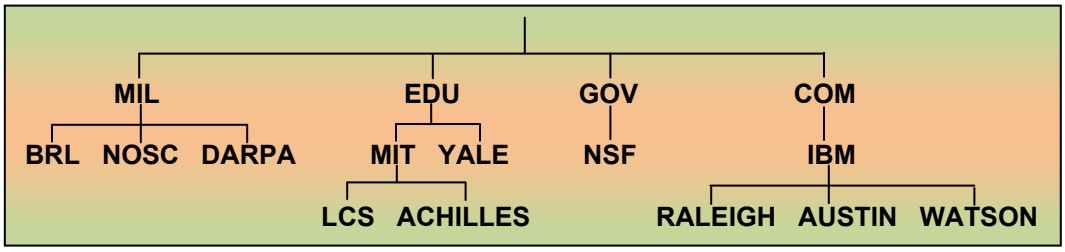


Figura 231 Espacio de nombres jerárquico

6.5.8.2 FQDN ("FULLY QUALIFIED DOMAIN NAMES)

Cuando se usa el DNS, es común trabajar con sólo una parte de la jerarquía de dominios, por ejemplo el dominio ral.ibm.com. El DNS proporciona un método sencillo para minimizar la cantidad de caracteres a escribir en estos casos. Si el nombre de dominio termina en un punto (por ejemplo wtscpok.itsc.pok.ibm.com.) se asume que está completo. Es lo que se llama un **FQDN (Fully Qualified Domain Name o Nombre Absoluto de Dominio)**. Si, sin embargo, no termina en punto, (por ejemplo wtscpok.itsc) estará incompleto y procesador de nombres del DNS, podrá completarlo,

por ejemplo, añadiendo un sufijo como .pok.ibm.com al nombre de dominio. Las reglas para hacer esto dependen de la implementación y son configurables localmente.

6.5.8.3 DOMINIOS GENERICOS

A los tres dominios de la cima se les llama dominios **genéricos u organizacionales**.

Nombre de dominio	Significado
edu	Instituciones educativas
gov	Instituciones gubernamentales
com	Organizaciones comerciales
mil	Grupos militares
net	Redes
int	Organizaciones internacionales
org	Otras organizaciones

Puesto que Internet comenzó en los Estados Unidos, la estructura del espacio de nombres jerárquico tenía inicialmente sólo organizaciones estadounidenses en la cima de la jerarquía, y sigue siendo cierto que gran parte de las organizaciones de la cima de la jerarquía son estadounidenses. Sin embargo, sólo los dominios .gov y .mil están restringidos a los US.

6.5.8.4 DOMINIOS DE PAISES

Además hay dominios de nivel de cima para cada uno de los códigos internacionales de dos caracteres ISO 3166 para países (de *ae* para los Emiratos Árabes Unidos a *zw* para Zimbabwe). Se les conoce como dominios de **países** o dominios **geográficos**. Muchos países tienen sus propios dominios de segundo nivel por debajo, paralelamente a los dominios genéricos. Por ejemplo, en el Reino Unido, los dominios equivalentes a .com y .edu son .co.uk y .ac.uk (ac es la abreviatura de academic). Está también el dominio .us, organizado geográficamente por estados (por ejemplo, .ny.us se refiere al estado de New York).

6.5.8.5 MAPEANDO NOMBRES DE DOMINIO A DIRECCIOPNES IP

El mapeado de nombres a direcciones, proceso denominado **resolución de nombres de dominio**, lo proporcionan sistemas independientes cooperativos, llamados **servidores de nombres**. Un servidor de nombres es un programa servidor que responde a peticiones de un cliente llamado **procesador de nombres**. Cada procesador de nombres está configurado con el nombre del servidor que va a usar (y posiblemente una lista de servidores alternativos con los que contactar si el servidor primario no está disponible), figura 232 - Resolución de nombres de dominio muestra esquemáticamente como un programa utiliza un procesador de nombres para convertir el nombre de un host en una dirección IP. El usuario proporciona el nombre de un host, y al programa de usuario emplea una rutina de librería, llamada **stub**, para comunicarse con un servidor de nombres que resuelve el nombre del host en una dirección IP y se la devuelve al stub, que a su vez lo devuelve al programa principal. El servidor de nombres puede obtener la respuesta de su caché de nombres, su propia base de datos o cualquier otro servidor de nombres.

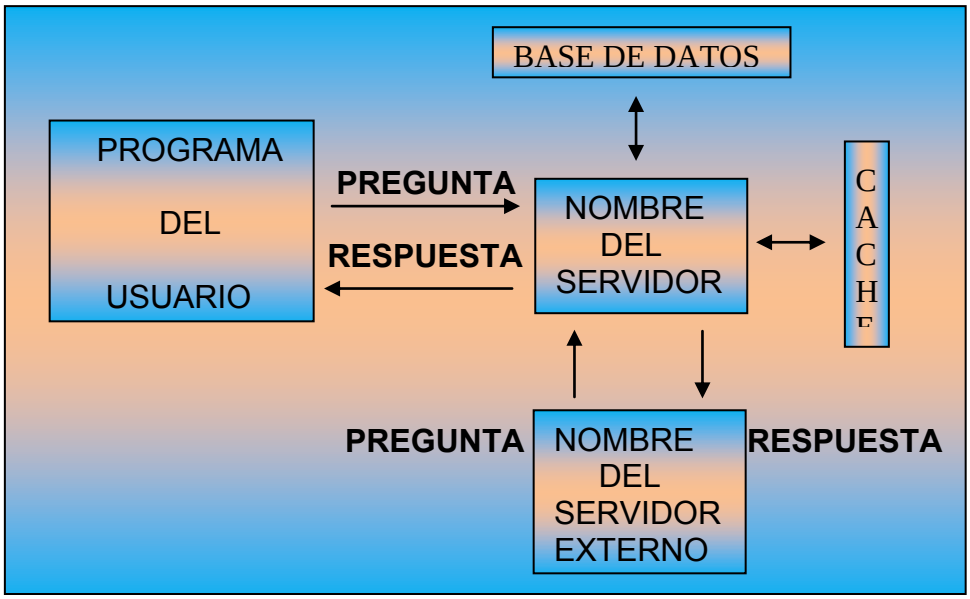


Figura 232 Resolución de nombres de dominio

6.5.8.6 MAPEANDO DIRECCIONES IP A NOMBRES DE DOMINIO CONSULTAS CON PUNTEROS

El DNS suministra el mapeado de nombres simbólicos a direcciones IP *y* viceversa. Mientras que en principio es algo sencillo buscar en la base de datos una dirección IP, dado su nombre simbólico, el proceso inverso no se puede hacer respetando la jerarquía. Por este motivo, existe otro espacio de nombres para el mapeado inverso. Se halla en el dominio in-addr.arpa (arpa porque Internet era originalmente la red de ARPA). Como las direcciones IP suelen escribirse en formato decimal con puntos, hay una capa de dominios para cada jerarquía. Sin embargo, debido a que los nombres de dominio tienen primero la parte menos significativa del nombre y el formato decimal con puntos los bytes más significativos primero, la dirección decimal se muestra en orden inverso. Por ejemplo, el dominio del DNS correspondiente a la dirección IP 129.34.139.30 es 30.139.34.129.in-addr.arpa. Dada una dirección IP, el DNS puede utilizarse para encontrar el nombre del host que sea su pareja. Una consulta de nombre de dominio para encontrar los nombres del host asociado a una dirección IP se llama **consulta con puntero**.

6.5.8.7 OTROS USOS PARA EL DNS

EL DNS está designado para ser capaz de almacenar una gran cantidad de información. Una de las más importantes es información del **intercambio de correo**, usada para el encaminamiento del correo electrónico. Esto aporta dos servicios: transparencia al reencaminar el correo a un host distinto del especificado y la implementación de pasarelas de correo, que pueden recibir correo electrónico y redirigirlo usando un protocolo diferente de aquel con el que lo reciben.

6.5.9 ARP (ADDRESS RESOLUTION PROTOCOL)

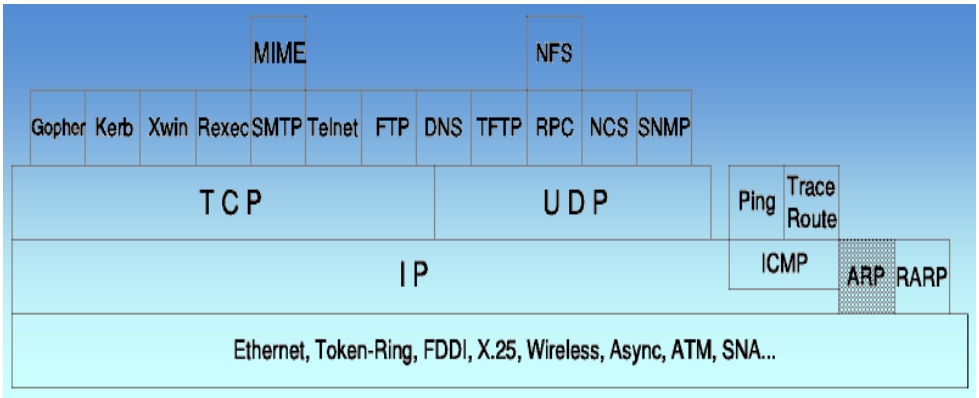


Figura 233 ARP ("Address Resolution Protocol")

El protocolo ARP es un protocolo de resolución de direcciones responsable de convertir las direcciones de protocolo de alto nivel (direcciones IP) a direcciones de red físicas.

6.5.9.1 DESCRIPCION DE ARP

En una sola red física, los hosts individuales se conocen en la red a través de su dirección física. Los protocolos de alto nivel direccionan a los hosts de destino con una dirección simbólica (en este caso la dirección IP). Cuando tal protocolo quiere enviar un datagrama a la dirección IP de destino w.x.y.z, el manejador de dispositivo no la entiende. En consecuencia, se suministra un módulo (ARP) que traducirá la dirección IP a la dirección física del host de destino. Utiliza una tabla (llamada a veces **caché ARP**) para realizar esta traducción. Cuando la dirección no se encuentra en la caché ARP, se envía un broadcast en la red, con un formato especial llamado **petición ARP**. Si una de las máquinas en la red reconoce su propia dirección IP en la petición, devolverá una **respuesta ARP** al host que la solicitó. La respuesta contendrá la dirección física del hardware así como información de encaminamiento (si el paquete ha atravesado puentes durante su trayecto) tanto esta dirección como la ruta se almacenan en la caché del host solicitante. Todos los posteriores datagramas enviados a esta dirección IP se podrán asociar a la dirección física correspondiente, que será la que utilice el manejador de dispositivo para mandar el datagrama a la red. ARP se diseño para ser usado en redes que soportan broadcast por hardware. Esto significa, por ejemplo, que ARP no funcionará en una red X.25.

6.5.9.2 CONCEPTO DETALLADO DE ARP

ARP se emplea en redes IEEE 802 además de en las viejas redes DIX Ethernet para mapear direcciones IP a dirección hardware. Para hacer esto, ha de estar estrechamente relacionado con el manejador de dispositivo de red. De hecho, las especificaciones de ARP en RFC 826 sólo describen su funcionalidad, no su implementación, que depende en gran medida del manejador de dispositivo para el tipo de red correspondiente, que suele estar codificado en el **microcódigo del adaptador.**

6.5.9.2.1 GENERACION DEL PAQUETE ARP

Si una aplicación desea enviar datos a una determinada dirección IP de destino, el mecanismo de encaminamiento IP determina primero la dirección IP del siguiente salto del paquete (que puede ser el propio host de destino o un router) y el dispositivo hardware al que se debería enviar. Si se trata de una red 802.3/4/5, deberá consultarse el módulo ARP para mapear el par <tipo de protocolo, dirección de destino> a una dirección física. El módulo ARP intenta hallar la dirección en su caché. Si encuentra el par buscado, devuelve la correspondiente dirección física de 48 bits al llamador (el manejador de dispositivo). Si no lo encuentra, **descarta el paquete** (se asume que al

ser un protocolo de alto nivel volverá a transmitirlo) y genera un broadcast de red para una solicitud ARP.

Figura 234 Paquete de petición/respuesta ARP

- **Hardware Address Space**.-Especifica el tipo de hardware; ejemplos son Ethernet o Packet Radio Net.
- **Protocol Address Space**.-Especifica el tipo de protocolo, el mismo que en el campo de tipo EtherType en la cabecera de IEEE 802.
- **Hardware Address Length**.-Especifica la longitud (en bytes) de la dirección hardware del paquete. Para IEEE 802.3 e IEEE 802.5 será de 6.
- **Protocol Address Length**.-Especifica la longitud (en bytes) de las direcciones del protocolo en el paquete. Para IP será de 4.
- **Operation Code**.-Especifica si se trata de una petición (1) o una solicitud (2) ARP.
- **Source/Target Hardware Address**.-Contiene las direcciones físicas hardware. En IEEE 802.3 son direcciones de 48 bits.
- **Source/Target Protocol Address**.-Contiene las direcciones del protocolo. En TCP/IP son direcciones IP de 32 bits.

Para el paquete de solicitud, la dirección hardware de destino es el único campo indefinido del paquete.

6.5.9.2.2 RECEPCION DEL PAQUETE ARP

Cuando un host recibe un paquete ARP (bien un broadcast o una respuesta punto a punto), el dispositivo receptor le pasa el paquete al módulo ARP, que lo trata como se indica en la figura 235. Recepción del paquete ARP.

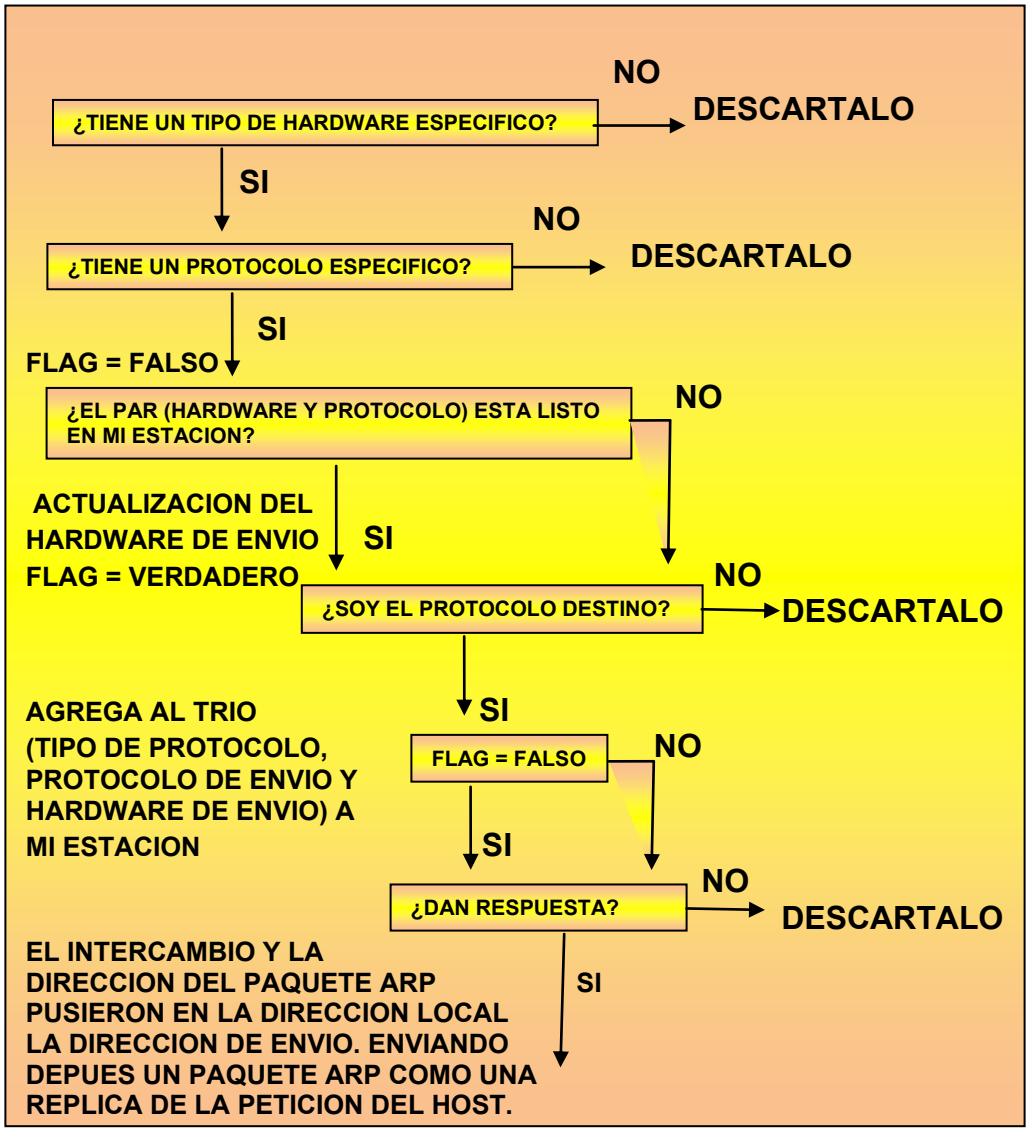


Figura 235 Recepción del paquete ARP

El host solicitante recibirá esta respuesta ARP, y seguirá el algoritmo ya comentado para tratarla. Como resultado, la tripleta <tipo de protocolo, dirección de protocolo, dirección hardware> para el host en cuestión se añadirá a la caché ARP. La próxima vez que un protocolo de nivel superior quiera enviar un paquete a ese host, el módulo de ARP encontrará la dirección hardware, a la que se enviará el paquete. Notar que debido a que la petición ARP original fue un broadcast en la red, todos los host en ella habrán actualizado la dirección del emisor en su propia caché (sólo si previamente ya existía esa entrada) en la tabla.

6.5.9.2.3 ARP Y SUBREDES

El protocolo ARP es el mismo aunque haya subredes. Recordar que cada datagrama IP pasa primero por el algoritmo de encaminamiento IP. Este algoritmo selecciona el manejador de dispositivo que debería enviar el paquete. Sólo entonces se consulta al módulo ARP asociado con ese manejador.

6.5.9.2.3.1 CONCEPTO DE PROXY ARP

Considerar una red IP, dividida en subredes, interconectadas por routers. Utilizamos el algoritmo IP viejo, lo que significa que ningún host conoce la existencia de múltiples redes físicas. Si se toman los hosts A y B, que se hallan en distintas redes físicas dentro de la misma red IP, y un router entre las dos subredes:

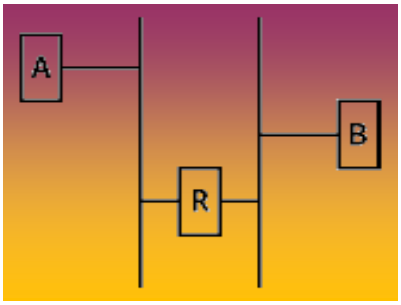


Figura 236 Hosts interconectados por un router

Cuando el host A quiere enviar un datagrama IP al host B, primero ha de determinar la dirección de red física del host B usando ARP. Como A no puede diferenciar entre las redes físicas, su algoritmo de encaminamiento IP piensa que el host B está en su misma red local y envía un broadcast de petición ARP. El host B no lo recibe, pero sí el router R. R entiende de subredes, es decir, ejecuta la versión de subred del algoritmo de encaminamiento y será capaz de ver que el destino de la petición ARP (en el campo de dirección de protocolo de destino) está localizado en otra red física. Si las tablas de encaminamiento de R especifican que el siguiente salto a otra red se produce a través de un dispositivo diferente, replicará al ARP **como si fuera el host B**, diciendo que la dirección de B es la del mismo router. El host A recibe esta respuesta ARP, la introduce en su caché y enviará los siguientes paquetes dirigidos a B al router R, que los retransmitirá a la subred adecuada. El resultado es subnetting transparente:
Los host normales (como A y B) desconocen el subnetting, por lo que usan el algoritmo de encaminamiento clásico.
Los router entre subredes:
Utilizan el algoritmo IP para subredes.
Usan un módulo ARP modificado, que puede responder en nombre de otros hosts.

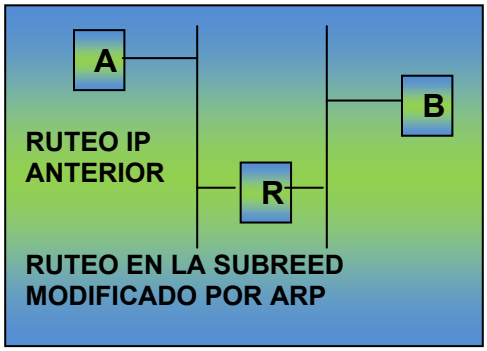


Figura 237 "Router" Proxy-ARP

6.5.10 RARP (REVERSE ADDRESS RESOLUTION PROTOCOL)

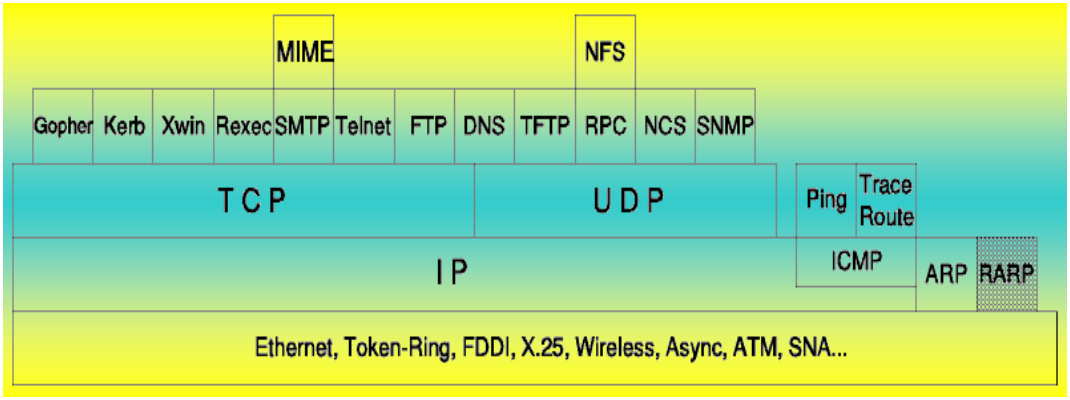


Figura 238 RARP (Reverse Address Resolution Protocol)

6.5.10.1 CONCEPTO DE RARP

El protocolo ARP es un **protocolo estándar específico de redes**. Algunos hosts, como por ejemplo estaciones de trabajo sin disco, desconocen su propia dirección IP cuando arrancan. Para determinarla, emplean un mecanismo similar al ARP, pero ahora el parámetro conocido es la dirección hardware el host y el requerido su dirección IP. La diferencia básica con ARP es el hecho de que debe existir un servidor RARP en la red que mantenga una base de datos de mapeados de direcciones hardware a direcciones de protocolo. El cálculo de direcciones inversas se efectúa del mismo modo que en ARP. Se usa el mismo formato de paquete figura 234 - Paquete petición/respuesta de ARP.
Una excepción es el campo **operation code** que ahora toma los siguientes valores:
3 para la petición RARP
4 para la respuesta RARP
Y, por supuesto, cabecera "física" de la trama indicará ahora que RARP es el protocolo de nivel superior (8035 hex) en vez de ARP (0806 hex) o IP (0800 hex) en el campo **EtherType**. El mismo concepto de RARP genera algunas diferencias:
ARP asume sólo que cada host conoce el mapeado entre su propia dirección hardware y de protocolo. RARP requiere uno o más hosts en la red para mantener una base de datos con los mapeados entre direcciones de red direcciones de protocolo de modo que serán capaces de responder a solicitudes de los host clientes.
Debido al tamaño que puede tomar esta base de datos, parte de las funciones del servidor suelen implementarse fuera del microcódigo del adaptador, con la opción de un pequeño caché en el microcódigo, que sólo es responsable de la recepción y transmisión de tramas RARP, estando el mapeado RARP en sí a cargo del software que se ejecuta en el servidor como un proceso normal.
La naturaleza de esta base de datos también requiere algún software para crear y actualizar la base de datos manualmente.
En caso de que haya múltiples servidores RARP en la red, el cliente RARP sólo hará uso de la primera respuesta RARP que reciba a su broadcast, y desechará las otras.

6.5.11 ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

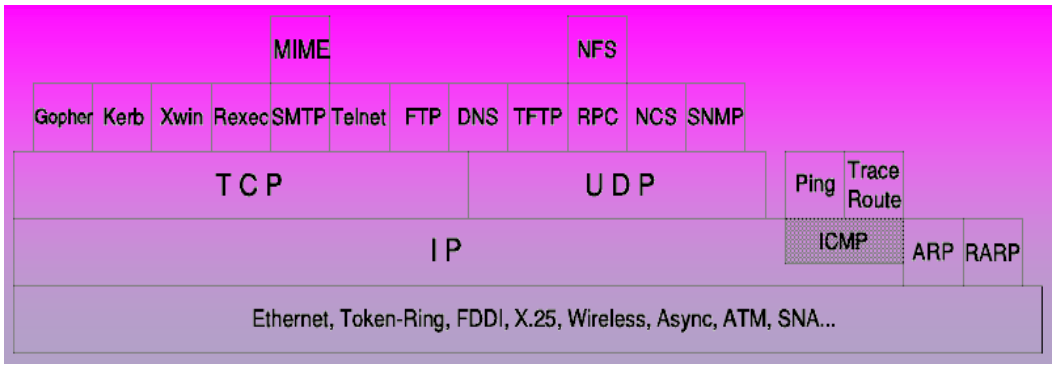


Figura 239 ICMP (Internet Control Message Protocol)

ICMP es un protocolo que incluye IP e IGMP (Internet Group Management). Cuando un router o un host de destino debe informar al host fuente acerca del procesamiento de datagramas, utiliza el ICMP. ICMP puede caracterizarse del modo siguiente:
ICMP usa IP como si ICMP fuera un protocolo del nivel superior (es decir, los mensajes ICMP se encapsulan en datagramas IP). Sin embargo, ICMP es parte integral de IP y debe ser implementado por todo módulo IP. ICMP se usa para informar de algunos errores, **no** para hacer IP fiable. Aún puede ocurrir que los datagramas no se entreguen y que no se informe de su pérdida. La fiabilidad debe ser implementada por los protocolos de nivel superior que usan IP. ICMP puede informar de errores en cualquier datagrama IP con la excepción de mensajes IP, para evitar repeticiones infinitas. Para datagramas IP fragmentados, los mensajes ICMP sólo se envían para errores ocurridos en el fragmento cero. Es decir, los mensajes ICMP nunca se refieren a un datagrama IP con un campo de desplazamiento de fragmento. Los mensajes ICMP nunca se envían en respuesta a datagramas con una dirección IP de destino que sea de broadcast o de multicast. Los mensajes ICMP nunca se envían en respuesta a un datagrama que no tenga una dirección IP de origen que represente a un único host. Es decir, la dirección de origen no puede ser cero, una dirección de loopback, de broadcast o de multicast.

Los mensajes ICMP nunca se envían en respuesta a mensajes ICMP de error. Pueden enviarse en respuesta a mensajes ICMP de consulta (los tipos de mensaje ICMP 0, 8, 9, 10 y 13 al 18). El RFC 792 establece que los mensajes ICMP **pueden** ser generados para informar de errores producidos en el procesamiento de datagramas IP, **no que deban**. En la práctica, los rotures generarán casi siempre mensajes ICMP para los errores, pero en el caso de los host de destino, el número de mensajes ICMP generados es una cuestión de implementación.

6.5.11.1 MENSAJES ICMP

Los mensajes ICMP se envían en datagramas IP. La cabecera IP siempre tendrá un número de protocolo de 1, indicando que se trata de ICMP y un servicio de tipo 0 (rutina). El campo de datos de IP contendrá el auténtico mensaje ICMP en el formato mostrado en la figura 240 Formato de mensajes ICMP.

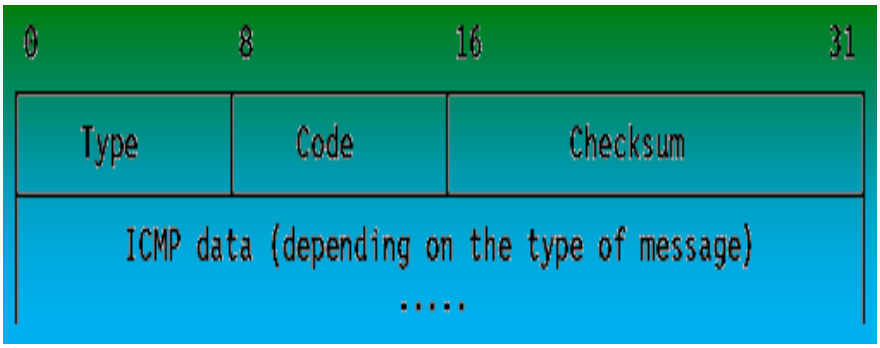


Figura 240 Formato de mensajes ICMP

- **Type**.-Especifica el tipo del mensaje:

- 0 Echo reply
- 3 Destination unreachable
- 4 Source quench
- 5 Redirect
- 0 Echo reply
- 3 Destination unreachable
- 4 Source quench
- 5 Redirect
- 8 Echo
- 9 Router Advertisement
- 10 Router Solicitation
- 11 Time exceeded
- 12 Parameter Problem
- 13 Timestamp request
- 14 Timestamp reply
- 15 Information request (obsolete)
- 16 Information reply(obsolete)
- 17 Address mask request
- 18 Address mask reply

- **Code**.-Contiene el código de error para el datagrama del que da parte el mensaje ICMP. La interpretación depende del tipo de mensaje.
- **Checksum**.-Contiene el complemento a 1 de 16 bits de la suma del **ICMP message starting with the ICMP Type field**. Para computar este checksum se asume en principio que su valor es cero. Este algoritmo es el mismo que el usado por IP para el cálculo de la cabecera IP. Compárese con el algoritmo de UDP y TCP que incluyen además una **pseudocabecera-IP** en el checksum.
- **Data**.-Contiene información para el mensaje ICMP. Típicamente se tratará de parte del mensaje IP original para el que se generó el mensaje ICMP. La longitud de los datos puede calcularse como la diferencia entre la longitud del datagrama IP que contiene el mensaje y la cabecera IP.

6.5.11.2 ECHO (8) Y ECHO REPLY (0)

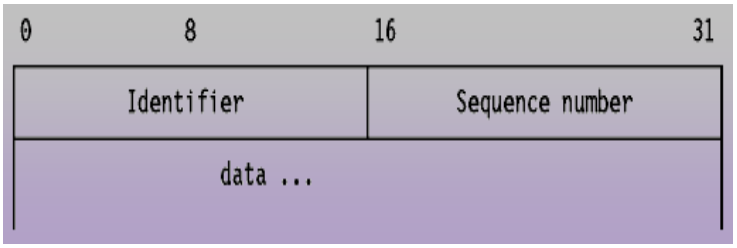


Figura 241 ICMP Echo y Echo Reply

Echo se usa para detectar si otro host está activo en la red. La fuente inicializa el identificador y el número de secuencia (que se utiliza cuando se envían múltiples mensajes **echo request**), añade algunos datos al campo de datos y envía el echo ICMP al host de destino. El código de la cabecera ICMP es cero. El receptor cambia el tipo del mensaje a echo reply y devuelve el datagrama al host fuente. El comando Ping emplea este mecanismo paca determinar si es posible alcanzar a un host de destino.

6.5.11.3 DESTINATION UNREEACHABLE (3)

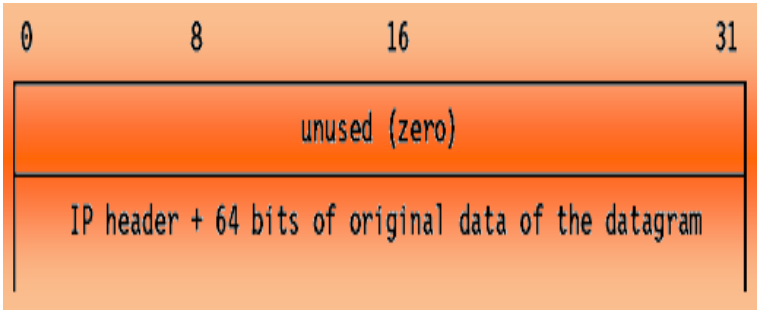


Figura 242 destination unreachable o destino inalcanzable de ICMP

Si este mensaje es recibido de un router intermediario, significa que el router considera la dirección IP de destino como inalcanzable. Si se recibe este mensaje del host de destino, significa que el protocolo especificado en el campo de número de protocolo del datagrama original no está activo, que ese protocolo no está activo en ese host o bien que es el puerto indicado el que no está activo. El campo de código de cabecera tendrá uno de los siguientes valores:

- 0 network unreachable
- 1 host unreachable
- 2 protocol unreachable
- 3 port unreachable
- 4 fragmentation needed but the **Do Not Fragment** bit was set
- 5 source route failed 6 destination network unknown
- 7 destination host unknown
- 8 source host isolated (obsolete)
- 9 destination network administratively prohibited
- 10 destination host administratively prohibited
- 11 network unreachable for this type of service
- 12 host unreachable for this type of service
- 13 communication administratively prohibited by filtering
- 14 host precedence violation
- 15 precedence cutoff in effect

Si un router implementa el protocolo de resolución de caminos MTU, el formato del mensaje Destination unreachable se cambia por el código 4 para incluir el MTU del enlace que no pudo aceptar el datagrama.

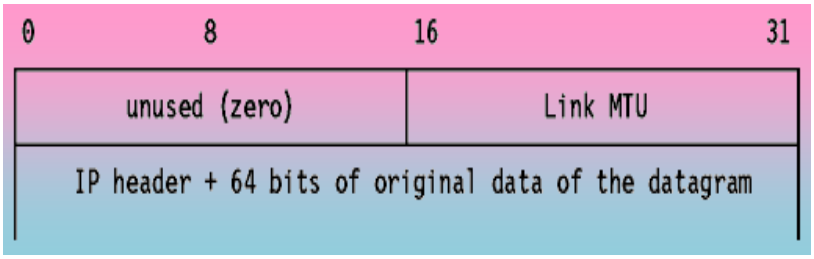


Figura 243 fragmentación de ICMP requerida con el enlace MTU

6.5.11.4 SOURCE QUENCH (4)

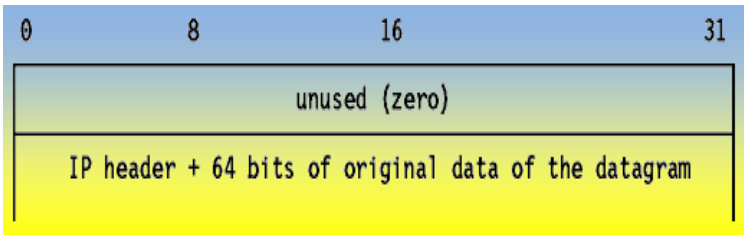


Figura 244 Source Quench de ICMP

Si se recibe este mensaje de un router intermedio, significa que el router no dispone de suficiente espacio en el buffer para encolar los datagramas de salida para la siguiente red. Si este mensaje procede del host de destino, significa que los datagramas entrantes llegan demasiado rápidos para ser procesados. El código de la cabecera ICMP siempre es cero.

6.5.11.5 REDIRECT (5)

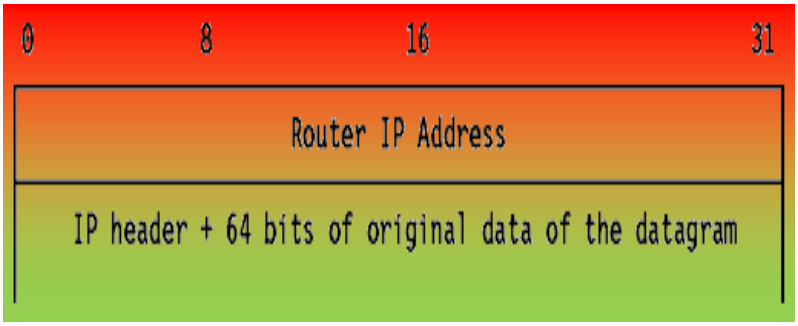


Figura 245 redirect de ICMP

Si se recibe este mensaje de un router intermedio, significa que el host debería los siguientes datagramas para esa red al router cuya dirección IP se especifica en el mensaje ICMP. Este otro router habrá de estar siempre en la misma subred que el host que envió el datagrama y el que lo devolvió. Enviará el datagrama a su siguiente dirección de salto; si la dirección del router coincide con la dirección fuente del datagrama original, indica un bucle. Este mensaje ICMP no se enviará si el datagrama IP contiene una ruta fuente. La cabecera ICMP tendrá uno de los siguientes valores:

- 0 Network redirect
- 1 Host redirect
- 2 Network redirect for this type of service
- 3 Host redirect for this type of service

6.5.11.6 ROUTER ADVERTISEMENT (9) Y ROUTER SOLICITATION (10)

Los mensajes ICMP 9 y 10 son opcionales.

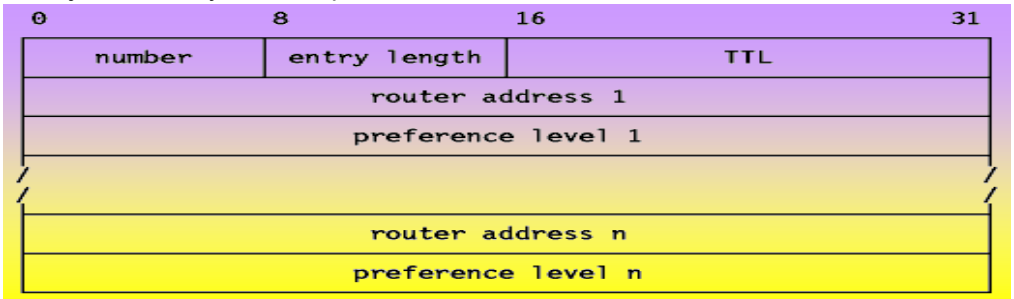


Figura 246 Router Advertisement de ICMP

Figura 247 Router Solicitation de ICMP

- **Number**.-El número de entradas del mensaje.
- **Entry Length**.-La longitud de una entrada en unidades de 32 bits. Vale 2 (32 bits para la dirección IP y 32 bits para el valor tomado por preferencia).
- **TTL**.-El número de segundos que se considerará válida una entrada.
- **Router Address**.-Una de las direcciones IP del host fuente.
- **Preference Level**.-Un nivel expresado con un valor de 32 bits con signo que indica la preferencia a asignar a esta dirección al seleccionar un router por defecto para una subred. Cada router de una subred es responsable de anunciar su propio nivel de preferencia. La preferencia aumenta cuanto mayor es el valor, y viceversa. El valor por defecto es cero, que está en el centro del rango de valores. Un valor de X'80000000' -2exp31 indica que el router no se debería usar jamás como router por defecto.

La cabecera ICMP es cero para ambos mensajes. Estos dos mensajes se usan si un host o un router soporta el **RDP (Router Discovery Protocol)**. El uso del multicast está recomendado, pero se puede usar el broadcast si la interfaz no soporta el multicast. Los router anuncian periódicamente sus direcciones IP en subredes si han sido configurados para que lo hagan. Los anuncios se hacen en la dirección de multicast (224.0.0.1) o de broadcast limitado (255.255.255.255). El comportamiento por defecto es enviar anuncios cada 10 minutos con un TTL de 1,800 segundos (30 minutos). Los routers también responden a los mensajes de solicitud que puedan recibir. Pueden responder directamente al solicitante, o esperar un intervalo de tiempo aleatorio y relativamente corto y responder con un multicast. Los hosts pueden enviar solicitudes hasta que reciben una respuesta. Las solicitudes se envían a la dirección de multicast para todos los rotures (224.0.0.2) o a la de broadcast limitado (255.255.255.255). Típicamente, tres mensajes de solicitud se envían a intervalos de 3 segundos. Alternativamente, un host puede esperar a los anuncios efectuados periódicamente. Cada vez que un host recibe un anuncio, actualiza su router por defecto si el nuevo anuncio tiene una preferencia superior y fija el TTL para que la entrada se ajuste al valor del nivel de preferencia. Cuando el host recibe un nuevo valor para su router por defecto actual, pone el valor TTL al del nuevo anuncio. Esto proporciona además un mecanismo para que los router se declaren no disponibles: envían un anuncio con un TTL de cero.

6.5.11.7 TIME EXCEEDED

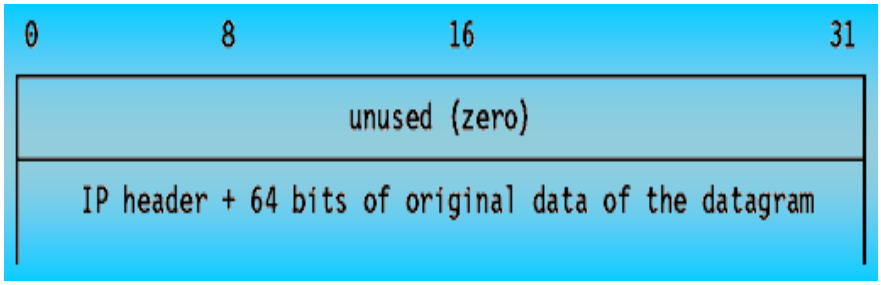


Figura 248 Time Exceeded de ICMP

Si se recibe este mensaje de un router intermedio, significa que el TTL de un datagrama IP ha expirado. Si se recibe del host de destino, significa que el TTL para ensamblar el datagrama ha expirado mientras el host esperaba uno de sus fragmentos. La cabecera ICMP puede tener uno de los siguientes valores:

- 0 transit TTL exceeded
- 1 reassembly TTL exceeded

6.5.11.8 PARAMETER PROBLEM (12)

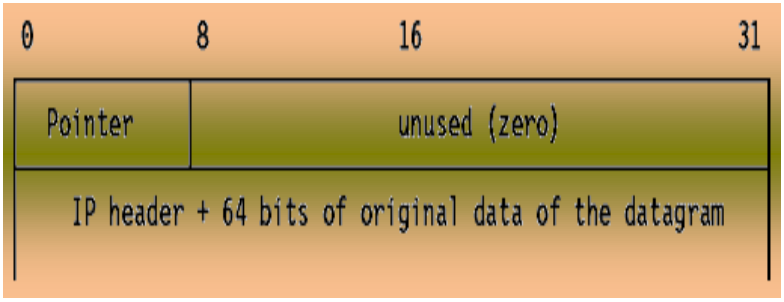


Figura 249 Parameter Problem de ICMP

Indica que se encontró un problema durante el procesamiento de los parámetros de la cabecera IP. El campo puntero apunta al byte del datagrama original en el que se encontró el problema. La cabecera ICMP puede tener uno de los siguientes valores:

- 0 unspecified error
- 1 required option missing

6.5.11.9 TIMESTAMP REQUEST (13) Y TIMESTAMP REPLY (14)

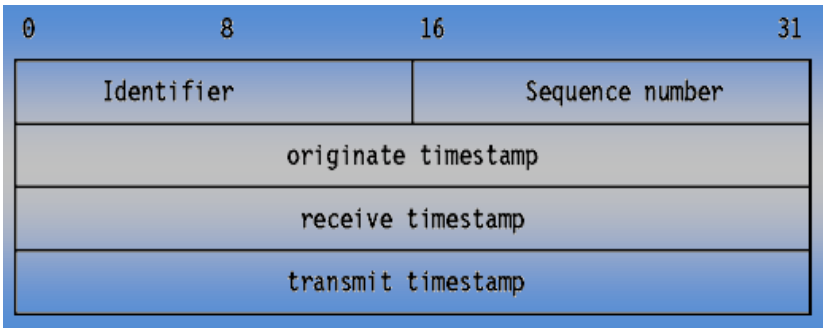


Figura 250 Timestamp Request y Timestamp Reply ICMP

Estos dos mensajes se emplean para medir el rendimiento y la depuración. No se emplean para la sincronización: para eso está el **NTP (Network Time Protocol)**. El host fuente envía el identificador y el número de secuencia (usado si se envían múltiples mensajes timestamp requests), fija su sello de tiempo y se lo envía al receptor. El host receptor fija el valor de los sellos de tiempo de recepción y de envío, cambia el tipo del mensaje a timestamp reply y se lo devuelve al receptor. El receptor dispone de dos sellos de tiempo en caso de que haya una diferencia sensible entre los tiempos de recepción y de transmisión, aunque en la práctica la mayoría de las implementaciones efectuarán ambas operaciones (recepción y respuesta) de una sola vez, dando a los dos sellos el mismo valor. Los sellos de tiempo indican el número de milisegundos transcurridos desde la medianoche según el meridiano de Greenwich (GMT).

6.5.11.10 INFORMATION REQUEST (15) E INFORMATION REPLY (16)

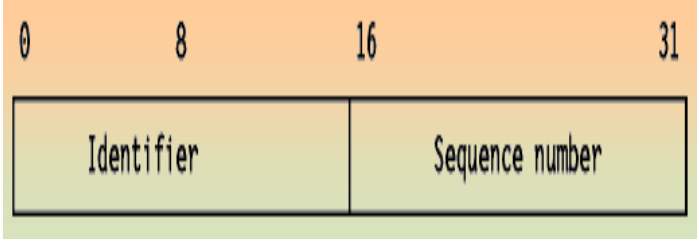


Figura 251 Information Request e Information Reply de ICMP

El mensaje Information Request lo lanza un host para obtener una dirección IP para una red con la que está conectado. El host fuente envía la solicitud con la dirección IP de destino puesta a cero en la cabecera IP (refiriéndose a su propia red) y espera una respuesta de un servidor autorizado a asignar direcciones IP a otros hosts. La cabecera ICMP vale cero. La respuesta contendrá la dirección IP de red en los campos de dirección fuente y dirección de destino de la cabecera IP. Este mecanismo está obsoleto.

6.5.11.11 ADDRESS MASK REQUEST (17) Y ADDRESS MASK REPLY (18)

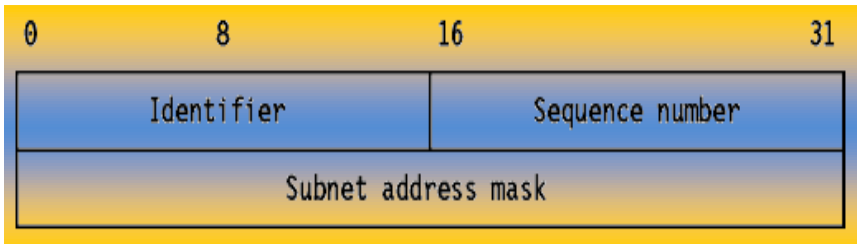


Figura 252 Address Mask Request y Reply de ICMP

El mensaje Address Mask Request es usado por un host cuando quiere determinar que máscara de subred usa la red a la que está conectado. La mayoría de los hosts se configurarán con su máscara de subred, pero algunos, tales como una estación de trabajo sin disco, deben obtener esta información de un servidor. Un host utiliza RARP, para obtener su dirección IP. Para obtener una máscara de subred, el host hace un broadcast del mensaje Address Mask Request. Cualquier host en la red que se haya configurado para enviar mensajes Address Mask Reply rellenará esta máscara, convertirá el tipo del mensaje a Address Mask Reply y se lo devolverá al host fuente. La cabecera ICMP tiene valor cero.

6.5.11.12 APLICACIONES DE ICMP

Hay dos aplicaciones simples y muy extendidas basadas en ICMP: el Ping y el Traceroute. El Ping usa los mensajes ICMP Echo y Echo Reply para determinar si un host es alcanzable. El Traceroute envía datagramas IP con bajos TTL's para que expiren durante la ruta que les dirige al destino. Utiliza los valores de los mensajes ICMP Time Exceeded para determinar en que parte de la red expiraron los datagramas y reconstruye así un esquema de la ruta hasta el host de destino.

6.5.11.13 ICMP PARA LA VERSIÓN 6 DE IP

La implementación de ICMP explicada arriba es específica de la versión 4 de IP (IPv4). La versión 6 de IP (IPv6) requerirá una nueva versión de ICMP. Las definiciones de ambas no están completas aún. Ya se conocen algunas características importantes:

- ICMP para IPv6 usará un nuevo número de protocolo para distinguirlo de ICMPv4.
- El formato de la cabecera ICMP permanecerá igual.
- Las longitudes de los campos de los mensajes cambiarán para ajustarse a los mensajes IPv6, que serán de mayor longitud.
- Los valores Type y Code cambiarán. Algunos valores poco usados se eliminarán.

- El tamaño de los mensajes ICMP aumentará con el fin de explotar el tamaño máximo aumentado de los paquetes que IPv6 puede trasmitir sin fragmentar.
- La variante Fragmentation Required del mensaje ICMP Destination unreachable será reemplazado por el mensaje Packet Too Big que incluirá la MTU (Maximum Transmission Unit) de salida en la que se ha localizado el problema.
- IGMP (Internet Group Management Protocol) se fundirá con ICMP.

6.5.12 UDP (USER DATAGRAM PROTOCOL)

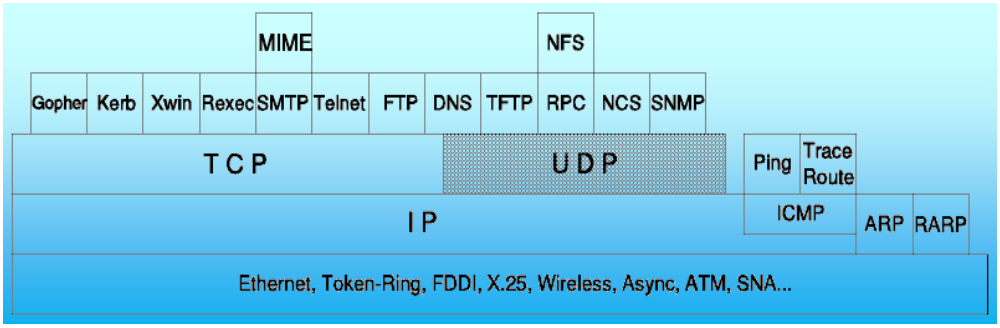


Figura 253 UDP (User Datagram Protocol)

UDP es básicamente una interfaz de aplicación. No añade fiabilidad, control de flujo o recuperación de errores a IP. Simplemente sirve como multiplexor/demultiplexor para enviar y recibir datagramas, usando **los puertos** para dirigir los datagramas tal como se muestra en la figura 254 UDP, un demultiplexor basado en puertos.

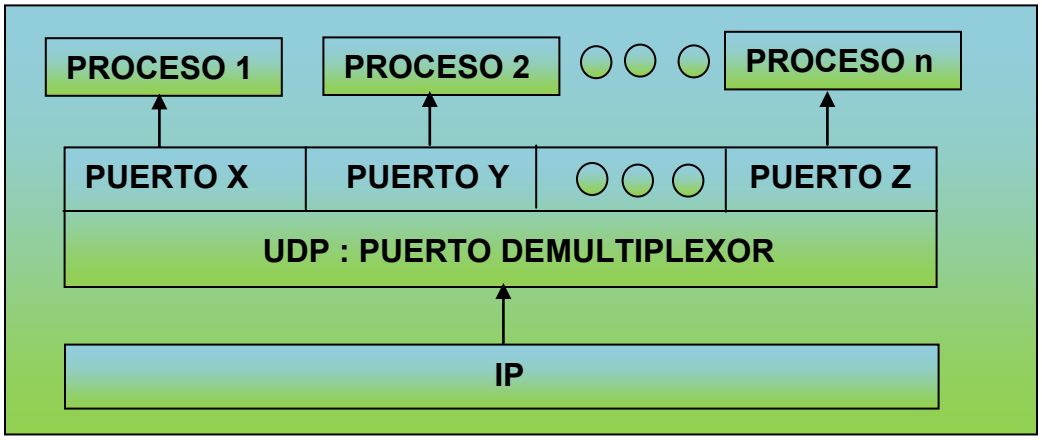


Figura 254 UDP, un demultiplexor basado en puertos

UDP suministra un mecanismo para que una aplicación envíe un datagrama a otra. Se considera que la capa de UDP es extremadamente delgada y en consecuencia tiene poco overhead, pero requiere que la aplicación se responsabilice de la recuperación de errores y todo lo que ello conlleva.

6.5.12.1 PUERTOS

Las aplicaciones que envían datagramas a un host necesitan identificar un objetivo más específico que la dirección IP, ya que los datagramas suelen dirigirse a procesos concretos y no a todo el sistema. UDP permite hacer esto al hacer uso de los **puertos**. Un puerto es un número de 16 bits que identifica en un host que proceso está asociado a un datagrama. Hay dos tipos de puerto:

- **Bien-conocidos (well-known)**.-Los puertos bien-conocidos pertenecen a servidores estándar, por ejemplo Telnet usa el puerto 23. Los puertos bien-conocidos se hallan en el

rango de 1 a 1,023 (anteriormente a 1992, el rango de 256 a 1,023 se usaba para servidores específicos de UNIX). Estos puertos suelen tener números impares, debido a que los primeros sistemas que usaron el concepto de puerto requerían para las operaciones en dúplex una pareja par/impar de puertos. La mayoría de los servidores requieren sólo un único puerto. Una excepción es el servidor BOOTP (BOOTstrap Protocol) que usa dos: el 67 y el 68. La razón de ser de los puertos bien-conocidos es permitir a los clientes encontrar a los servidores sin necesidad de información de configuración.

- **Efímeros**.-Los clientes no necesitan puertos bien-conocidos porque inician la comunicación con los servidores y los datagramas UDP enviados al servido contienen su número de puerto. El host en funcionamiento proporciona un puerto a cada proceso cliente mientras este lo necesite. Los números de puertos efímeros tienen valores mayores de 1,023, por lo general en el rango de 1,024 a 5,000. Un cliente puede usar cualquier número en ese rango, siempre que la combinación <protocolo de transporte, dirección IP, número de puerto> sea unívoca.

Nota: TCP también usa puertos con los mismos valores. Estos puertos son totalmente independientes de los de UDP. Normalmente, un servidor usará TCP o UDP, aunque hay excepciones. Por ejemplo, el DNS usa tanto el puerto 53 de UDP como el 53 de TCP.

6.5.12.2 FORMATO DEL DATAGRAMA UDP

Cada datagrama UDP se envía en un sólo datagrama de IP. Aunque el datagrama IP se fragmente durante la transmisión, la implementación de IP que lo reciba lo reensamblará antes de pasárselo a la capa de UDP. Todas las implementaciones de IP deben aceptar datagramas de 576 bytes, lo que significa que si se supone un tamaño máximo de 60 bytes para la cabecera IP, queda un tamaño de 516 bytes para el datagrama UDP, aceptado por todas las implementaciones. Muchas implementaciones aceptan datagramas más grandes, pero no es algo que esté garantizado. El datagrama UDP tiene una cabecera de 16 bytes que se describe en la figura 255 formato del datagrama UDP.

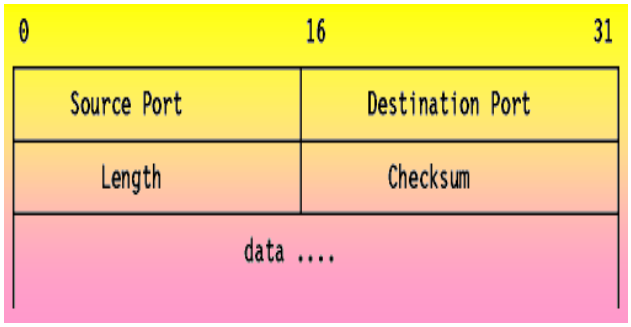


Figura 255 Formato del datagrama UDP

- **Puerto Origen**.-Indica el puerto del proceso que envía el datagrama. Es el puerto al que se deberían dirigir las respuestas.
- **Puerto Destino**.-Especifica el puerto destino en el host de destino.
- **Longitud**.-Es la longitud (en bytes) del mismo datagrama de usuario, incluyendo la cabecera.
- **Checksum**.-Es un campo opcional consistente en el complemento a uno de 16 bits de la suma en complemento a uno de una pseudocabecera IP, la cabecera UDP y los datos del datagrama UDP. La pseudocabecera IP contiene las direcciones IP de origen y destino, el protocolo y la longitud del datagrama UDP.

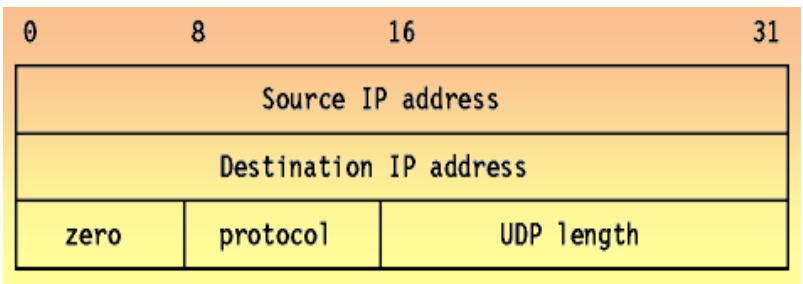


Figura 256 Pseudocabecera IP

La pseudocabecera IP extiende de modo efectivo su checksum que incluya al datagrama IP original (sin fragmentar).

6.5.12.3 INTERFAZ DE PROGRAMACIÓN DE APLICACIÓN DE UDP

La API proporciona:

- La creación de nuevos puertos para la recepción.
- Operación de recepción que devuelve los bytes de datos recibidos y una indicación del puerto y la dirección IP de origen.
- Operación de envío que tiene como parámetros los datos, los puertos de origen y destino y las direcciones IP.
- La forma en que se implementa esto queda a elección del cada distribuidor.

Hay que ser consciente de que IP y UDP no proporcionan una entrega garantizada, control de flujo ni recuperación de errores, así que estos deberán ser implementados por la aplicación.
Aplicaciones estándar que usan UDP son:
TFTP (Trivial File Transfer Protocol)
DNS (Domain Name System)
RPC (Remote Procedure Call), usado por el NFS (Network File System)
NCS (Network Computing System)
SNMP (Simple Network Management Protocol)

6.5.13 TCP (TRANSMISION CONTROL PROTOCOL)

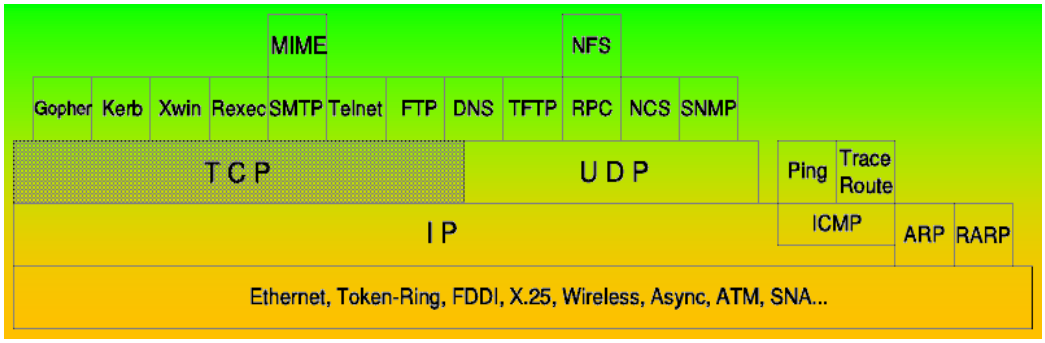


Figura 257 TCP (Transmission Control Protocol)

TCP proporciona una cantidad considerablemente mayor de servicios a las aplicaciones que UDP, notablemente, la recuperación de errores, control de flujo y fiabilidad. Se trata de un protocolo **orientado a conexión** a diferencia de UDP. La mayoría de los protocolos de aplicación de usuario, como TELNET y FTP, usan TCP.

6.5.13.1 ZOCALOS

Dos procesos se comunican a través de **zócalos TCP**. El modelo de zócalo proporciona a un proceso una conexión con un flujo full dúplex de bytes con otro proceso. La aplicación no necesita preocuparse de la gestión de este canal; estos servicios son suministrados por TCP. TCP usa el mismo principio de puerto que UDP para conseguir multiplexación. Al igual que UDP, TCP utiliza puertos efímeros y bien conocidos. Cada extremo de una conexión TCP tiene un zócalo que puede identificarse con la tripleta <TCP, dirección IP address, número de puerto>. Es lo que se llama una **medio asociación**. Si dos procesos se están comunicando sobre TCP, tendrán una **conexión lógica** identificable unívocamente por medio de los dos zócalos implicados, es decir, con la combinación <TCP, dirección IP local, puerto local, dirección IP remota, puerto remoto>,figura 258 Conexión TCP. Los procesos del servidor son capaces de gestionar múltiples conversaciones a través de un único puerto.

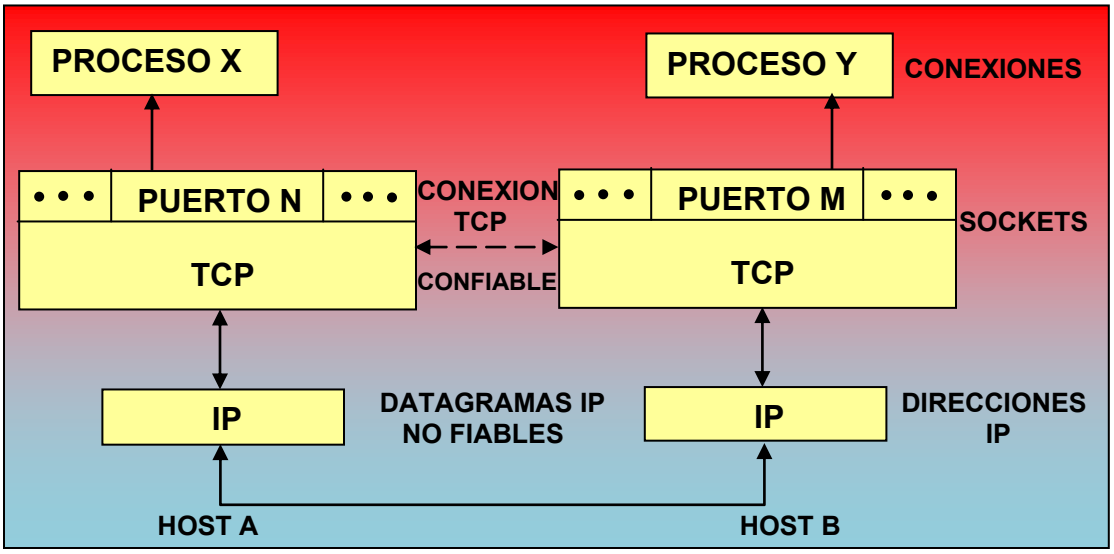


Figura 258 Conexión TCP - Los procesos X e Y se comunican sobre una conexión TCP que emplea datagramas IP.

6.5.13.2 CONCEPTO DE TCP

Como se señaló arriba, el principal propósito de TCP es **proporcionar una conexión lógica fiable entre parejas procesos**. No asume la fiabilidad de los protocolos de niveles inferiores (como IP) por lo que debe ocuparse de garantizarla. TCP se puede caracterizar por los siguientes servicios que suministra a las aplicaciones que lo usan:

- Transferencia de datos a través de un canal
- Desde el punto de vista de la aplicación, TCP transfiere **un flujo continuo de bytes** a través de Internet. La aplicación no ha de preocuparse de fragmentar los datos en bloques o en datagramas. TCP se encarga de esto al agrupar los bytes en **segmentos TCP**, que se pasan a IP para ser retransmitidos al destino. Además, TCP decide por sí mismo cómo segmentar los datos y puede enviarlos del modo que más le convenga. A veces, una aplicación necesita estar segura de que todos los datos pasados a TCP han sido transmitidos efectivamente al destino. Por esa razón, se define la función **push**. Esta función mandará todos los segmentos que sigan almacenados al host de destino. El **cierre normal de la conexión** también provoca que se llame a esta función, para evitar que la transmisión quede incompleta.
- Fiabilidad: TCP asigna un número de secuencia a cada byte transmitido, y espera un reconocimiento afirmativo (ACK) del TCP receptor. Si el ACK no se recibe dentro de un intervalo de timeout, los datos se retransmiten. Como los datos se transmiten en bloques (segmentos de TCP), al host de destino sólo se le envía el número de secuencia del byte de cada segmento. El TCP receptor utiliza los números de secuencia para organizar los segmentos cuando llegan fuera de orden, así como para eliminar segmentos duplicados.

- Control de flujo: El TCP receptor, al enviar un ACK al emisor, indica también el número de bytes que puede recibir aún, sin que se produzca sobrecarga y desbordamiento de sus buffers internos. Este valor se envía en el ACK en la forma del número de secuencia más elevado que se puede recibir sin problemas. Este mecanismo se conoce también como mecanismo de **ventanas**
- Multiplexación: Se consigue usando puertos, al igual que en UDP.
- Conexiones lógicas: La fiabilidad y el control de flujo descritos más arriba requieren que TCP inicialice y mantenga cierta información de estado para cada canal. La combinación de este estado, incluyendo zócalos, números de secuencia y tamaños de ventanas, se denomina conexión lógica. Cada conexión se identifica unívocamente por el par de zócalos del emisor y el receptor.
- Full Dúplex: TCP garantiza la concurrencia de los flujos de datos en ambos sentidos e la conexión.

6.5.13.3 EL PRINCIPIO DE LA VENTANA

Un simple protocolo de transporte podría emplear el siguiente principio: enviar un paquete, y esperar un reconocimiento del receptor antes de enviar el siguiente. Si el ACK no se recibe dentro de cierto límite de tiempo, se retransmite.

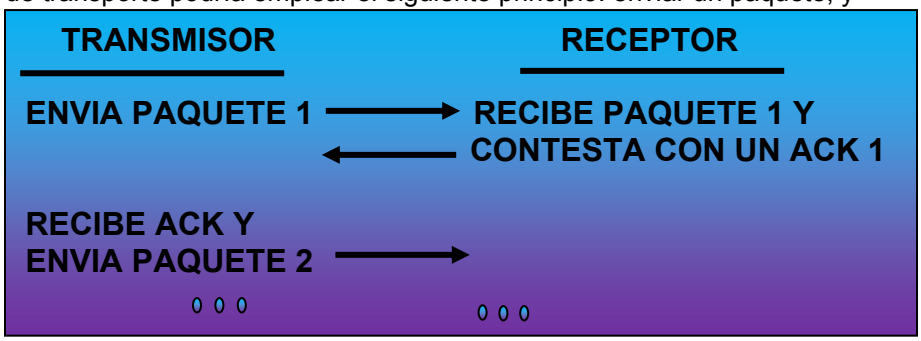


Figura 259 El principio de la ventana

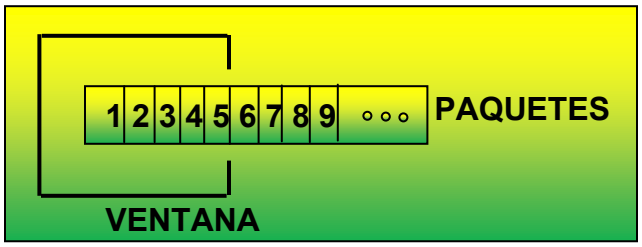


Figura 260 Paquetes del mensaje

Aunque este mecanismo asegura fiabilidad, sólo usa una parte del **ancho de banda de la red** que está disponible. Considerar ahora un protocolo en el que el emisor agrupa los paquetes que va a transmitir como se muestra en la figura 260 Paquetes del mensaje:

Y utiliza las siguientes reglas:

- El emisor puede enviar todos los paquetes dentro de la ventana sin recibir un ACK, pero debe disparar un cronómetro para el timeout para cada uno de ellos.
- El receptor debe reconocer cada paquete recibido, indicando el número de secuencia del último paquete bien recibido.
- El emisor desliza la ventana para cada ACK recibido.
- En nuestro ejemplo, el emisor puede transmitir paquetes del 1 al 5 sin esperar respuesta:

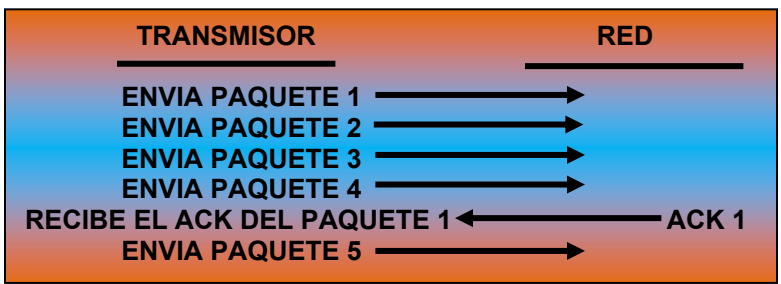


Figura 261 El principio de la ventana

En el momento en que el emisor recibe el ACK 1, puede deslizar su ventana para excluir el paquete 1:

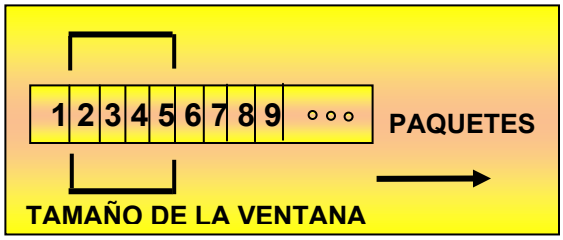


Figura 262 Paquetes del mensaje

En este punto, el emisor puede transmitir también el paquete 6. Imaginar algunos casos especiales:

- El paquete 2 se pierde: el emisor no recibirá ACK 2, por lo que su ventana permanecerá en posición 1 (como se ve en al última figura). De hecho, como el receptor no recibió el paquete 2, reconocerá los paquetes 3, 4 y 5 con un ACK 1, que fueron los últimos paquetes recibidos en secuencia. En el extremo del emisor, al final se producirá un timeout para el paquete 2 y se retransmitirá. Notar que la recepción de este paquete en el receptor generará un ACK 5, ya que se habrán recibido con éxito los paquetes del 1 al 5, y la ventana del emisor se deslizará cuatro posiciones al recibir el ACK 5.
- El paquete 2 llegó, pero el reconocimiento se perdió: el emisor no recibe ACK 2, pero recibe ACK 3. ACK 3 es un reconocimiento de **todos** los paquetes hasta el 3 (incluyendo el 2) y el emisor ya puede deslizar su ventana hasta el paquete 4.

Conclusión:
Este mecanismo de ventanas asegura:
Transmisión fiable
Mejor aprovechamiento del ancho de banda (mejora del flujo).
Control de flujo, ya que el receptor puede retrasar la respuesta a un paquete con un reconocimiento, conociendo los buffers libres de los que dispone y el tamaño de la ventana de comunicación.

6.5.13.4 EL PRINCIPIO DE LA VENTANA APLICADO A TCP

El mecanismo mostrado más arriba se utiliza en TCP, pero con unas cuantas diferencias: Como TCP proporciona una conexión con un flujo de bytes, los números de secuencia se asignan a cada byte del canal. TCP divide el flujo de bytes en segmentos. El principio de la ventana se aplica a nivel de bytes; es decir, los segmentos enviados y los ACK's recibidos llevarán números de secuencia de forma que el tamaño de la ventana se exprese con un número de bytes, en vez del de paquetes. El tamaño de la ventana lo determina el receptor, cuando se establece la conexión, y puede *variar* durante la transmisión de datos. Cada ACK incluirá el tamaño de la ventana que acepta el receptor en ese momento. Ahora, el flujo de datos del emisor se puede ver como:

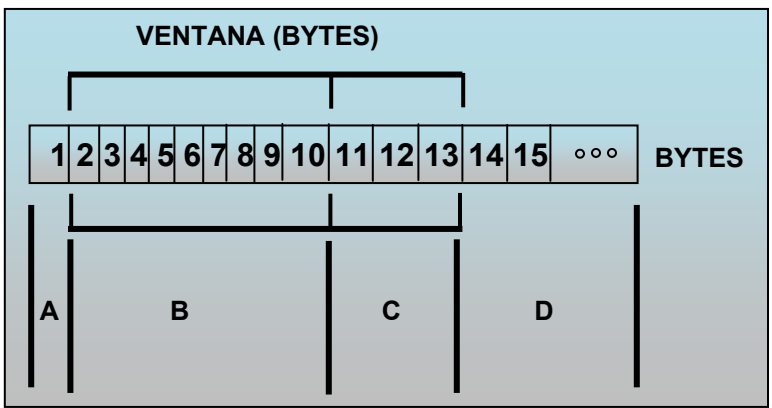


Figura 263 Principio de la ventana aplicado a TCP

- A Bytes transmitidos que han sido reconocidos.
- B Bytes enviados pero no reconocidos.
- C Bytes que se pueden enviar sin esperar ningún tipo de reconocimiento.
- D Bytes que no se pueden enviar aún.

Recordar que TCP agrupa los bytes en segmentos, y un segmento TCP sólo lleva el número de secuencia del primer byte.

6.5.13.5 FORMATO DEL MENSAJE EN TCP

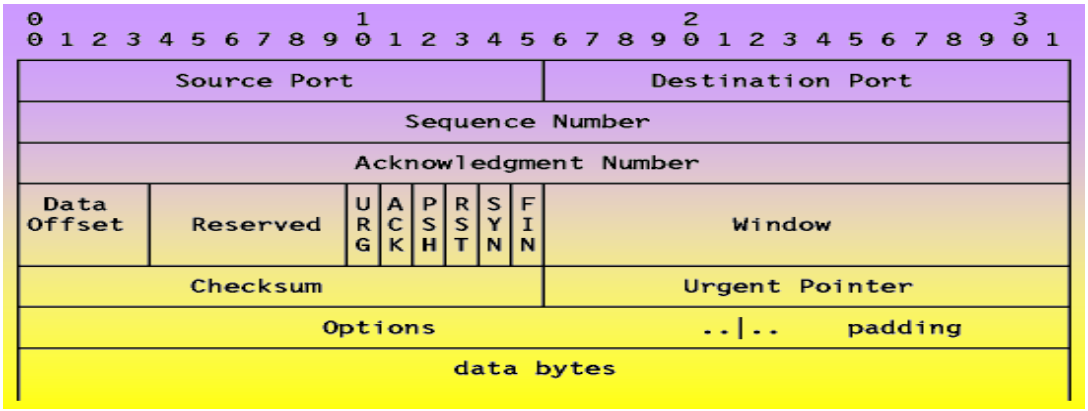


Figura 264 Formato de segmento en TCP

- **Source Port**.-El número de puerto de 16 bits del emisor, que el receptor usa para responder.
- **Destination Port**.-El número de puerto de 16 bits del receptor.
- **Sequence Number**.-El número de secuencia del primer byte de datos del segmento. Si el byte de control SYN está a 1, el número de secuencia es el inicial (n) y el primer byte de datos será el n+1.
- **Acknowledgment Number**.-Si el bit de control ACK está a 1, este campo contiene el valor del siguiente número de secuencia que se espera recibir.
- **Data Offset**.-El número de palabras de 32 bits de la cabecera TCP. Indica dónde empiezan los datos.
- **Reserved**.-Seis bits reservados para su uso futuro; deben ser cero.
- **URG**.-Indica que el campo urgent pointer es significativo en el segmento.
- **ACK**.-Indica que el campo de reconocimiento es significativo en el segmento.
- **PSH**.-Función Push.
- **RST**.-Resetea la conexión.
- **SYN**.-Sincroniza los números de secuencia.
- **FIN**.-No hay más datos del emisor.
- **Window**.-Usado en segmentos ACK. Especifica el número de bytes de datos que comienzan con el byte indicado en el campo número de reconocimiento que el receptor esta dispuesto a aceptar.

- **Checksum**.-El complemento a uno de 16 bits de la suma de los complementos a uno de todas las palabras de 16 bits de la pseudocabecera, la cabecera TCP y los datos TCP. Al computar el checksum, el mismo campo checksum se considera cero. La pseudocabecera es la misma que utiliza UDP para calcular el checksum. Es una pseudocabecera IP, usada sólo para calcular el checksum, con el formato mostrado en la figura 265 Pseudocabecera IP:

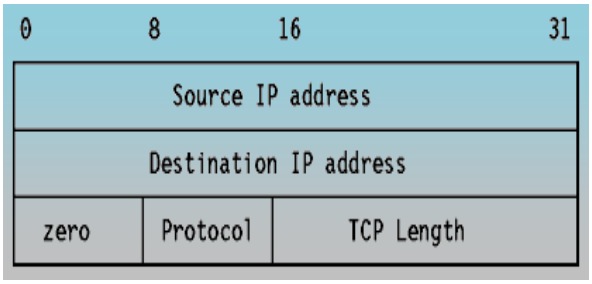


Figura 265 Pseudocabecera IP

- **Urgent Pointer**.-Apunta al primer octeto de datos que sigue a los datos importantes. Sólo es significativo cuando el bit de control URG está a uno.
- **Options**.-Sólo para el caso de opciones de datagramas IP, las opciones pueden ser: Un sólo byte conteniendo el número de opción, o una opción de longitud variable con el siguiente formato:

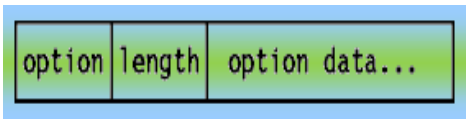


Figura 266 Opción del datagrama IP - Opción de longitud variable.

Actualmente hay definidas tres opciones:

Tipo	Longitud	Significado
0	-	Fin e la lista de opciones.
1	-	No-Operación.
2	4	Tamaño máximo del segmento.

Esta opción sólo se usa durante el establecimiento de la conexión (bit de control SYN puesto a uno) y se envía desde el extremo que ha de recibir datos para indicar la máxima longitud de segmento que es capaz de manejar. Si esta opción no se usa, se admiten segmentos de cualquier tamaño.

- **Padding**.-Bytes todos a cero para rellenar la cabecera TCP a una longitud total que sea un múltiplo de 32 bits.

6.5.13.6 RECONOCIMIENTOS Y RETRANSMISIONES

TCP envía los datos en segmentos de longitud variable. Los números de secuencia se basan en una cuenta de los bytes. Los **reconocimientos especifican el número de secuencia del siguiente byte que el receptor espera recibir.** Ahora suponer que un segmento se pierde o se corrompe. En ese caso, el receptor reconocerá cualquier segmento sucesivo con un reconocimiento referido al primer byte del paquete perdido. Finalmente, se producirá un timeout y el segmento perdido se retransmitirá. Suponer un tamaño de ventana de 1,500 bytes, y segmentos de 500 bytes.

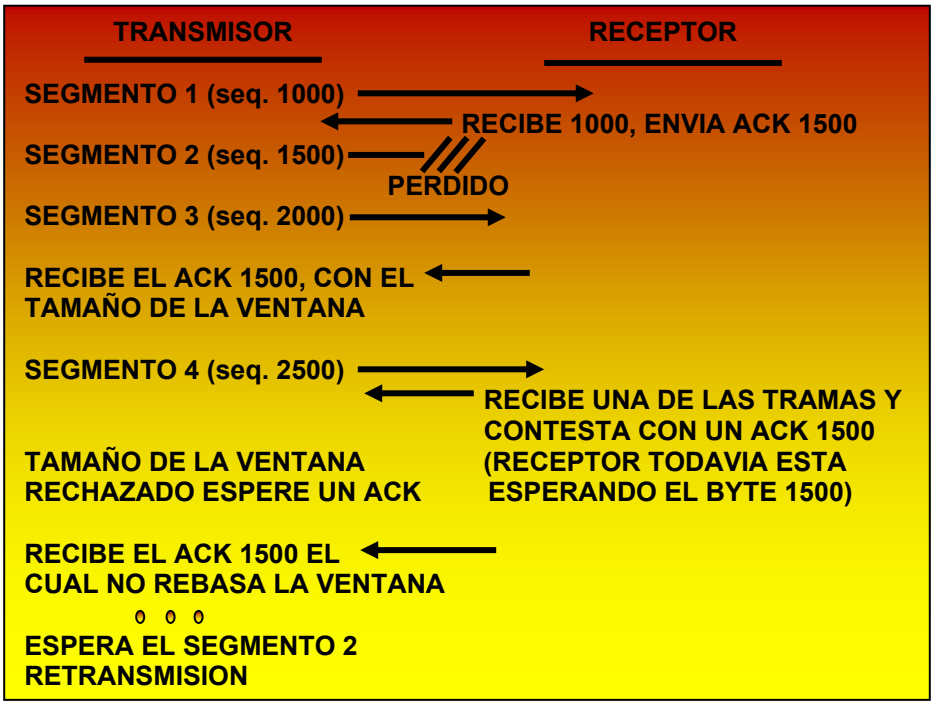


Figura 267 Proceso de reconocimiento y retransmisión

Ahora surge un problema, ya que el emisor sabe que el segmento 2 está perdido o corrompido, pero no sabe nada de los segmentos 3 y 4. El emisor debería retransmitir al menos el segmento 2, pero también podría retransmitir los segmentos 3 y 4. Es posible que:
El segmento 3 haya sido recibido, y no se sepa nada del 4: podría haber sido recibido ya, sin que el ACK haya llegado, o se podría haber perdido también.
El segmento 3 se haya perdido, y se haya recibido el ACK 1,500 a la recepción del segmento 4.
Cada implementación de TCP es libre de reaccionar ante un timeout del modo que deseen los diseñadores. Podría retransmitir sólo el segmento 2, pero en el segundo caso indicado arriba, estaremos esperando hasta que el timeout del segmento 3 expire. En este caso, se pierden todas las ventajas del rendimiento del mecanismo de ventanas. O bien TCP podría reenviar inmediatamente todos los segmentos de la ventana actual. Sea cual sea la elección, el rendimiento máximo se pierde. Esto se debe a que el ACK no contiene un segundo número de secuencia indicando la trama actual que se ha recibido.

6.5.13.7 INTERVALOS DE TIMEOUT VARIABLE

Cada TCP debería implementar un algoritmo para adaptar los tiempos de timeout a usar para el viaje de los segmentos. Para hacerlo, TCP registra el momento de envío de un segmento, y el de recepción del ACK. Se promedia un valor para varios de estos viajes que se empleará como valor de timeout para el siguiente segmento a enviar. Esto es una característica importante, ya que los retardos pueden ser variables en la red, dependiendo de múltiples factores, tales como la carga de las redes intermedias de baja velocidad o la saturación de los gateways.

6.5.13.8 ESTABLECIMIENTO DE UNA CONEXION TCP

Antes de que se pueda transferir cualquier dato, se ha de establecer una conexión entre los dos procesos. Uno de los procesos (normalmente el servidor) lanza una llamada **OPEN pasiva**, el otro una llamada **OPEN activa**. El OPEN pasivo permanece dormido hasta que otro proceso intenta comunicarse con él a través de un OPEN activo. En la red, se intercambian tres segmentos TCP:

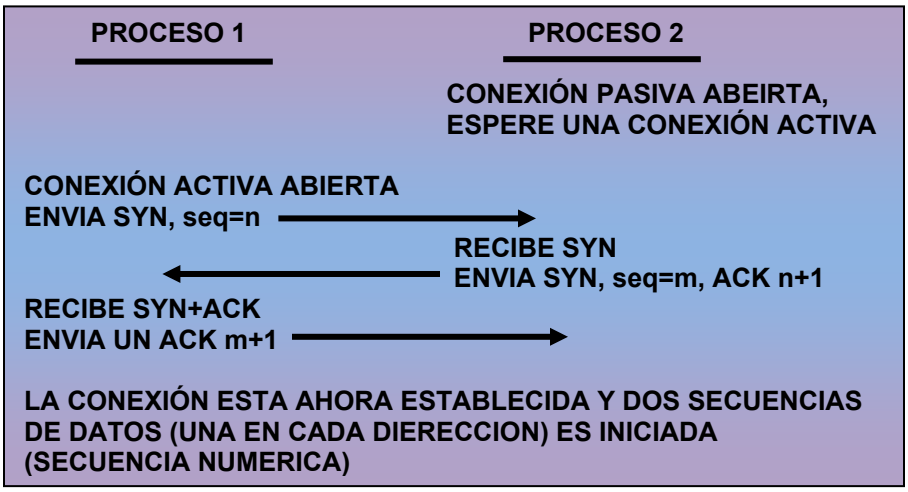


Figura 268 Establecimiento de la conexión TCP

Este proceso completo se conoce como **three-way handshake**, o acuerdo en tres fases. Notar que los segmentos TCP intercambiados incluyen los números de secuencia iniciales de ambas partes, para ser usados en posteriores transferencias. El **cierre** de la conexión se hace de forma implícita enviando un segmento TCP con el bit FIN activo. Como la conexión es full dúplex, el segmento FIN sólo cierra la conexión en un sentido del canal. El otro proceso enviará los datos restantes, seguidos de un segmento TCP en el que el bit FIN está activo. La conexión se borra (es decir, la información de estado en ambos extremos) una vez que el canal se ha cerrado en ambos sentidos.

6.5.13.9 SEGMENTOS TCP TRANSPORTADOS EN DATAGRAMAS IP

Los TCP segmentos se transportan sobre datagramas IP con la siguiente configuración de parámetros:

- Tipo de servicio = 00000000
- es decir: precedencia = rutina
- retraso = normal
- rendimiento = normal
- TTL = 00111100 (un minuto)

6.5.13.10 API DE TCP

La API de TCP no está definida del todo. Sólo algunas funciones básicas que deberían ser proporcionadas se describen en el **RFC 793 - TCP**. Como ocurre con la mayoría de los RFC's de la pila de protocolos TCP/IP, se deja un elevado grado de libertad a los diseñadores, permitiendo en consecuencia implementaciones óptimas (dependientes del sistema operativo), lo que resulta en una mayor eficiencia. El RFC describe las siguientes llamadas a funciones:

- Open.-Para establecer una conexión, tiene varios parámetros:
- Activo/pasivo
- Zócalo remoto
- Número de puerto local
- Timeout (opcional)

Y muchas otras opciones. Devuelve un **nombre para la conexión local**, que se usa para referenciarla en todas las otras funciones.

- Send.-Hace que los datos del buffer del usuario señalado se envíen por la conexión. Opcionalmente puede tener los flags URGENT o PUSH activo.
- Receive.-Copia los datos TCP que van llegando a un buffer de usuario.

- Close.-Cierra la conexión; provoca un push de todos los restantes datos y segmentos TCP con el flag FIN activo.
- Status.-Es una llamada dependiente de la implementación que devuelve información como:
  - Zócalo local y remoto
  - Tamaños de las ventanas de recepción y envío
  - Estado de la conexión
  - Nombre de la conexión local
  - Abort.-Hace que todas las operaciones de recepción y envío aborten, y se envíe un RESET al TCP remoto.

6.5.14 TELNET

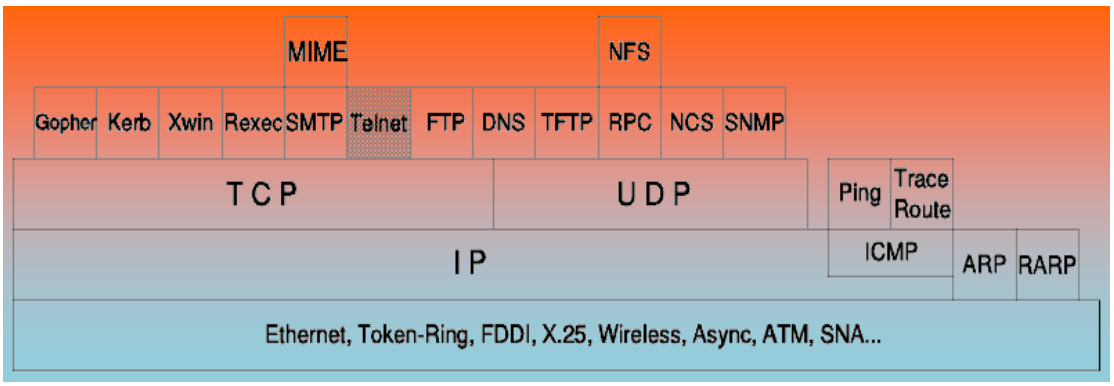


Figura 269 TELNET- Protocolo de conexión remota.

El protocolo TELNET proporciona una interfaz estandarizada, a través de la cual un programa de un host (el cliente de TELNET) puede acceder a los recursos de otro host (el servidor de TELNET) como si el cliente fuera una terminal local conectada al servidor. Por ejemplo, un usuario de una estación de trabajo situada en una LAN se puede conectar al host. Por supuesto, TELNET se puede usar tanto en LAN's como en WAN's.

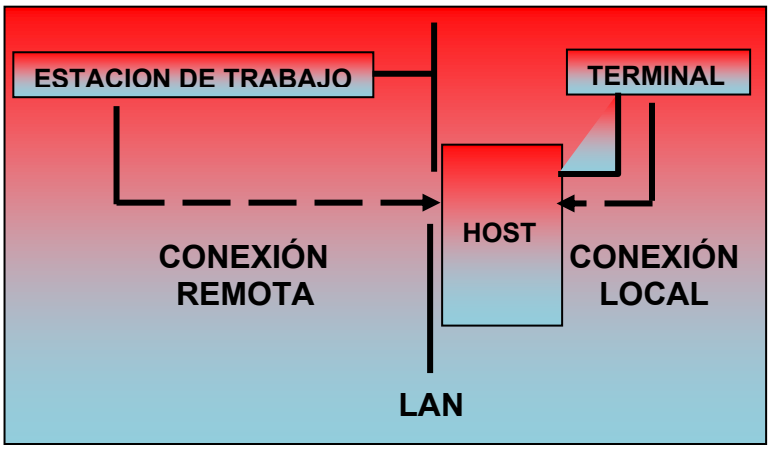


Figura 270 Conexión remota usando TELNET

TELNET permite la entrada del usuario conectado a la LAN del mismo modo que lo haría el usuario de una terminal local. La mayoría de las implementaciones de TELNET no soportan entornos gráficos.

6.5.14.1 FUNCIONAMIENTO DE TELNET

TELNET es un protocolo basado en las siguientes ideas:

- El concepto de **NVT (Network Virtual Terminal)**. Una NVT es un dispositivo imaginario que posee una estructura básica común a una amplia gama de terminales reales. Cada host mapea las características de su propia terminal sobre las de su correspondiente NVT, y asume todos los demás hosts harán lo mismo. Una perspectiva simétrica de las terminales y los procesos.

- Negociación de las opciones de la terminal. El protocolo TELNET usa el principio de opciones negociadas, ya que muchos host pueden desear suministrar servicios adicionales, más allá de los disponibles en la NVT. Se pueden negociar diversas opciones. El cliente y el servidor utilizan una serie de convenciones para establecer las características operacionales de su conexión TELNET a través de los mecanismos **DO, DON'T, WILL, WON'T (hazlo, no lo hagas, lo harás, no lo harás)**. Los dos hosts comienzan verificando que existe una comprensión mutua entre ellos. Una vez que se ha completado esta negociación inicial, son capaces de trabajar en el nivel mínimo implementado por la NVT. Después de haber logrado este entendimiento mutuo, pueden negociar opciones adicionales para ampliar las capacidades de la NVT y así reflejar con precisión la capacidad del hardware real que se está usando. Debido al modelo simétrico usado por TELNET, tanto el cliente como el servidor pueden proponer el uso de opciones adicionales.

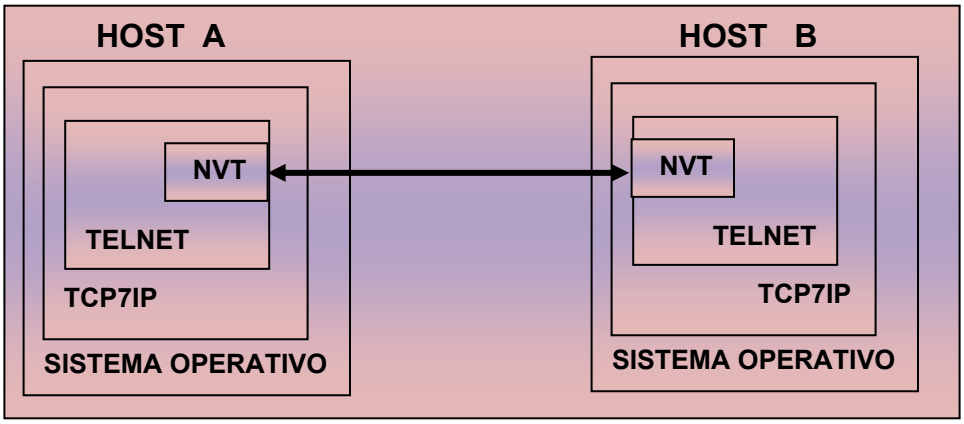


Figura 271 El modelo simétrico de TELNET - La negociación comienza con la NVT como punto de partida.

6.5.14.2 NVT (NETWORK VIRTUAL TERMINAL)

La NVT cuenta con un monitor o display y un teclado. El teclado produce datos de salida, que se envían por la conexión TELNET. El monitor recibe los datos de entrada que llegan. Las características básicas de una NVT, a menos que sean modificadas por opciones establecidas de común acuerdo, son:

- Los datos se representan en código ASCII de 7 bits, transmitido en bytes de 8 bits.
- La NVT es un dispositivo semidúplex que opera en modo de buffer en línea.
- La NVT proporciona una función de eco local.

Todas estas opciones pueden ser negociadas por los dos hosts. Por ejemplo, se prefiere el eco local porque la carga de la red es inferior y el rendimiento superior pero existe la opción de usar el eco remoto, aunque no se le requiera a ningún host.

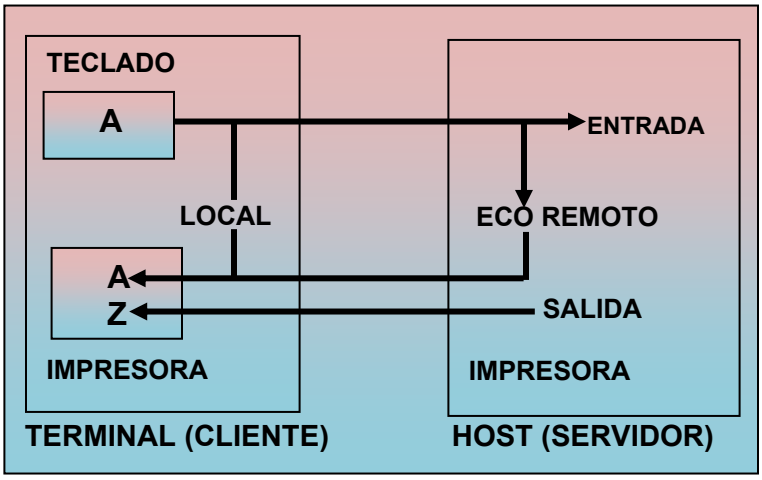


Figura 272: Opción de eco -Se puede usar la función de eco remoto en vez del local si ambas partes están de acuerdo.

La anchura del retorno de carro y la longitud de la página en un monitor NVT no están especificados. Puede manejar caracteres ASCII imprimibles (códigos ASCII del 32 al 126) y puede entender algunos caracteres ASCII de control tales como:

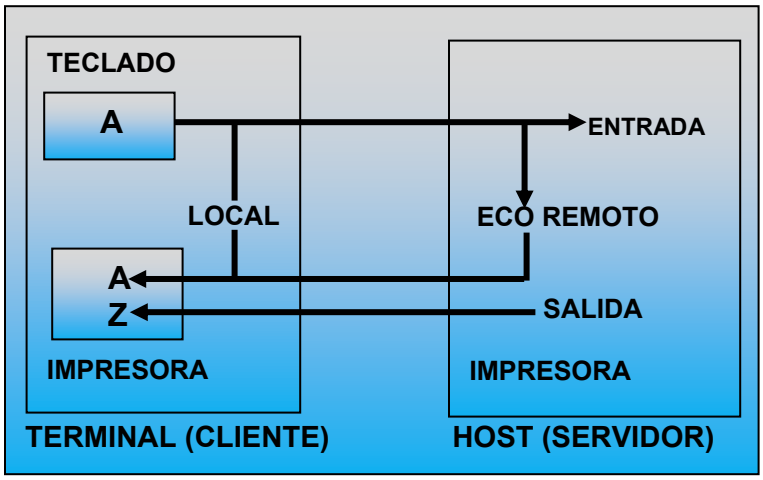
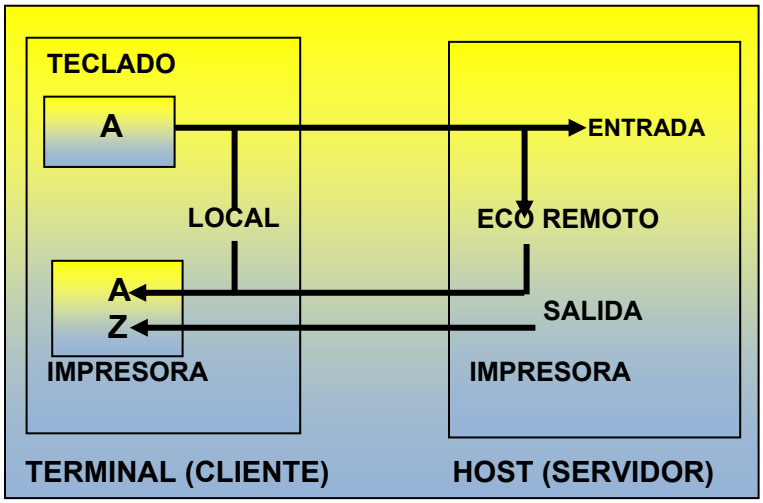


Figura 273

6.5.14.3 OPCIONES DE TELNET



Hay un gran número de opciones de TELNET; definidas las siguientes opciones:

Figura 274 Opciones (Parte 1 de 2) de TELNET

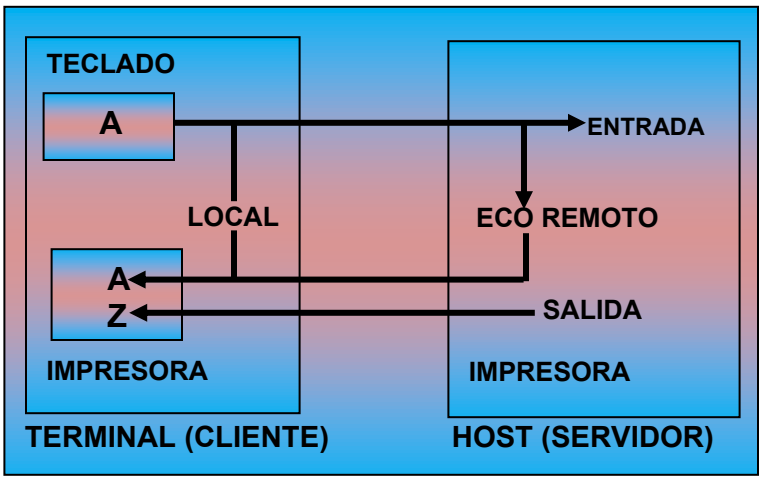


Figura 275 Opciones (Parte 2 de 2) de TELNET

El TELNET a pantalla completa es posible siempre que el cliente y el servidor tengan medios compatibles para el uso de esta. Por ejemplo, VM y MVS proporcionan un servidor capaz de soportar un TN3270. Para usar este recurso, el cliente debe soportar también el TN3270.

6.5.14.4 ESTRUCTURA DE COMANDOS EN TELNET

La comunicación entre cliente y servidor es manejada por comandos internos, que no son accesibles a los usuarios. Todos los comandos internos de TELNET consisten en secuencias de 2 o 3 bytes, dependiendo del tipo de comando.

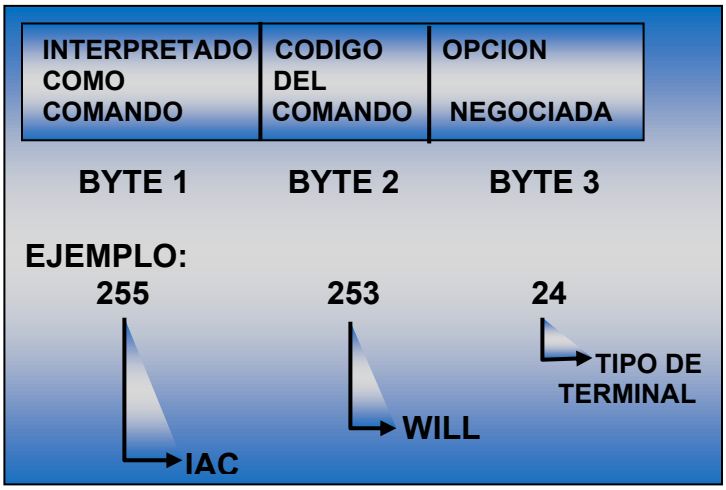


Figura 276 Estructura de los comandos internos de TELNET - Este comando propone la negociación sobre el tipo de terminal

El carácter **IAC (Interpret As Command, Interpretar Como Comando)** es seguido de un código de comando. Si este comando trata con opciones de negociación, el comando tendrá un tercer byte para Si este comando trata con opciones de negociación, el comando tendrá un tercer byte para mostrar el código asociado a la opción indicada.

6.5.14.5 NEGOCIACION DE OPCIONES

Usando los comandos internos, TELNET es capaz de negociar opciones en cada host. La base inicial de la negociación es la NVT: cada host que se quiera conectar debe estar de acuerdo con este mínimo. Cada opción se puede negociar haciendo uso de los cuatro códigos de comando WILL, WON'T, DO, DON'T. Además, algunas opciones tienen a su vez subopciones: si ambas partes acuerdan una opción, usarán los comandos SB y SE para llevar a cabo la subnegociación. Aquí se muestra un ejemplo simplificado de como funciona la negociación de opciones:

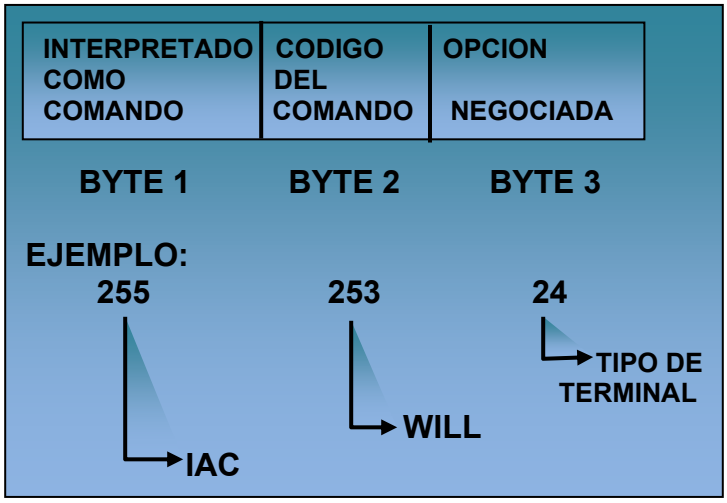


Figura 277 Los tipos de terminal se definen en STD 2 - Números asignados.

6.5.14.6 COMANDOS BÁSICOS DE TELNET

El objetivo principal del protocolo TELNET es proporcionar una interfaz estándar para hosts en una red. Para permitir que comience una conexión. TELNET establece una representación estándar para algunas funciones:
IP Interrumpir proceso
AO Abortar la salida

AYT ¿Estás ahí?
EC Borrar carácter
EL Borrar línea
SYNCH Sincronizar

6.5.15 TFTP (TRIVIAL FILE TRANSFER PROTOCOL)

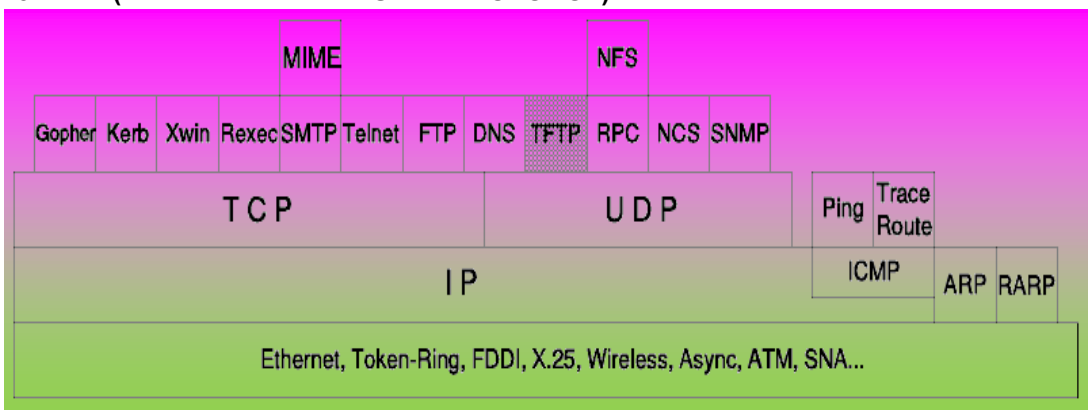


Figura 278 TFTP (Trivial File Transfer Protocol)

La transferencia de ficheros en TCP/IP es una transferencia de datos de disco a disco, en oposición, por ejemplo, al comando SENDFILE de VM, una función que en el mundo de TCP/IP se considera de correo, en la que envías a los datos al buzón de alguien (el lector en el caso de VM). TFTP es un protocolo extremadamente trivial para la transferencia de ficheros. Se implementa sobre la capa UDP y carece de la mayoría de las características de FTP. La única cosa que es capaz de hacer es leer/escribir un fichero de/en un servidor.
Nota: No dispone de medios para la autentificación de usuarios: es un protocolo inseguro.

6.5.15.1 USO DE TFTP

El comando: TFTP <nombre del host> conduce al prompt interactivo en el que se pueden introducir subcomandos:

- Connect <host> especifica el identificador del host de destino
- Mode <ascii/binary> especifica el tipo del modo de transferencia
- Get <remote filename> [<nombre del fichero local>] recupera un fichero
- Put <remote filename> [<nombre del fichero local>] almacena un fichero
- Verbose Activa o desactiva el modo **verbose**, en el que muestra información adicional durante la transferencia del fichero.
- Quit salir TFTP

6.5.15.2 DESCRIPCION DEL PROTOCOLO TFTP

Cualquier transferencia comienza con una solicitud para leer o escribir un fichero. Si el servidor concede la solicitud, se abre la conexión y el fichero se envía en bloques consecutivos de 512 bytes (longitud fija). Los bloques del fichero se numeran correlativamente, comenzando en 1. Cada paquete de datos debe ser reconocido mediante un paquete de reconocimiento antes de que se envíe el siguiente paquete. Se asume la terminación de la transferencia al recibir un paquete de menos de 512 bytes. La mayoría de los errores provocarán la terminación de la conexión (falta de fiabilidad), Si un paquete se pierde en la red, se producirá un **timeout**, tras el que se efectuará la retransmisión del último paquete (de datos o de reconocimiento). En el RFC 783 se describió un bug bastante grave, conocido como el Síndrome del Aprendiz de Brujo. Puede causar una retransmisión excesiva en ambas partes de la conexión en algunas circunstancias en las que se producen retardos de red. Se documentó en el RFC 1123 y se corrigió en el 1350. Para más detalles, remitirse a estos RFC's.

6.5.15.3 PAQUETES TFTP

Sólo existen cinco tipos de paquetes:
1 Read Request (Solicitud de lectura RRQ)
2 Write Request (Solicitud de escritura WRQ)
3 Data Datos
4 Acknowledgment (Reconocimiento ACK)
5 Error
La cabecera de TFTP contiene el identificador opcode asociado al paquete.

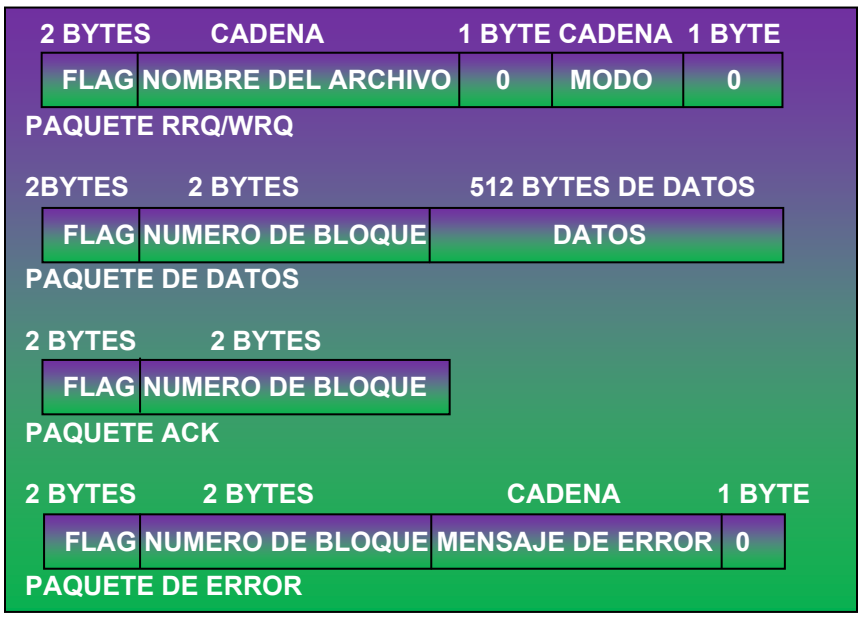


Figura 279 Paquetes TFTP

6.5.15.4 MODOS DE TRANSFERENCIA

Actualmente se definen tres modos de transferencia en el RFC 1350:

- NetASCII
- US-ASCII tal como se define en el Código Estadounidense Estándar para el Intercambio de Información (**USA Standard Code for Information Interchang**") con modificaciones especificadas en el RFC 854 - Especificaciones del protocolo Telnet y extendido para usar el bit de mayor orden. Es decir, se trata de un juego de caracteres de 8 bits, a diferencia del US-ASCII, que es de 7-bits.
- Octeto También llamado binario, consiste simplemente en bytes de 8 bits.
- Correo Este modo se definió originalmente en el RFC 783 y el RFC 1350 lo declaró obsoleto. Permitía efectuar la transferencia enviando correo a un usuario en vez de un fichero. El modo empleado se indica en el paquete Request for Read/Write (RRQ/WRQ).

12 FTP (FILE TRANSFER PROTOCOL)

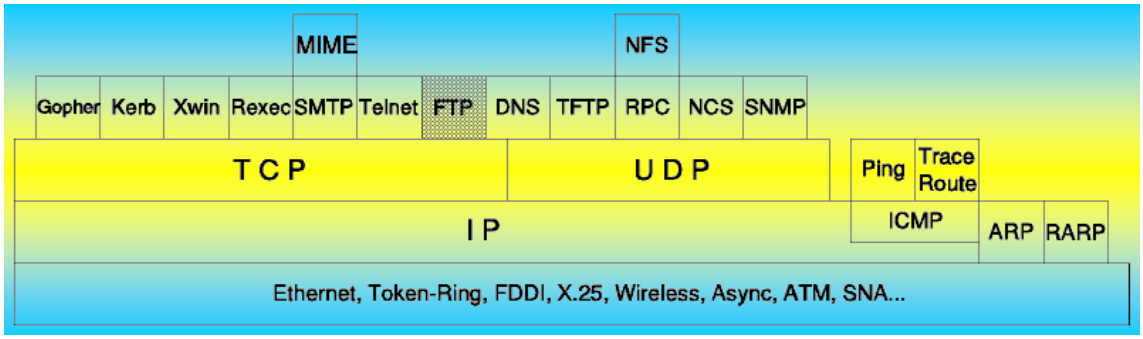


Figura 280 FTP

La copia de ficheros de una máquina a otra es una de las operaciones más frecuentes. La transferencia de datos entre cliente y servidor puede producirse en cualquier dirección. El cliente puede enviar o pedir un fichero al servidor. Para acceder a ficheros remotos, el usuario debe identificarse al servidor. En este punto el servidor es responsable de autentificar al cliente antes de permitir la transferencia de ficheros. Desde el punto de vista de un usuario de FTP, el enlace está orientado a conexión. En otras palabras, es necesario que ambos hosts estén activos y ejecutando TCP/IP para establecer una transferencia de ficheros.

6.5.16.1 DESCRIPCION DE FTP

FTP usa TCP como protocolo de transporte para proporcionar conexiones fiables entre los extremos. Se emplean dos conexiones: la primera es para el login y sigue el protocolo TELNET y la segunda es para gestionar la transferencia de datos. Como es necesario hacer un login en el host remoto, el usuario debe tener un nombre de usuario y un password para acceder a ficheros y a directorios. El usuario que inicia la conexión asume la función de cliente, mientras que el host remoto adopta la función de servidor En ambos extremos del enlace, la aplicación FTP se construye con intérprete de protocolo (PI), un proceso de transferencia de datos, y una interfaz de usuario, figura 281 Principios de FTP. La interfaz de usuario se comunica con el PI, que está a cargo del control de la conexión. Este intérprete de protocolo ha de comunicar la información necesaria a su propio sistema de archivos. En el otro extremo de la conexión, el PI, además de su función de responder al protocolo TELNET, ha de iniciar la conexión de datos. Durante la transferencia de ficheros, los DTP's se ocupan de gestionar la transferencia de datos. Una vez que la operación del usuario se ha completado, el PI ha de cerrar la conexión de control.

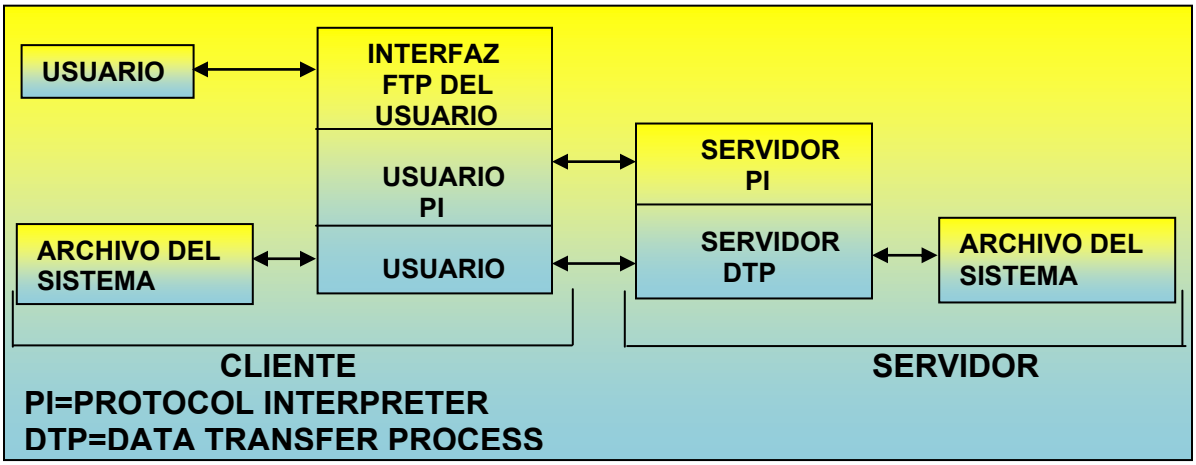


Figura 281 Principios de FTP

6.5.16.2 OPERACIONES DE FTP

Al usar FTP, el usuario realizará alguna de las siguientes operaciones:

- Conexión a un host remoto
- Selección de un directorio
- Listado de ficheros disponibles para una transferencia
- Especificación del modo de transferencia
- Copiar ficheros del/el host remoto
- Desconectar del host remoto

6.5.16.2.1 CONEXIÓN A UN HOST REMOTO

Para ejecutar una transferencia de ficheros, el usuario comienza haciendo un login en el host remoto. Este es el método primario para manejar la seguridad. El usuario debe tener un identificador y un password para el host remoto, a menos que use un FTP anónimo, descrito en FTP anónimo. Se usan tres comandos:

- Open Selecciona el host remoto de inicia la sesión con el login
- User Identifica al ID del usuario remoto
- Pass Autentifica al usuario
- Site Envía información al host remoto utilizado para proporcionar servicios específicos para ese host

6.5.16.2.2 SELECCIÓN DE UN DIRECTORIO

Cuando se establece el enlace de control, el usuario puede emplear el subcomando **CD (change directory)** para seleccionar un directorio remoto de trabajo. Obviamente, el usuario sólo podrá acceder a directorios a los que su ID le da acceso. El usuario puede seleccionar un directorio local con el comando **LCD (local change directory)**. La sintaxis de estos comandos depende del sistema operativo.

6.5.16.2.3 LISTADOS DE FICHEROS DISPONIBLES PARA UNA TRANSFERENCIA

Se hace con los subcomandos **dir** o **ls.**.

6.5.16.2.4 ESPECIFICACION DEL MODO DE TRANSFERENCIA

La transferencia de datos entre sistemas diferentes suele requerir transformaciones de los datos como parte del proceso de transferencia. El usuario ha de decidir dos aspectos de la manipulación de los datos:

- La forma en qué se transferirán los bits.
- Las distintas representaciones de los datos en la arquitectura del sistema.

Esto se controla por medio de dos subcomandos:

- **Mode**.-Especifica si el fichero se ha de tratar como si tuviera estructura de registros o como un flujo de bytes.
- **Block**.-Se respetan las separaciones lógicas entre registros.
- **Stream**.-El fichero se trata como un flujo de bytes. Esta es la opción por defecto, y proporciona una transferencia más eficiente, pero puede que no produzca los resultados deseados cuando se trabaja con ficheros estructurados por registros.
- **Type**.-Especifica el conjunto de caracteres usado para los datos.
- **ASCII**.-Indica que ambos host están basados en ASCII, o que si uno está basado en ASCII y el otro en EBCDIC, se debería realizar una traducción ASCII-EBCDIC.
- **EBCDIC**.-Indica que ambos host se basan en EBCDIC.
- **Image**.-Indica que los datos deben tratarse como bits contiguos empaquetados en bytes de 8 bits.

Debido a que estos subcomandos no cubren todas las posibles diferencias entre sistemas, el subcomando **SITE** está disponible para lanzar comandos dependientes del sistema.

6.5.16.2.5 COPIA DE FICHEROS

Get.-Copia un fichero del host remoto al host local.
Put.-Copia un fichero del host local al host remoto.

6.5.16.2.6 FINALIZACIÓN DE LA SESIÓN DE TRANSFERENCIA

Quit.-Desconecta del host remoto y cierra el FTP. Algunas implementaciones usan el subcomando BYE.
Close.-Desconecta del host remoto pero deja al cliente FTP ejecutándose. Se puede lanzar un comando open para trabajar con otro host remoto.

6.5.16.3 CÓDIGOS DE RESPUESTA

Con el fin de gestionar estas operaciones, el cliente y el servidor mantienen un diálogo por medio de TELNET. El cliente lanza comandos, y el servidor contesta con **códigos de respuesta**. Las respuestas incluyen también comentarios para el usuario, pero el cliente usa sólo los códigos.
Los códigos de respuesta tienen tres dígitos, siendo el primero el más significante.

Código de Respuesta	Descripción
1xx	Contestación Preeliminar Positiva
2xx	Contestación de Terminación Positiva
3xx	Contestación Intermedia Positiva
4xx	Contestación de Terminación Transitoria Negativa
5xx	Contestación de Terminación Permanente Negativa

Tabla 34 Códigos de respuesta de FTP - Los dígitos primero y segundo proporcionan más detalles de la respuesta.

Ejemplo
Para comando de usuario, mostrado **así**, el servidor FTP responde con un mensaje que comienza con un código de 3 dígitos, mostrado así:
FTP foreignhost
220 service ready
USERNAME cms01
331 user name okay
PASSWORD xyxyx
230 user logged in
TYPE Image
200 command okay

6.5.16.4. EJEMPLO DE UNA SESION

[C:\SAMPLES]**ftp host01.itsc.raleigh.ibm.com**
Connected to host01.itsc.raleigh.ibm.com.
220 host01 FTP server (Version 4.1 Sat Nov 23 12:52:09 CST 1991) ready.
Name (rs60002): **cms01**
331 Password required for cms01.
Password: **xxxxxx**
230 User cms01 logged in.

ftp> **put file01.tst file01.tst**
200 PORT command successful.
150 Opening data connection for file01.tst (1252 bytes).
226 Transfer complete.
local: file01.tst remote: file01.tst
1285 bytes received in 0.062 seconds (20 Kbytes/s)
ftp> **close**
221 Goodbye.
ftp> **quit**

6.5.16.5. FTP ANONIMO

Muchos sitios TCP/IP implementan lo que se conoce como **FTP anónimo**, lo que significa que permiten el acceso público a los ficheros de algunos directorios. El usuario remoto sólo tiene que usar el ID **anonymous** y el password **guest** o alguna otra convención de password, por ejemplo el identificador de usuario para el E-mail. La convención que usa cada sistema se le explica al usuario durante el proceso de login.

6.5.17 SMTP (SIMPLE MAIL TRANSFER PROTOCOL)

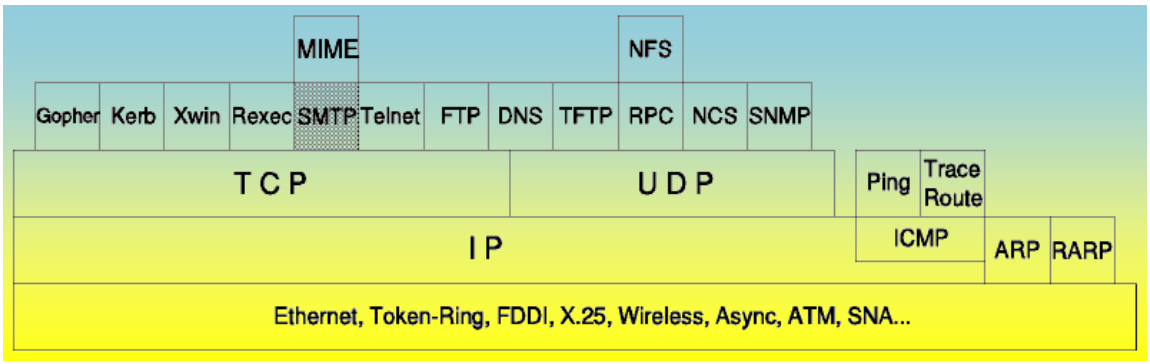


Figura 282 SMTP (Simple Mail Transfer Protocol)

El correo electrónico (e-mail) es probablemente la aplicación TCP/IP más usada. Los protocolos de correo básicos de correo proporcionan intercambio de correo y mensajes entre hosts TCP/IP hosts; se han añadido servicios para la transmisión de datos que no se pueden representar con texto ASCII de 7 bits. Hay tres **protocolos estándares** que se aplican a este tipo de correo. El término SMTP se emplea con frecuencia para referirse a la combinación de los tres protocolos, por su estrecha interrelación, pero estrictamente hablando, SMTP es sólo uno de los tres. Normalmente, el contexto hace evidente de cual de los tres se está hablando. Cuando haya ambigüedad, se emplearán los números STD o RFC. Los tres estándares son:

- Un estándar para el intercambio de correo entre dos estacione (STD 10/RFC 821), que especifica el protocolo usado para enviar correo entre hosts TCP/IP. Este estándar es SMTP.
- Un estándar (STD 11) para el formato de los mensajes de correo, contenido en dos RFC's. El RFC 822 describe la sintaxis de las cabeceras y su interpretación. El RFC 1049 describe como un conjunto de documentos de tipos diferentes del texto ASCII plano se pueden usar en el cuerpo del correo (los mismos documentos están en ASCII de 7 bits con información de formato embebida: PostScript, Scribe, SGML, TEX, TROFF y DVI aparecen en el estándar). El nombre oficial del protocolo para este estándar es MAIL.
- Un estándar para el encaminamiento de correo usando el DNS, descrito en el RFC 974. El nombre oficial del protocolo para este estándar es DNS-MX.

El STD 10/RFC 821 establece que los datos enviados por SMTP son ASCII de 7-bis, con el bit de orden superior a cero. Esto es adecuado para mensajes en inglés, pero no para otros lenguajes o datos que no sean texto. Hay dos estrategias para superar estas limitaciones:

- **MIME (Multipurpose Internet Mail Extensions)**, definido en los RFC's 1521 y 1522, que especifica un mecanismo para codificar texto y datos binarios en ASCII de 7 bits en el mensaje RFC 822. MIME
- **SMTP-SE (SMTP Service Extensions)**, que define un mecanismo para extender las posibilidades de SMTP más allá de las limitaciones impuestas por RFC 821. Actualmente hay tres RFC's que lo describen:
  Un estándar para que un receptor SMTP informe al emisor que extensiones de servicio soporta (SMTP-SE) soporta (RFC 1651).
  El RFC 1651 modifica el 821 para permitir que un cliente agente SMTP solicite al servidor una lista de las extensiones de servicio que soporta el inicio de una sesión SMTP. Si el servidor no soporta este RFC, responderá con un error y el cliente podrá terminar la sesión o intentar iniciar una sesión según las reglas RFC 821. Si sí lo soporta, puede responder con una lista de las extensiones que soporta. IANA mantiene un registro de servicios: la lista inicial del RFC 1651 contiene los comandos listados en el RFC 1123 - Requerimientos para hosts de Internet - Aplicación y soporte como opcionales en servidores SMTP. Se han definido otras extensiones con RFC's del modo habitual. Los dos siguientes RFC's definen extensiones específicas:
  Un protocolo para transmisión de texto de 8 bits (RFC 1652) que permite a un servidor SMTP indicar que puede aceptar datos formados por bytes de 8 bits. Un servidor que informa que dispone de esta extensión no debe modificar el bit de orden superior de los bytes recibidos en un mensaje SMTP si el cliente así se lo pide.
  Las extensiones de MIME y SMTP son estrategias que se complementan más que competir entre sí. En particular, el RFC 1652 se titula SMTPSE para transporte MIME en codificación 8 bit, ya que MIME permite declarar mensajes con bytes de 8 bits, en vez de 7. Tales mensajes no se pueden transmitir con agentes SMTP que sigan estrictamente el RFC 821, pero se pueden transmitir cuando tanto el cliente como el servidor siguen los RFC's 1651 y 1652. Siempre que un cliente intenta enviar datos de 8 bits a un servidor que no soporta esta extensión, el cliente SMTP debe codificar el mensaje a 7 bits según el estándar MIME o devolver un mensaje de error permanente al usuario.

Esta extensión no permite el envío de datos binarios arbitrarios porque el RFC 821 fija la longitud máxima de las líneas aceptadas por un servidor SMTP a 1000 caracteres. Los datos que no son texto pueden tener con facilidad secuencias de más de 1000 caracteres sin una secuencia <CRLF>.

Nota: Las extensiones limitan específicamente el uso de caracteres no ASCII (aquellos con valor decimal superior a 127) al cuerpo de los mensajes **no** están permitidos en las cabeceras RFC 822.
Un protocolo para la declaración del tamaño del mensaje (RFC 1653) que permite a un servidor informar al cliente del tamaño máximo de mensaje que puede aceptar. Sin esta extensión, un cliente sólo puede ser informado de que un mensaje ha excedido el tamaño máximo (sea fijo o temporal, por falta de espacio en el servidor) tras transmitir todo el mensaje. Cuando esto sucede, el servidor desecha el mensaje. Con ella, el cliente puede declarar el tamaño estimado del mensaje y el servidor devolverá un error si es demasiado grande.

6.5.17.1 FUNCIONAMIENTO DE SMTP

SMTP está basado en la **entrega punto-a-punto**; un cliente SMTP contactará con el servidor SMTP del host de destino directamente para entregar el correo. Guardará el correo hasta que se haya copiado con éxito en el receptor. Esto difiere del principio de retransmisión común a muchos sistemas de correo en las que el correo atraviesa un número de host intermedios de la misma red y donde una transmisión con éxito implica sólo que el correo ha alcanzado el host correspondiente al siguiente salto. En varias implementaciones, existe la posibilidad de intercambiar correo entre los sistemas de correo locales y SMTP. Estas aplicaciones se denominan **gateway o puentes de correo**. Enviar correo a través de una pasarela puede alterar la entrega punto-a-punto, ya que SMTP sólo garantiza la entrega fiable al gateway, no al host de destino, más allá de la red local. La transmisión punto SMTP en estos casos es host-gateway, gateway-host o gateway-gateway; SMTP no define lo que ocurre más allá del gateway. CSNET proporciona un interesante ejemplo de servicio de gateway de correo. Diseñada en principio como un servicio barato para interconectar

centros científicos y de investigación, CSNET opera un gateway que permite a sus suscriptores enviar y recibir correo en Internet con sólo un módem con dial. El gateway sondea a los suscriptores a intervalos regulares, les entrega su correo y recoge el correo de salida. A pesar de no ser una entrega punto-a-punto, ha demostrado ser un sistema muy útil. Cada mensaje tiene:
Una cabecera, o sobre, con estructura RFC 822. La cabecera termina con una línea nula (una línea con sólo la secuencia <CRLF>).
Contents: Todo lo que hay tras la línea nula es el cuerpo del mensaje, una secuencia de líneas con caracteres ASCII (aquellos con valor menor del 128 decimal).
El RFC 821 define un protocolo cliente/servidor. Como siempre, el cliente SMTP es el que inicia la sesión (el emisor) y el servidor el que responde a la solicitud de sesión (el receptor). Sin embargo, como el cliente suele actuar como servidor para un programa de correo del usuario, es más sencillo referirse a él como emisor SMTP, y al servidor como receptor SMTP.

6.5.17.1.1 FORMATO DE LA CABECERA

Normalmente, el usuario no tiene por que preocuparse de la cabecera, que es responsabilidad de SMTP. El RFC 822 contiene un análisis completo de la cabecera. La sintaxis es **BNF (Backus-Naur Form)** extendida. El RFC 822 contiene una descripción de BNF, y muchos RFC's relacionados usan el mismo formato. Además describe como convertir una cabecera a su **forma canónica**, uniendo las líneas de continuación, los espacios no significativos, los comentarios, etc. Es una sintaxis poderosa, pero relativamente difícil de analizar. Aquí se incluye una breve descripción. Brevemente, la cabecera es una lista de líneas de la forma:
field-name: field-value
Los campos comienzan en la columna 1: las líneas que comienzan con caracteres en blanco (SPACE o TAB) son líneas de continuación que se unen para crear una sola línea para cada campo en la forma canónica. Las cadenas entre comillas ASCII señalan que los caracteres especiales que limitan no son significativos sintácticamente. Muchos valores importantes (como los de los campos **To** y **From**) son buzones. Las formas más corrientes para estos son:
octopus@garden.under.the.sea
The Octopus <octopus@garden.under.the.sea>
"The Octopus" <octopus@garden.under.the.sea>
La cadena "The Octopus" ha de ser leída por receptores humanos y es el nombre del propietario del buzón. "octopus@garden.under.the.sea" es la dirección para la máquina del buzón (el > y el < delimitan la dirección pero no forman parte de ella). Se ve que esta forma de direccionamiento está relacionada con DNS. De hecho, el cliente SMTP utiliza el DNS para determinar la dirección de destino del buzón.
Algunos campos habituales son:
Keyword.-valor
to.-Receptores primarios del mensaje.
cc.-Receptores Secundario (carbon-copy) del mensaje.
from Identidad del emisor.
reply-to.-El buzón al que se han de enviar las repuestas. Este campo lo añade el emisor.
return-path.-Dirección y ruta hasta el emisor. Lo añade el sistema de transporte final que entrega el correo.
Subject.-Resumen del mensaje. Suele proporcionarlo el usuario.

6.5.17.1.2 INTERCAMBIO DE CORREO

El diseño de SMTP se basa en el modelo de comunicación mostrado en la figura 283 Modelo para SMTP. Como resultado de la solicitud de correo de un usuario, el emisor SMTP establece una conexión en los dos sentidos con el receptor SMTP. El receptor puede ser el destinatario final o un intermediario (gateway de correo). El emisor generará comandos a los que replicará el receptor.

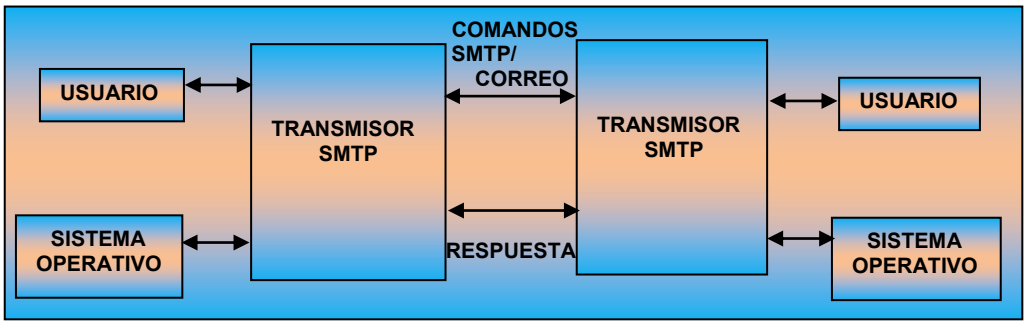


Figura 283 Modelo para SMTP

Flujo de transacción de correo de SMTP:
Aunque los comandos y réplicas de correo están definidas rígidamente, el intercambio se puede seguir en la figura 284 Flujo de datos normal de SMTP. Todos los comandos, réplicas o datos intercambiados son líneas de texto, delimitadas por un <CRLF>. Todas las réplicas tienen un código numérico el comienzo de la línea. El emisor SMTP establece una conexión TCP con el SMTP de destino y espera a que el servidor envíe un mensaje **220 Service ready** o **421 Service not available** cuando el destinatario es temporalmente incapaz de responder. Se envía un HELO (abreviatura de hello), con el que el receptor se identificará devolviendo su nombre de dominio. El SMTP emisor puede usarlo para verificar si contactó con el SMTP de destino correcto. Si el emisor SMTP soporta las extensiones de SMTP definidas en el RFC 1651, puede sustituir el comando HELO por EHLO. Un receptor SMTP que no soporte las extensiones responderá con un mensaje **500 Syntax error, command unrecognized**. El emisor SMTP debería intentarlo de nuevo con HELO, o si no puede retransmitir el mensaje sin extensiones, enviar un mensaje QUIT.
Si un receptor SMTP soporta las extensiones de servicio, responde con un mensaje multi-línea **250 OK** que incluye una lista de las extensiones de servicio que soporta. El emisor inicia ahora una transacción enviando el comando MAIL al servidor. Este comando contiene la ruta de vuelta al emisor que se puede emplear para informar de errores. Nótese que una ruta puede ser más que el par **buzón@nombre de dominio del host**. Además, puede contener una lista de los hosts de encaminamiento. Si se acepta, el receptor replica con un 250 OK.

El segundo paso del intercambio real de correo consiste en darle al servidor SMTP el destino del mensaje (puede haber más de un receptor). Esto se hace enviando uno o más comandos RCPT TO:<forward-path>. Cada uno de ellos recibirá una respuesta 250 OK si el servidor conoce el destino, o un **550 No such user here** si no. Cuando se envían todos los comandos rcpt, el emisor envía un comando **DATA** para notificar al receptor que a continuación se envían los contenidos del mensaje. El servidor replica con **354 Start mail input, end with <CRLF>.<CRLF>**. Nótese que se trata de la secuencia de terminación que el emisor debería usar para terminar los datos del mensaje. El cliente envía los datos línea a línea, acabando con la línea <CRLF>. <CRLF> que el servidor reconoce con 250 OK o el mensaje de error apropiado si cualquier cosa fue mal. Ahora hay varias acciones posibles:

- El emisor no tiene más mensajes que enviar; cerrará la conexión con un comando QUIT, que será respondido con **221 Service closing transmission channel**.
- El emisor no tiene más mensajes que enviar, pero está preparado para recibir mensajes (si los hay) del otro extremo. Mandará el comando **TURN**. Los dos SMTP's intercambian sus papeles y el emisor que era antes receptor puede enviar ahora mensajes empezando por el paso 3 de arriba.
- El emisor tiene otro mensaje que enviar, y simplemente vuelve al paso 3 para enviar un nuevo MAIL.

Figura 284 Flujo de datos normal de SMTP - Se entrega un correo al buzón de destino.

La dirección de destino SMTP (dirección de buzón), en su forma general, **parte-localt@nombre de dominio**, puede adoptar distintos esquemas:
usuario@host.-Para un destino directo en la misma red TCP/IP.
usuario%host.remoto@host-gateway.-Para un usuario en un host remoto de destino no SMTP, vía un gateway.
@host-a, @host-b:usuario@host-c.-Para un mensaje **retransmitido**. Contiene explícitamente información de encaminamiento. El mensaje será entregado primero al host a, que lo retransmitirá al host b. El host b enviará el mensaje al host de destino real, el c. Nótese que el mensaje se almacena en cada uno de los host intermedios, por lo que no se necesita un mecanismo de entrega punto-a-punto.

En la descripción anterior, sólo los comandos más importantes se han mencionado. Todos ellos son comandos que deben estar reconocidos en cualquier implementación SMTP. Existen otros comandos, pero la mayoría son opcionales, es decir, el RFC no los requiere. Sin embargo, implementan funciones muy interesantes tales como retransmisión, correo, listas, etc. Ejemplo:
En el siguiente escenario, el usuario abc en el host vm1.stockholm.ibm.comando envía una nota a los usuarios xyz, opq u rst en el host delta.aus.edu. Las líneas precedidas por R: son las enviadas por el receptor, las que empiezan por S: las enviadas por el emisor.
R: 220 delta.aus.edu Simple Mail Transfer Service Ready
S: HELO stockholm.ibm.comando
R: 250 delta.aus.edu
S: MAIL FROM:<abc@stockholm.ibm.comando>
R: 250 OK
S: RCPT TO:<xyz@delta.aus.edu>
R: 250 OK
S: RCPT TO:<opq@delta.aus.edu>
R: 550 No such user here
S: RCPT TO:<rst@delta.aus.edu>
R: 250 OK
S: DATA
R: 354 Start mail input, end with <CRLF>.<CRLF>
S: Date: 23 Jan 89 18:05:23
S: From: Alex B. Carver <abc@stockholm.ibm.comando>

S: Subject: Important meeting
S: To: <xyz@delta.aus.edu>
S: To: <opq@delta.aus.edu>
S: cc: <rst@delta.aus.edu>
S:
S: Blah blah blah
S: etc.....
S:
R: 250 OK
S: QUIT
R: 221 delta.aus.edu Service closing transmission channel
Nótese que la cabecera del mensaje es parte de los datos a transmitir.

6.5.17.2 SMTP Y EL DNS

Si la red usa el concepto de dominio, un SMTP no puede entregar simplemente correo a TEST.IBM.comando abriendo una conexión TCP con TEST.IBM.comando. Primero debe consultar al servidor de nombres para hallar a que host (en un nombre de dominio) debería entregar el mensaje. Para la entrega de mensajes, el servidor de nombres almacena los **RR's (Resource Records)** denominados MX RR's. Mapean un nombre de dominio a dos valores:

- Un valor de preferencia.-Como pueden existir múltiples RR's MX para el mismo nombre de dominio, se les asigna una prioridad. El valor de prioridad más bajo corresponde al registro de mayor preferencia. Esto es útil siempre que el host de mayor preferencia sea inalcanzable; el emisor SMTP intenta conectar con el siguiente host en orden de prioridad.
- Un nombre de host.-También es posible que el servidor de nombres responda con una lista vacía de RR's MX. Esto significa que el nombre de dominio se halla bajo la autoridad del servidor, pero no tiene ningún MX asignado. En este caso, el emisor SMTP puede intentar establecer la conexión con el mismo nombre del host.

El RFC 974 da una recomendación importante. Recomienda que tras obtener los registros MX, el emisor SMTP debería consultar los registros **WKS (Well-Known Services)** del host, y chequear que el host referenciado tiene como entrada WKS a SMTP.
Nota: Esto es sólo una opción del protocolo, aunque aparece en numerosas implementaciones.
Aquí hay un ejemplo de RR's MX:

```
fsc5.stn.mlv.fr.  IN    MX 0  fsc5.stn.mlv.fr.
                  IN    MX 2  psfred.stn.mlv.fr.
                  IN    MX 4  mvs.stn.mlv.fr.
                  IN    WKS   152.9.250.150 TCP (SMTP)
```

En el ejemplo anterior, el correo para fsc5.stn.mlv.fr debería, por prioridad, ser entregado al propio host, pero en caso de que el host sea inalcanzable, el correo también podría ser entregado a psfred.stn.mlv.fr o a mvs.stn.mlv.fr (si psfred.stn.mlv.fr no se pudiera alcanzar tampoco).

6.5.17.3 SERVIDORES DE CORREO POP (Post Office Protocol)

Debido a que un receptor de correo SMTP es un servidor, y SMTP es una aplicación punto-a-punto más que de retransmisión, es necesario que el servidor esté disponible cuando un cliente desea enviarle correo. Si el servidor SMTP reside en una estación de trabajo o en una PC, ese host debe estar ejecutando el cuando el cliente quiera transmitir. Esto no suele ser un problema en sistemas multiusuario porque están disponibles la mayor parte del tiempo. En sistemas monousuario, sin embargo, este no es el caso, y se requiere un método para asegurar que el usuario tiene un buzón disponible en otro servidor. Hay varias razones por las que es deseable descargar a la estación de trabajo de las funciones del servidor de correo, entre ellas la falta de recursos en estaciones de trabajo pequeñas, la falta o encarecimiento de la conectividad TCP, etc. La estrategia más simple es, por supuesto, usar un sistema multiusuario para las funciones de correo, pero esto no suele ser deseable quizá el usuario no lo va a usar para nada más, o quiere tener acceso a Alternativamente, el usuario final puede ejecutar un cliente que comunique con un

programa servidor en un host. Este servidor actúa tanto como emisor como receptor. Recibe y envía el correo del usuario. Un método intermedio es descargar la función de servidor SMTP de la estación de trabajo del usuario final, pero no la función de cliente. Es decir, el usuario envía correo directamente desde la estación, pero tiene un buzón en un servidor. El usuario debe conectar con el servidor para recoger su correo. El POP describe como un programa que se ejecuta en una estación de trabajo final puede recibir correo almacenado en sistema servidor de correo. POP usa el término **maildrop** para referirse a un buzón gestionado por un servidor POP.

6.5.17.3.1 DIRECCIONANDO BUZONES EN SERVIDORES

Cuando un usuario emplea un servidor para las funciones de correo, la dirección del buzón que ven otros usuarios SMTP se refiere exclusivamente al servidor. Por ejemplo, si dos sistemas se llaman:
hayes.itso.ral.ibm.comando e
itso180.itso.ral.ibm.comando
usándose el primero como cliente y el segundo como servidor, la dirección de correo podría ser:
hayes@itso180.itso.ral.ibm.comando
Esta dirección de buzón aparecería en el campo **From**: de la cabecera de todo el correo saliente y en los comandos SMTP a servidores remotos lanzados por el servidor. Sin embargo, cuando el usuarios emplea un servidor POP, la dirección de correo contiene el nombre de host de la estación de trabajo (por ejemplo steve@hayes.itso.ral.ibm.comando). En este caso, el emisor debería incluir un campo **Reply-To**: en la cabecera para indicar que las réplicas **no** se deberían enviar al emisor. Por ejemplo, la cabecera podría tener este aspecto:

```
Date: Fri, 10 Feb 95 15:38:23
From: steve@hayes.itso.ral.ibm.comando
To: "Steve Hayes" <tsgsh@gford1.warwick.uk.ibm.comando>
Reply-To: hayes@itso180.itso.ral.ibm.comando
Subject: Test Reply-To: header field
```

Se espera que el agente de correo envíe las respuestas a la dirección Reply-To: y no a From: Usando DNS para dirigir correo Una alternativa al uso del campo Reply-To: es usar el DNS para dirigir el correo al buzón correcto. El administrador del DNS con autoridad para el dominio que contiene la estación del usuario y el servidor de nombres pueden añadir registros MX al DNS para dirigir el correo, tal como se describe en SMTP y el DNS. Por ejemplo, los siguientes registros MX indican a los clientes SMTP que, si el servidor SMTP en hayes.itso.ral.ibm.comando no está disponible, hay un servidor de correo en itso.180.ral.ibm.comando (9.24.104.180) que se debería usar en su lugar.

```
itso180.itso.ral.ibm.comando.  IN    WKS  9.24.104.180 TCP (SMTP)
hayes.itso.ral.ibm.comando.    IN    MX 0 hayes.itso.ral.ibm.comando.
                               IN    MX 1 itso180.itso.ral.ibm.comando.
```

6.5.17.3.2 GATEWAYS SMTP

Un gateway SMTP es un host con dos conexiones a redes distintas. Los gateways SMTP se pueden implementar de forma que conecten distintos tipos de redes. Un gateway SMTP-RSCS/NJE se configura utilizando un fichero de configuración SMTP como el que se muestra en la figura 285. Para configurar un host que no es gateway, no se debe especificar la sentencia GATEWAY.

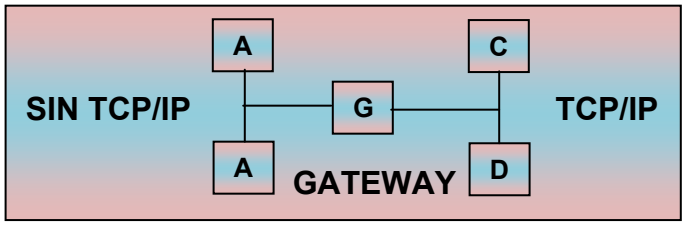


Figura 285 SMTP-RSCS/NJE Mail Gateway

```
GATEWAY                 accept mail from and deliver mail to RSCS host
RSCSDOMAIN RSCSNET      pseudo domain name of associated RSCS network
```

LOCALFORMAT NETDATA	local recipients receive mail in Netdata format
RSCSFORMAT NETDATA	RSCS recipients receive mail in Netdata format
REWRITE822HEADER NO	Only set to no if you do not want SMTP to rewrite the 822 headers on all mail passing from RSCS to TCP through gateway.

Se puede prohibir el acceso al gateway a determinados nodos de la red, empleando la sentencia de configuración RESTRICT.Alternativamente, la seguridad se puede implementar con un fichero de autorización de accesos, que es una tabla en la que se especifican de quién y a quién se puede enviar correo por el gateway. La tabla 35 es un ejemplo de este tipo de archivo:

DEBULOI	MLVFSC0			
DEBULOIS	MLVFSC1	FRED0	Y	N
DEBULOIS	MLVFSC5	FRED1	N	Y
TCPMAINT	MLVFSC5	TCP0	N	N
DEBULOIS	MLVFSC1	TCP1	Y	Y

Tabla 35

Los sistemas IBM VM y VMS están preparados para funcionar como gateways de correo seguros. Así mismo, OS/400 se puede configurar para que funcione como gateway SMTP

6.5.18 SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)

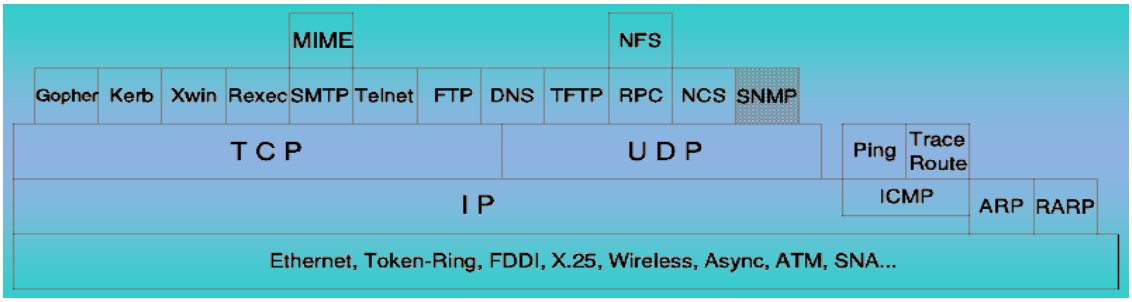


Figura 286 Gestión de red

Con el crecimiento en tamaño y complejidad de las redes basadas en TCP/IP, la necesidad de mecanismos de gestión de red se ha vuelto muy importante. En la actualidad, los protocolos que forman el soporte de la gestión de red son:

- **SMI (Structure and Identification of Management Information**, RFC 1155).-Describe como se definen los objetos gestionados contenidos en el MIB.
- **MIB-II (Management Information Base**, RFC 1213).-Describe los objetos gestionados contenidos en el MIB.
- **SNMP (Simple Network Management Protocol**, RFC 1098).-Define el protocolo usado para gestionar estos objetos.
- **El IAB (Internet Architecture Board)**.-Emitió un RFC al respecto, en el que adoptaba dos actitudes diferentes:
  A corto plazo, se recomienda el uso de SNMP.
  El IAB recomienda que todas las implementaciones de IP y TCP sean gestionables. Actualmente, esto implica la implementación de MIB-II, y de al menos el protocolo recomendado de gestión SNMP (RFC 1157).
  Notar que los protocolos históricos SGMP (Simple Gateway Monitoring Protocol, RFC 1028) y MIB-I (RFC-1156) no están recomendados.

A largo plazo, se debería investigar el uso del incipiente protocolo de gestión de red de OSI (**CMIP Common Management Information Protocol**). Es lo que se conoce como **CMIP sobre TCP/IP (CMOT Common Management Information Protocol over TCP/IP)**. Tanto SNMP y CMOT utilizan los mismos conceptos básicos en la descripción y definición la información de gestión denominada **SMI (Structure and Identification of Management Information)** descrita en el RFC 1155 y **MIB (Management Information Base)**, descrita en el RFC 1156.

6.5.18.1 SMI (STRUCTURE AND IDENTIFICATION OF MANAGEMENT INFORMATION)

El SMI define las reglas para describir los objetos gestionados y como los protocolos sometidos a la gestión pueden acceder a ellos. La descripción de los objetos gestionados se hace utilizando un subconjunto de **ASN.1 (Abstract Syntax Notation 1, estándar ISO 8824)**, un lenguaje de descripción de datos. La definición del tipo de objeto consta de cinco campos:

- Objeto: nombre textual, llamado **descriptor del objeto**, para el tipo del objeto, junto con su correspondiente **identificador de objeto**.
- Sintaxis: la sintaxis abstracta para el tipo el objeto. Las opciones son Simple Syntax (entero, octeto de caracteres, identificador de objeto, Null), Application Syntax (dirección de red, contador, escala, ticks, opaco) u otro tipo de sintaxis de aplicación
- Definición: descripción textual de la semántica del tipo.
- Acceso: sólo lectura, sólo escritura, lectura - escritura o inaccesible.
- Status: obligatorio, opcional u obsoleto.

Como ejemplo, podemos tener:

OBJET
sysDescr {system 1}
SYNTAX OBTET STRING
Definition This value should incluye the fullname and version Identification of the system`s ardware type, software Operating-system, and networking software. It is Mandatore that thiscotan lyprintable ASCII
Characters.
Access read-only.
Status mandatory.

Este ejemplo muestra la definición de un objeto contenido en el MIB. Su nombre es sysDescr y pertenece al grupo sistema. Un objeto gestionado no sólo ha de ser descrito, también debe ser identificado. Esto se hace utilizando el **identificado de objeto (Object Identifier)** ASN.1 como si fuera un número de teléfono, reservando grupos de números para distintas localizaciones. En el caso de la gestión de red para TCP/IP, el número reservado fue 1.3.6.1.2 y SMI lo usa como base para la definición de nuevos objetos.
Este número se obtiene al unir a grupos de números con el siguiente significado:
El primer grupo define el nodo administrador:
(1) para ISO
(2) para CCITT
(3) para la unión ISO-CCITT.
El segundo grupo para el nodo administrador ISO define (3) para su uso por parte de otras organizaciones.
El tercer grupo define (6) para su uso por parte del DoD (U.S. Department of Defense).
En el cuarto grupo, el DoD no ha indicado como ha de gestionarse se grupo correspondiente por lo que la comunidad de Internet ha asumido (1).
El quinto grupo fue aprobado por el IAB para ser:
(1) para el uso del directorio OSI en Internet
(2) para la identificación de objetos con propósitos de gestión
(3) para la identificación de objetos con fines experimentales
(4) para la identificación de objetos para uso privado
En el ejemplo, {system 1} significa que el identificador del objeto es 1.3.6.1.2.1.1.1. Es el primer objeto en el primer grupo (sistema) en el MIB.

6.5.18.2 MIB (MANAGEMENT INFORMATION BASE)
6.5.18.2.1 DESCRIPCION

El MIB define los objetos que pueden ser gestionados para cada capa en el protocolo TCP/IP. Hay dos versiones, MIB-I y MIB-II. MIB-I fue definida en el RFC 1156, y está clasificado ahora como protocolo **histórico**.

GRUPO	OBJETOS	#
sistema	Sistema básico de información	7
interfaces		23
AT	Dirección de destino	3
IP	Internet Protocol	38
ICMP	Internal Control Message Protocol Statics	26
TCP	Transmission Control Protocol	19
UDP	User Datagram Protocol	7
EGP	Exterior Gateway Protocol	18
Transmiss	Transmisión, media-specific	0
SNMP	SNMP entidades de aplicación	

Tabla 36 Número de objetos en el grupo.

Cada nodo gestionado soporta sólo los grupos apropiados. Por ejemplo, si no hay gateway, el grupo EGP no tiene por que estar incluido. Pero si un grupo es apropiado, todos los objetos en ese grupo deben estar soportados. La lista de objetos gestionados definidos deriva de aquellos elementos considerados esenciales. Este enfoque, consistente en tomar sólo los objetos esenciales no es restrictivo, ya que el SMI proporciona mecanismos de extensibilidad tales como la definición de una nueva versión de MIB o de objetos privados o no estandarizados.
Debajo hay algunos ejemplos de objetos de cada grupo. La lista completa está definida en el RFC 1213.

- Grupo de sistema
  - sysDescr - Descripción completa del sistema (versión, HW, OS)
  - sysObjectID - Identificación que da el distribuidor al objeto
  - sysUpTime - Tiempo desde la última reinicialización
  - sysContact - Nombre de la persona que hace de contacto
  - sysServices - Servicios que ofrece el dispositivo
- Grupo de interfaces
  - ifIndex - Número de interfaz
  - ifDescr - Descripción de la interfaz
  - ifType - Tipo de la interfaz
  - ifMtu - Tamaño máximo del datagrama IP
  - ifAdminisStatus - Status de la interfaz
  - ifLastChange - Tiempo que lleva la interfaz en el estado actual
  - ifINErrors - Número de paquetes recibidos que contenían errores
  - ifOutDiscards - Número de paquetes enviados y desechados
- Grupo de traducción de direcciones
  - atTable - Tabla de traducción de direcciones
  - atEntry - Cada entrada que contiene una correspondencia de dirección de red a dirección física
  - atPhysAddress - La dirección física dependiente del medio
  - atNetAddress - La dirección de red correspondiente a la dirección física
- Grupo IP
  - ipForwarding - Indicación de si la entidad es un gateway IP
  - ipInHdrErrors - Número de datagramas de entrada desechados debido a errores en sus cabeceras IP
  - ipInAddrErrors - Número de datagramas de entrada desechados debido a errores en sus direcciones IP

    - ipInUnknownProtos - Número de datagramas de entrada desechados debido a protocolos desconocidos o no soportados
    - ipReasmOKs - Número de datagramas IP reensamblados con éxito
    - ipRouteMask - Máscara de subred para el encaminamiento
- Grupo ICMP
    - icmpInMsgs - Número de mensajes ICMP recibidos
    - icmpInDestUnreachs - Número de mensajes ICMP destino inalcanzable (destination unreachable) recibidos
    - icmpInTimeExcds - Número de mensajes ICMP time exceded (tiempo excedido) recibidos
    - icmpInSrcQuenchs - Número de mensajes ICMP source quench (desbordamiento del emisor) recibidos
    - icmpOutErrors - Número de mensajes ICMP no enviados debido a problemas en ICMP
- Grupo TCP
    - tcpRtoAlgorithm - Algoritmo que determina el timeout para retransmitir octetos para los que no se ha recibido reconocimiento
    - tcpMaxConn - Límite en el número de conexiones TCP que puede soportar la entidad
    - tcpActiveOpens - Número de veces que las conexiones TCP han efectuado una transición directa del estado SYN-SENT al estado CLOSED
    - tcpInSegs - Número de segmentos recibidos, incluyendo aquellos con error
    - tcpConnRemAddress - La dirección IP remota para esta conexión TCP
    - tcpInErrs - Número de segmentos desechados debido a errores de formato
    - tcpOutRsts - Número de resets generados
- Grupo UDP
    - udpInDatagrams - Número de datagramas UDP entregados a usuarios UDP
    - udpNoPorts - Número de datagramas UDP recibidos para los que no existía aplicación en el puerto de destino
    - udpInErrors - Número de datagramas UDP recibidos que no se pudieron entregar por razones otras que la ausencia de la aplicación en el puerto de destino
    - udpOutDatagrams - Número de datagramas UDP enviados por la entidad
- Grupo EGP
    - egpInMsgs - Número de mensajes EGP recibidos sin error
    - egpInErrors - Número de mensajes EGP con error
    - egpOutMsgs - Número de mensajes EGP generados localmente
    - egpNeighAddr - La dirección IP del vecino de esta entrada EGP
    - egpNeighState - El estado EGP del sistema local con respecto a la entrada EGP vecino

Esta no es la definición completa del MIB pero sirve de ejemplo de los objetos de cada grupo. El grupo de interfaces contiene dos objetos de nivel superior: el número de interfaces del nodo (**ifNumber**) y una tabla con información de estas (**ifTable**). Cada entrada de la tabla (**ifEntry**) contiene los objetos de esa interfaz. Entre ellos, el tipo de interfaz (**ifType**) se identifica en el árbol MIB con notación ASN.1 como 1.3.6.1.2.1.2.2.1.3. Para un adaptador de red en anillo, su valor sería 9 (iso88025-tokenRing), figura 287 Identificador de objeto.

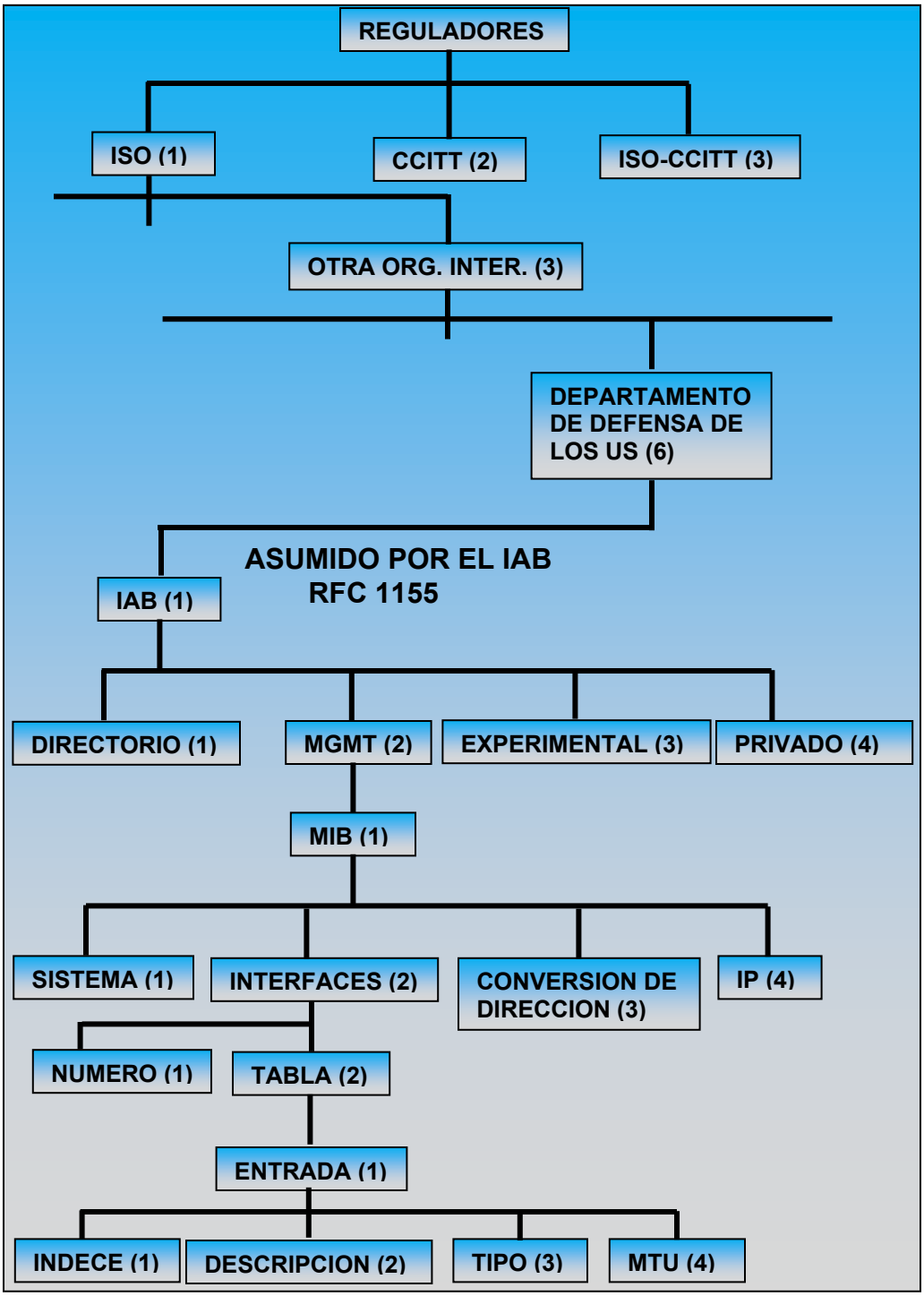


Figura 287 Identificador de objeto - Asignación para redes TCP/IP.

6.5.18.3 SNMP

SNMP añadió las mejoras de muchos años de experiencia con SGMP y le permitió trabajar con los objetos definidos en el MIB con la representación del SIM. El RFC 1157 define **NMS (Network Management Station)** como una estación que ejecuta **aplicaciones de gestión de red (NMA)** que monitorizan y controlan **elementos de red (NE)** como hosts, gateways y servidores de

terminales. Estos elementos usan un **agente de gestión (MA)** para realizar estas funciones. El SNMP para la comunicación de información entre las NMS y los MA.

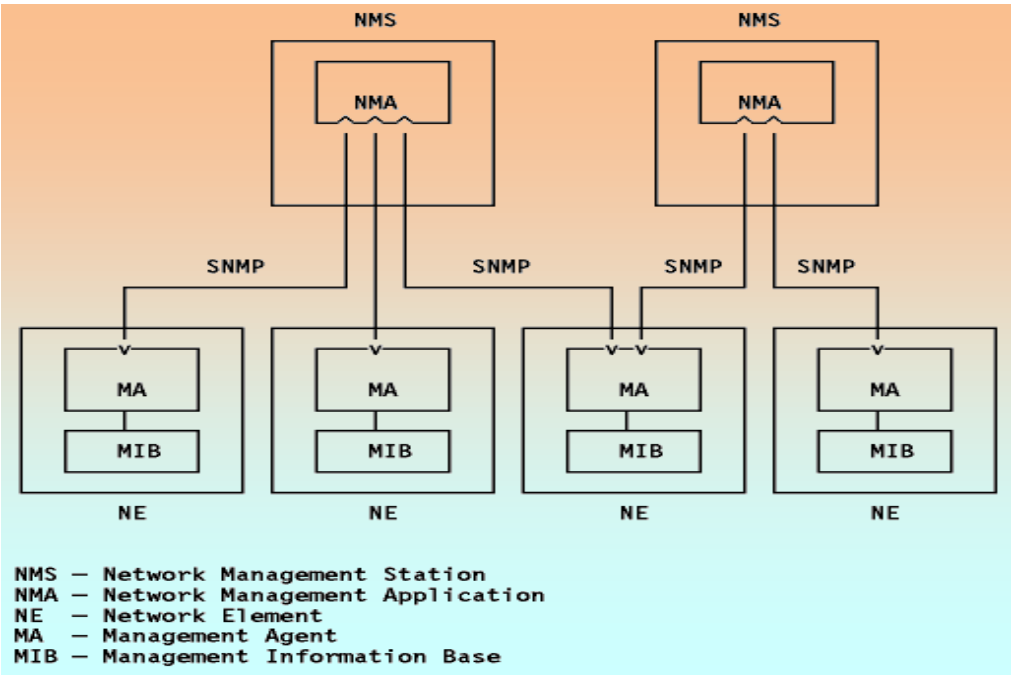


Figura 288 Componentes de SNMP.

Todas las funciones de los MA son sólo alteraciones (set) o consultas (get) de variables, limitando así el número de funciones esenciales a dos y simplificando el protocolo. En la comunicación NE-NMS, se utilizan un número limitado de mensajes no solicitados (traps) para informar de eventos asíncronos. Del mismo modo, en un intento de mantener la sencillez, el intercambio de información requiere sólo un servicio de datagramas y cada mensaje se envía en un único datagrama. Esto significa que SNMP es adecuado para una gran variedad de protocolos de transporte. El RFC 1157 especifica el intercambio de mensajes vía UDP, aunque es posible emplear otros. Las entidades que residen en las NMS y los elementos de red que se comunican con otros a través de SNMP se denominan entidades de aplicación de SNMP. Los procesos que las implementan son las entidades de protocolo. Un agente SNMP con un conjunto arbitrario de entidades es una comunicad SNMP, en la que cada entidad se nombra con una ristra de bytes que debe ser unívoca para esa comunidad. Un mensaje de SNMP consiste en un identificador de la versión, un nombre de la comunidad SNMP y un PDU (Protocol Data Unit). Toda implementación de SNMP debe soportar las cinco PDU's siguientes:

- **Get Request**: Recuperar los valores de un objeto del MIB
- **Get Next Request**: Recorrer parte del MIB
- **Set Request**: Alterar los valores de un objeto del MIB
- **Get Response**: Respuesta de Get Request, Get Next Request y Set Request
- **Trap**: Capacidad de los elementos de red para generar eventos como la inicialización, reinicio o fallo en el enlace del MA. Hay siete tipos de traps definidos en el RFC 1157: cold Start, warm Start, link Down, link Up, authentication Failure, egp Neighbor Loss y enterprise Specific.
  Los formatos de estos mensajes son los siguientes:

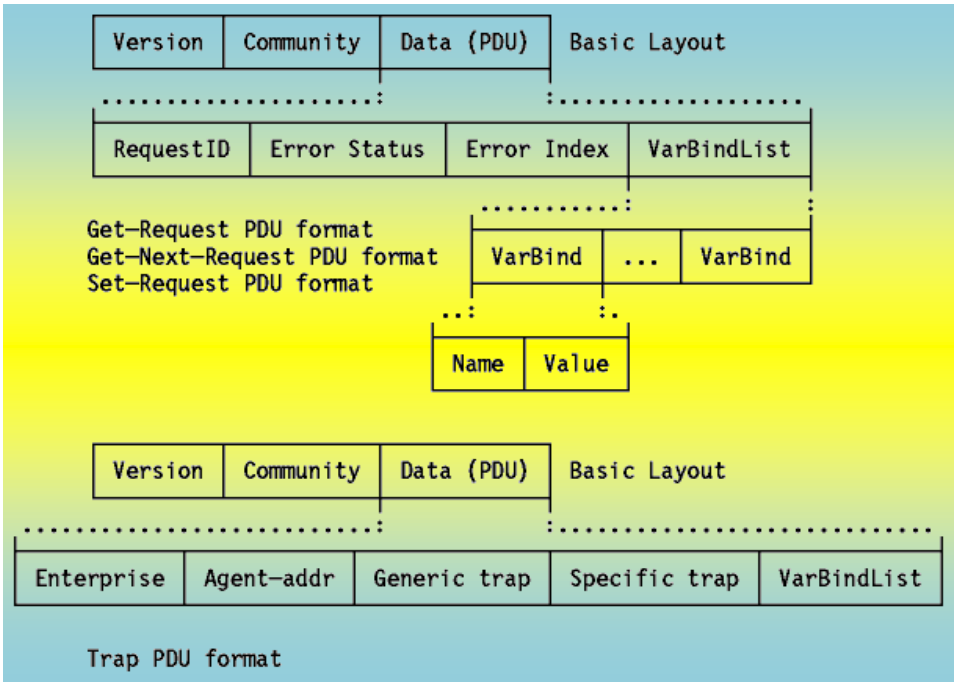


Figura 289 Formato de mensaje SNMP Formato de las PDU Request, Set y Trap.

6.5.18.4 CMOT (COMMON MANAGEMENT INFORMATION PROTOCOL OVER TCP/IP)

CMOT es la arquitectura de gestión de red desarrollada con vistas a mantener una relación más estrecha con el **CMIP (Common Management Information Protocol)** de OSI. Con esta premisa, CMOT se divide, como en OSI, en un modelo organizacional, funcional e informacional. En los dos primeros el mismo concepto de OSI se usa en CMOT y SNMP. La identificación de objetos se efectúa empleando el subárbol relacionado con DoD con subdivisiones en lo que respecta a gestión, directorio, experimental y privado. Todos los objetos de gestión se definen en el MIB (Management Information Base), y se representan con el SMI (Structure and Identification of Management Information), un subconjunto de ASN.1 (Abstract Syntax Notation 1 de OSI).

En el modelo funcional, CMOT adopta el modelo OSI que divide los componentes de gestión en managers y agentes. El agente recoge información, realiza comandos y ejecuta tests, y el manager recibe datos, genera comandos y envía instrucciones a los agentes. El manager y el agente están constituidos por un conjunto específico de entidades de información de gestión por cada capa de comunicación, denominadas **LME (Layer Management Entities)**.

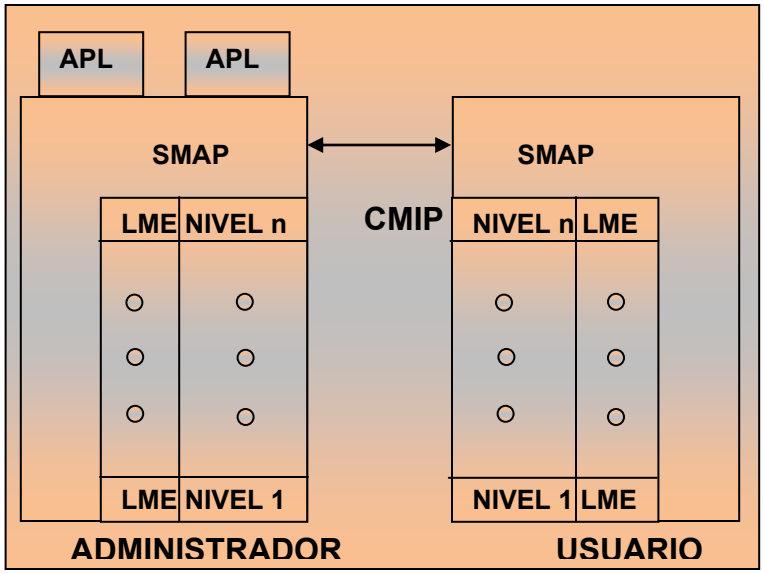


Figura: CMOT 290 Componentes de CMIP sobre TCP/IP.

Todos los LME los coordina el **SMAP (System Management Application Process)** que es capaz de comunicarse entre diferentes sistemas a través de **CMIP (Common Management Information Protocol).** En el mundo OSI, la gestión sólo se puede producir sobre conexiones establecidas por completo entre managers y agentes. CMOT permite el intercambio de información de gestión usando servicios no orientados a conexión (datagramas). Pero para mantener la misma interfaz del servicio que requiere CMIP, llamada **CMIS (Common Management Information Services)**, la arquitectura de CMOT define una nueva capa, el **LPP (Lightweight Presentation Protocol)**. Esta capa se ha definido para proporcionar los servicios de presentación que necesita CMIP de tal forma que la totalidad de los estándares OSI para la gestión de red se adapten a la arquitectura TCP/IP de CMOT.

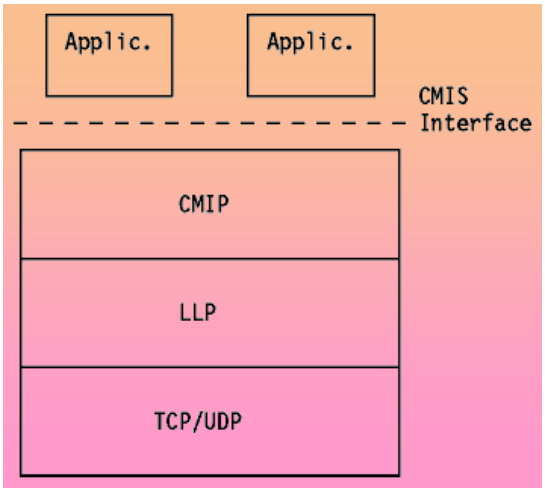


Figura 291 LPP (Lightweight Presentation Protocol)

6.5.18.5 El DPI de SNMP (SNMP DISTRIBUTED PROGRAMMING INTERFACE)

SNMP define un protocolo que permite efectuar operaciones en una serie de variables. Este conjunto de variables (el MIB) y un conjunto básico o núcleo está predefinidas. Sin embargo, el diseño del MIB cuenta con la posibilidad de expandir este núcleo sea expandido. Desafortunadamente, las implementaciones convencionales de agentes SNMP no suministran mecanismos para que el usuario cree nuevas variables. El DPI enfoca esta cuestión proporcionando mecanismos que permiten al usuario añadir, borrar o reemplazar dinámicamente variables en el MIB local sin tener que recompilar el agente SNMP. Esto es posible gracias a un subagente que se comunica con el agente a través del DPI. El RFC 1228 lo describe. El DPI de SNMP habilita a un proceso para registrar la existencia de una variable MIB en el agente SNMP, que pasará la solicitud al subagente. El subagente devuelve a su vez la respuesta apropiada al agente. Este, finalmente, empaqueta una respuesta SNMP y envía la respuesta a la NMS que inició la solicitud. El subagente es completamente invisible (transparente) para la NMS. La comunicación entre el agente SNMP y sus clientes (subagentes) tiene lugar sobre un canal. Típicamente se trata de una conexión TCP, pero se pueden emplear otros protocolos de transporte orientados a conexión. El agente en el DPI puede:

- Crear y borrar subárboles del MIB
- Crear un paquete de solicitud de registro para que el subagente informe al agente SNMP
- Crear un paquete de respuesta para que el subagente responda a la solicitud del agente SNMP
- Crear un paquete de solicitud TRAP

La figura 292 muestra el flujo entre el agente SNMP y el subagente.

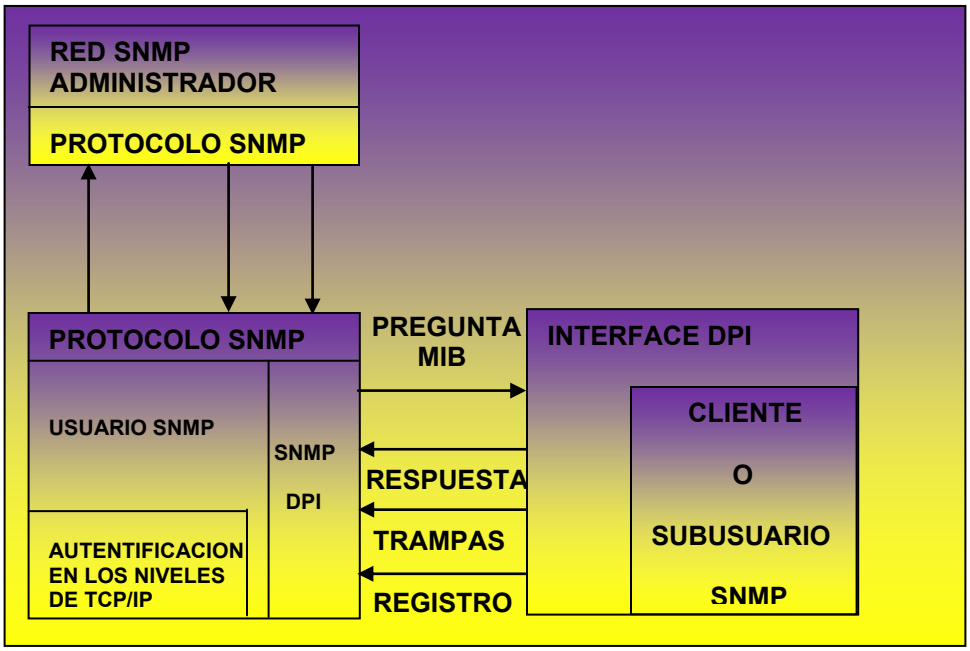


Figura 292 Descripción del DPI de SNMP

El agente SNMP se comunica con el manager por medio de SNMP. La comunicación del agente con las capas TCP/IP y con el núcleo del sistema operativo depende de la implementación. Un subagente SNMP, ejecutando un proceso aparte (que potencialmente puede estar en otra máquina), puede registrar objetos con el agente SNMP (Register). El agente SNMP decodificará los paquetes. Si un paquete contiene una solicitud Get/Get Next o Set para un objeto registrado en el subagente, se la enviará en el correspondiente paquete (MIB query). El subagente SNMP responde con un paquete RESPONSE (Reply). El agente codifica la respuesta en un paquete SNMP y lo envía al manager. Si el subagente desea informar de un cambio de estado importante, envía un Trap al agente que a su vez lo codificará y enviará al manager.

6.5.18.6 SNMPv2 (SNMP VERSION 2)

La infraestructura de la versión 2 de SNMP se publicó en abril de 1993 y consiste en 12 RFC's, incluyendo el primero, el 1441, que es una introducción. Esta infraestructura consta de las siguientes disciplinas:

- SMI (Structure of Management Information).-Definición del subconjunto de ASNN.1 para la creación de módulos MIB. Descripción en el RFC 1442.
- Convenios textuales.-Definición del conjunto inicial de convenios textuales disponible para todos los módulos MIB. Descripción en el RFC 1443.
- Operaciones del protocolo.-Definición de las operaciones del protocolo con respecto a las PDU's enviadas y recibidas en el RFC 1448.
- Mapeados de transporte.-Definición del mapeado de SNMPv2 sobre un conjunto inicial de dominios de transporte ya que se puede utilizar en diferentes pilas de protocolo. El mapeado en UDP es el preferido. El RFC también define OSI, AppleTalk, IPX, etc. Descripción en el RFC 1449.
- Instrumentación del protocolo.-Definición del MIB y del MIB Manager-Manger. Descripción en los RFC's 1450 y 1451.
- Infraestructura administrativa.-Definición de SNMPv2 Party, **SP (Security Protocols)** y Party MIB. Descripción en los RFC's 1445, 1446 y 1447.
- Compatibilidades.-Definición de la **compatibilidad o capacidad** de notación de los agentes. Descripción en el RFC 1444.

6.5.18.6.1 ENTIDAD SNMPv2

Una entidad SNMPv2 es un proceso real que realiza operaciones de gestión de red mediante la generación y/o respuesta a/de mensajes SNMPv2. Todas las posibles operaciones de una entidad se pueden restringir a un subconjunto de las operaciones que puede efectuar el entorno de gestión (SNMPv2 Party o EG). Una entidad SNMPv2 podría pertenecer a múltiples entidades gestoras, y mantiene las siguientes bases de datos locales:
Una base de datos para todos los EG que conoce la entidad, que podrían ser:
Operación local realizada por interacciones con EG o dispositivos remotos
Operación realizada por otras entidades SNMPv2
Otra base de datos que representa todos los recursos de los objetos gestionados que conoce la entidad
Como mínimo, una base de datos que representa una política de control de acceso que define los privilegios de acceso de acuerdo con los EG conocidos. Una entidad SNMPv2 puede actuar como agente o como manager SNMPv2.

6.5.18.6.2 ENTORNO DE GESTION (SNMPv2 Party o EG)

Un entorno de gestión es un entorno de ejecución virtual cuyas operaciones se restringen, por razones de seguridad o de otra índole, a un subconjunto definido administrativamente de todas las operaciones que puede realizar una entidad SNMPv2 particular. Arquitectónicamente, cada EG comprende:

- Una identidad unívoca del entorno
- Una localización lógica de red en la que se ejecuta el EG, caracterizada por un dominio del protocolo de transporte y por información de direccionamiento del nivel de transporte
- Un sólo protocolo de autentificación y parámetros asociados con los que se autentifican el origen y la integridad de los mensajes del protocolo generados por el entorno
- Un sólo protocolo de privacidad y parámetros asociados con los que los mensajes de protocolo que recibe el entorno se protegen de cualquier intrusión

6.5.18.6.3 GETBULKREQUEST

El GetBulkRequest está definido en el RFC 1448 y forma por tanto parte de las operaciones del protocolo. Un mensaje GetBulkRequest se genera y se transmite como una petición de una aplicación SNMPv2. Su fin es solicitar la transferencia de una cantidad de datos potencialmente elevada, incluyendo, sin que ello le condicione, la rapidez y eficiencia en la recuperación de grandes tablas. GetBulkRequest es más eficiente que GetNextRequest en la recuperación de grandes tablas MIB de objetos. Su sintaxis es:

```
GetBulkRequest [non-repeaters = N, max-repetitions = M]
            (RequestedObjectName1,
             RequestedObjectName2,
             RequestedObjectName3)
```

Donde:
RequestedObjectName 1, 2, 3: Identificador MIB del objeto, como sysUpTime, etc. Los objetos están en una lista ordenada léxicamente. Cada identificador de objeto está ligado como mínimo a una variable. Por ejemplo, el identificador **ipNetToMediaPhysAddress** está ligado a una variable para cada dirección IP de la tabla ARP y su contenido es la dirección MAC asociada.

- **N**: Especifica el valor de non-repeaters, lo que significa que se solicita sólo el contenido de la variable inmediata al objeto indicado en la solicitud, para los primeros N objetos nombrados entre paréntesis. Se trata de la misma función que desempeña GetNextRequest.
- **M**: Especifica el valor max-repetitions, lo que significa que se solicita del resto de los objetos (habiéndose solicitado N) el contenido de las M variables inmediatas al objeto indicado en la solicitud. Es similar a un GetNextRequest iterado pero transmitido en una sola solicitud.

Con GetBulkRequest se pueden conseguir los valores de sólo la siguiente variable o de las siguientes M variables con una sola solicitud.
Asumiendo la siguiente tabla ARP en un host que ejecuta un agente NMPv2:

Interface-Number	Network-Address	Physical-Address	Type
1	10.0.0.51	00:00:10:01:23:45	static
1	9.2.3.4	00:00:10:54:32:10	dynamic
2	10.0.0.15	00:00:10:98:76:54	dynamic

Un manager SNMPv2 envía la siguiente respuesta para conseguir sysUpTime y la tabla ARP completa:

```
GetBulkRequest [non-repeaters = 1, max-repetitions = 2]
        (SysUpTime,
         IpNetToMediaPhysAddress,
         IpNetToMediaType)
```

La entidad SNMPv2 que actúa como agente responde con la PDU Response:

```
Response (sysUpTime.0 = "123456"),
    ((ipNetToMediaPhysAddress.1.9.2.3.4 =
                    "000010543210"),
    (ipNetToMediaType.1.9.2.3.4= "dynamic"),
    (ipNetToMediaPhysAddress.1.10.0.0.51=
                     "000010012345"),
    (ipNetToMediaType.1.10.0.0.51=  "static"))
```

La entidad SNMPv2 que hace de manager continúa con:

```
GetBulkRequest [non-repeaters = 1, max-repetitions = 2]
        (SysUpTime,
         ipNetToMediaPhysAddress.1.10.0.0.51,
         ipNetToMediaType.1.10.0.0.51)
```

El agente responde con:

```
Response ((sysUpTime.0 = "123466")
    (ipNetToMediaPhysAddress.2.10.0.0.15 =
                    "000010987654"),
    (ipNetToMediaType.2.10.0.0.15=
                        "dynamic"),
    (ipNetToMediaNetAddress.1.9.2.3.4 =
                        "9.2.3.4"),
    (ipRoutingDiscards.0 =  "2"))
```

Esta respuesta señala el final de la tabla al manager. Con GetNextRequest se hubieran necesitado cuatro solicitudes para conseguir la misma información. Si se hubiera fijado el valor **max-repetition** de GetBulkRequest a tres, en este ejemplo sólo se hubiera necesitado una solicitud.

6.5.18.6.4 INFORM REQUEST

Un mensaje InformRequest se genera y se transmite como una solicitud de una aplicación de una entidad manager SNMPv2 que desea notificar a otra aplicación, que se ejecuta también en un manager SNMPv2, información en el ámbito del MIB (MIB view) para un entorno local a la aplicación que envía el mensaje. El paquete se utiliza para indicar al manager del otro entorno de la información accesible en el emisor. (comunicación manager-manager a través de los límites del entorno). Las dos primeras variables en la lista de asociaciones de variables de un mensaje InformRequest son sysUpTime.0 y snmpEventID.i respectivamente. Les pueden seguir otras variables.

6.5.18.7 EL MIB PARA SNMPv2

Este MIB define los objetos gestionados que determinan el comportamiento de la entidad SNMPv2.
Nota: No es una sustitución del MIB-II.

Las siguientes son algunas definiciones de objetos para hacerse una idea de sus contenidos:

```
SnmpORLastChange OBJECT-TYPE
   SYNTAX        Timestamp
   MAX-ACCESS read-only
   STATUS         current
   DESCRIPTION
         "El valor de sysUpTime en el momento del cambio más reciente en el valor o estado de
          cualquier instancia de snmpORID."
WarmStart NOTIFICATION-TYPE
   STATUS  current
   DESCRIPTION
         "Un trap warmStart significa que la entidad SNMPv2, actuando como agente, se está
           reinicializando a sí misma de tal modo que la configuración no se altere."
```

6.5.18.8 EG DEL MIB (PARTY MIB)

El EG del MIB define los objetos gestionados que se corresponden con las propiedades asociadas a un EG SNMPv2. Un ejemplo de algunos objetos del MIB:

```
partyIdentity OBJECT-TYPE
   SYNTAX          Party
   MAX-ACCESS  not-accessible
   STATUS          current
   DESCRIPTION
         "Un identificador de EG unívoco para un EG de SNMPv2 particular."

partyAuthProtocol OBJECT-TYPE
   SYNTAX      OBJECT IDENTIFIER
   MAX-ACCESS  read-create
   STATUS          current
   DESCRIPTION
         "El protocolo de autentificación por el que se autentifican el origen y la integridad de todos
         los mensajes que genera el EG. El valor noAuth significa que los mensajes no están
         autentificados. Una vez que se crea una instancia de este objeto, su valor no puede ser
         alterado."
```

6.5.18.8.1 MIB MANAGER-MANAGER

La finalidad de este MIB es proporcionar los medios para la coordinación entre múltiples estaciones de gestión. Es decir, los medios por los que las funciones de control y monitorización de la gestión de red se pueden distribuir entre múltiples NMS en una gran red. Específicamente, este MIB suministra mecanismos para que una NMS solicite servicios de gestión de otra. Por tanto, una entidad SNMPv2 puede tener un doble papel; cuando proporciona información de gestión a otro manager, actúa como agente, y cuando pide información, actúa como manager. El MIB manager-manager consta de las tres tablas siguientes:

- Alarmas
- Eventos
- Notificaciones

Cada alarma es una condición específica detectada mediante la monitorización periódica, en un intervalo de muestreo configurable, de los valores de una determinada variable con información de gestión. Un ejemplo de condición de alarma es cuando la variable monitorizada toma un valor fuera de rango. Cada condición de alarma dispara un evento, que puede a su vez desencadenar una o más notificaciones para otras NMS usando el InformRequest.

6.5.18.9 SAPP (SINGLE AUTHENTIFICATION AND PRIVACY PROTOCOL)

El protocolo de autentificación proporciona un mecanismo para que la gestión de SNMPv2 permita identificar que las comunicaciones que genera un entorno se originan efectivamente en ese entorno. El protocolo de autentificación proporciona un mecanismo para que la gestión de SNMPv2 permita proteger las comunicaciones que genera un entorno de cualquier intrusión. Las principales amenazas contra las que el protocolo de seguridad de SNMPv2 aporta protección son:
Modificación de información
Enmascaramiento
Modificación del flujo de mensajes
Intrusión en la información
Los siguientes servicios de seguridad proporcionan medidas contra las anteriores amenazas:

- Integridad de los datos.-La proporciona el algoritmo de condensación de mensajes MD5. Se calcula un resumen o extracto de 128 bits de la porción indicada del mensaje SNMPv2 y se incluye como parte del mensaje enviado al receptor.
- Autentificación del origen de los datos.-A cada mensaje se le añade un prefijo con un valor secreto que comparten el emisor del mensaje y el receptor, antes de calcular el extracto.
- Replay o retardo del mensaje.-En cada mensaje se incluye un sello de tiempo,
- Confidencialidad de los datos.-La proporciona el protocolo simétrico de privacidad que encripta una porción adecuada del mensaje de acuerdo con una llave secreta conocida sólo por el emisor y el receptor. Este protocolo se usa conjuntamente con el algoritmo simétrico de encriptación, en el modo de encadenamiento de cifrado de bloques, que forma parte del **DES (Data Encryption Standard)**. La parte designada del mensaje se encripta y se incluye como parte el mensaje enviado el receptor.

6.5.18.10 EL NUEVO MODELO ADMINISTRATIVO

Uno de los propósitos del modelo administrativo para SNMPv2 es definir como la infraestructura administrativa se aplica para llevar a cabo una administración de red efectiva en diversas configuraciones y entornos. El modelo implica el uso de diferentes identidades en el intercambio de mensajes. De esta forma, representa abandonar el basado en comunidades del SNMPv1 original. Al identificar sin ambigüedad al emisor y al receptor de cada mensaje, esta nueva estrategia mejora el esquema histórico de comunidades ya que permite un diseño del control de acceso a los datos más conveniente así como el empleo de protocolos de seguridad asimétricos (con llave pública) en el futuro, figura 293 Formato de mensaje de SNMPv2 para conocer el nuevo formato de mensaje.

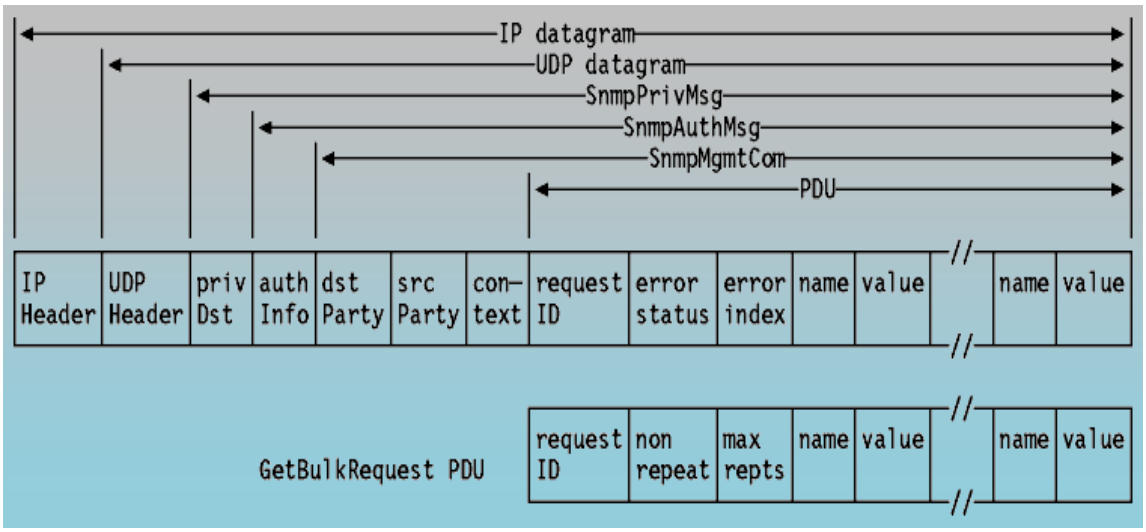


Figura 293: Formato de mensaje de SNMPv2

PDU Incluye una de las siguientes PDU's
GetRequest
GetNextRequest
Response
SetRequest
InformRequest
SNMPv2-Trap
El GetBulkRequest tiene un formato de PDU distinto al mostrado arriba, figura 293 GetBulkRequest.
Nota: El SNMP-Trap tiene ahora el mismo formato que las demás solicitudes.
SnmpMgmtCom (SNMP Management Comunication): Añade el identificador del entorno emisor (srcParty), del receptor (dstParty) y el contexto a la PDU. El contexto especifica el ámbito de SNMPv2 que contiene la información de gestión a la que referencia la comunicación.
SnmpAuthMsg: Este campo se utiliza como información de autentificación para el protocolo de información usado por el entorno en cuestión. El SnmpAuthMsg está serializado de acuerdo con ASN.1 BER por lo que puede ser encriptado.
SnmpPrivMsg SNMP Private Message: El SNMPv2 Private Message es un mensaje SNMPv2 autentificado que posiblemente está protegido de intrusiones en la información que contiene. Un destino privado (privDst) se añade al entorno de destino. El mensaje pasa a ser encapsulado en un datagrama UDP/IP normal y se envía a su destino a través de la red.

6.6 WIRELESS

6.6.1 ANTECEDENTES

Hoy en día, la red inalámbrica principalmente es usada para la comunicación de voz, en donde la voz se pueda enviar por mail; puede ser que se convierta en el servicio más popular y mejor valuado. Como sea, un nuevo tópico está siendo mencionada cada vez más en el mercado: **WAP (Wireless Application Protocol, Protocolo de Aplicaciones Inalámbricas)**. WAP es completamente un nuevo concepto. Esto provee un servicio orientado a datos hacia el mercado y es capaz de brindar servicios, en donde sea cuando uno quiera, por más lejos que se encuentre el usuario final. WAP es un estándar global que es independiente del navegador principal. Con WAP, una nueva dimensión será anexada a los teléfonos móviles, a través de la introducción al mercado de los servicios orientados a datos. WAP es un estándar global que no está controlado por ninguna compañía, lo que asegura su democracia, su apertura y su universalidad. Aunque lo más conocido del WAP es la integración de la red y el móvil, conviene dejar muy claro que es capaz de funcionar sobre cualquier dispositivo que disponga de conexión inalámbrica; por otro lado, el WAP no ha sido sólo ideado para transmitir contenidos desde Internet, sino que cualquier empresa puede disponer de un servidor de este tipo para ofrecer aquellos servicios y contenidos que le parezcan sin que por ello tengan que guardar ninguna relación en Internet. No obstante, sí es cierto que el mayor crecimiento de esta tecnología se deberá a su interrelación con la red. A mediados de 1997 Ericsson, Motorola, Nokia y Phone.com (antes Unwired Planet), se unieron para definir un nuevo protocolo para los dispositivos móviles. Estas tres empresas fundaron el Foro WAP, con intención de desarrollar nuevas aplicaciones de amplia aceptación para la industria de las telecomunicaciones inalámbricas, el objetivo era ofrecer nuevos servicios hacia los usuarios, servicios inalámbricos orientados a la comunicación de datos, en una forma de relacionar a Internet con sus aplicaciones y las telecomunicaciones.

6.6.2 CONCEPTO DE TELEFONIA MOVIL

Existen múltiples elementos que conforman una red celular, con los cuales se puede explicar el concepto de telefonía móvil, entre los más importantes se encuentran:

- **Central Celular**.-Es una central de conmutación especialmente dedicada al servicio celular, además de desempeñar las funciones relativas al tratamiento, monitoreo, manejo de los canales de control y voz del sistema, también sirve de interfaz entre el abonado

celular y la red fija u otros sistemas celulares. La central celular cuenta con recursos para el control y registro de la tarificación de los móviles para procesos de facturación.

- **Sitio Celular**.-Es el elemento responsable de atender a las llamadas originadas o destinadas a su área de cobertura. Representa la interfaz entre la unidad móvil y el sistema. Desempeña funciones locales de control, monitoreo y supervisión de llamadas, además de iniciar el proceso de Handoff cuando la unidad móvil se desplaza de un sitio celular a otro.
- **Abonado Móvil**.-Es el dispositivo por medio del cual se comunica el usuario bajo el comando del sistema. El abonado móvil es capaz de sintonizarse a cualquier canal y transmitir al nivel de potencia seleccionado.
- **Red Pública**.-La central celular está conectada por medio de troncales a una o más centrales de la red pública fija, a fin de integrar la red celular con las otras redes de comunicaciones existentes y permitir las llamadas entre los abonados móviles y los abonados de la red pública.
- **Canales**.-Los canales utilizados en los sistemas móviles se componen de un par de frecuencias, una destinada a la transmisión de la comunicación (forward) y otra para la recepción de la comunicación (reverse).

6.6.3 CONCEPTO DE INTERNET, EL MODELO WORLD WIDE WEB

Conjunto de redes y ruteadores que utilizan el protocolo TCP/IP y que funcionan como una sola y gran red. Internet comprende al Gobierno, comercio y organizaciones educativas alrededor del mundo. Internet es el nombre de un grupo de recursos de información mundial. Desde nuestro punto de vista, las redes de computadoras son simplemente el medio que transporta la información. No hay que pensar en Internet como una red de computadoras, sino como una gran fuente de información práctica y divertida. Internet es mucho más que una red de computadoras o un servicio de información, es la demostración de aquellas personas que puedan comunicarse libre y convenientemente. El modelo World Wide Web, es la arquitectura de la Web de Internet que provee un muy flexible y poderoso modelo de programación. Las aplicaciones y contenido son presentados en un formato de datos estándar y son buscadas por aplicaciones conocidas como navegadores. Los navegadores en la Web son aplicaciones que envían requerimientos por objetos de datos determinados a servidores de red, los cuales les responden con datos codificados en formatos estándar.

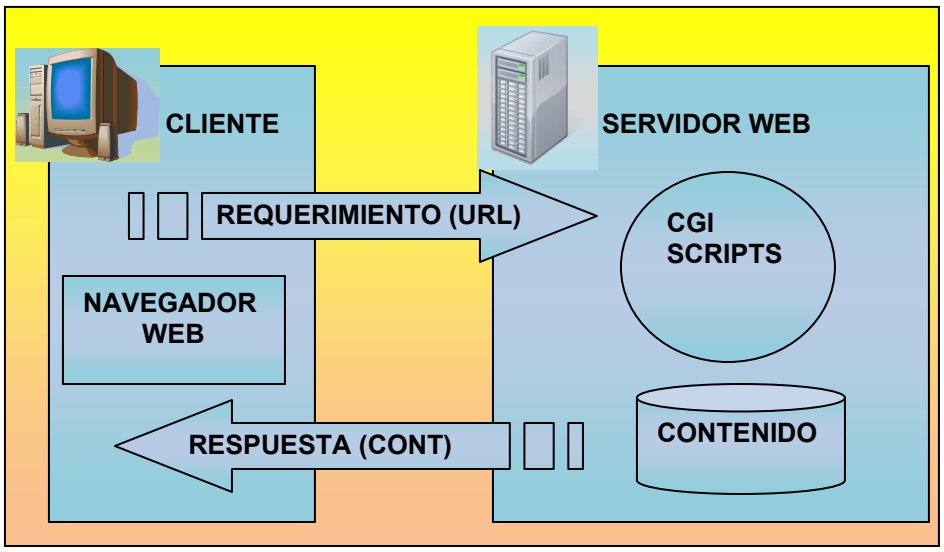


Figura 294 Modelo de Programación de la Web

Las especificaciones estándar de la Web especifican muchos de los mecanismos necesarios para construir entornos de aplicaciones de propósito general, entre los que se incluyen:

- **Modelo estándar de nombres**: Todos los servidores y el contenido de la Web son llamados por un estándar de Internet llamado **Localizador Uniforme de Recursos (Uniform Resource Locator, URL)**.
- **Formatos de contenido estándar**: Todos los navegadores soportan distintos formatos de contenido entre los que se puede mencionar HTML y Java Script.
- **Protocolos estándar**: Los protocolos le permiten a un navegador comunicarse con un servidor, él más popular es el Protocolo de Transferencia de Hipertexto (HTTP).

Esta infraestructura permite a los usuarios alcanzar fácilmente un gran número de aplicaciones y servicios de contenido. También le permite a los desarrolladores de aplicaciones crear fácilmente servicios de contenido y programas dirigidos a una gran comunidad de clientes. El protocolo de la Web define tres clases de servidores:

- **Servidor Origen**: El servidor sobre el cual reside un recurso dado (contenido) o es creado.
- **Proxy**: Programa intermedio entre el cliente y el servidor con el propósito de la hechura de requerimientos de contenido en beneficio de otros clientes. El Proxy reside típicamente entre el cliente y el servidor, lo que implica que no hay comunicación directa entre ellos, sino a través de un firewall. Los requerimientos son atendidos por el Proxy o pasan a través de él, con una posible traducción, hacia otros servidores.
- **Gateway**: Se trata de un servidor que actúa como intermediario a otro servidor. A diferencia del Proxy, el gateway recibe requerimientos como si fuera el servidor origen al cual se le solicita el recurso. El cliente puede no estar enterado que se esta comunicando utilizando un gateway.

6.6.4 MARCO TEORICO

6.6.4.1 CONCEPTO DE WAP

El WAP se trata de un protocolo que permite el acceso a Internet desde un sistema móvil a través de la red GSM (Protocolo que utilizan los móviles para comunicarse, basado en tecnología digital). WAP es una especificación para un conjunto de protocolos de comunicaciones con el ánimo de normalizar la forma en la que los dispositivos inalámbricos (tales como teléfonos móviles, emisores/receptores de radio, etc.) accedan a Internet. Aunque esto ya era posible, cada fabricante usaba tecnología distinta. A partir de ahora los dispositivos y servicios que usen WAP, serán capaces de interoperar entre ellos. Es un estándar abierto, cualquiera puede acceder a él y desarrollar dispositivos, gateways o contenidos WAP. WAP es un protocolo basado en los estándares de Internet que ha sido desarrollado para permitir a los teléfonos celulares navegar a través de Internet. Con la tecnología WAP se pretende que desde cualquier teléfono celular WAP se pueda acceder a la información que hay en Internet, así como realizar operaciones de comercio electrónico.

6.6.4.2 DESCRIPCION DE WAP.

El Protocolo de Aplicaciones Inalámbricas surge como la combinación de dos tecnologías de amplio crecimiento y difusión durante los últimos años: Las Comunicaciones Inalámbricas e Internet. Mas allá de la posibilidad de acceder a los servicios de información contenidos en Internet, el protocolo pretende proveer de servicios avanzados adicionales como, por ejemplo, el desvío de llamadas inteligente, en el cual se proporcione una interfaz al usuario en el cual se le pregunte la acción que desea realizar: aceptar la llamada, desviarla a otra persona, desviarla a un buzón vocal, etc. Para ello, se parte de una arquitectura basada en la arquitectura definida para el World Wide Web (WWW), pero adaptada a los nuevos requisitos del sistema. De esta forma, en la terminal inalámbrica existiría un “micronavegador” encargado de la coordinación con el gateway, al cual la realiza peticiones de información que son adecuadamente tratadas y redirigidas al servidor de información adecuado. Una vez procesada la petición de información en el servidor, se envía esta información al gateway que de nuevo procesa adecuadamente para enviarlo a la terminal inalámbrica.

Para conseguir consistencia en la comunicación entre la terminal móvil y los servidores de red que proporcionan la información, WAP define un conjunto de componentes estándar:
Un modelo de nombres estándar. Se utilizan las URL's definidas en WWW para identificar los recursos locales del dispositivo (tales como funciones de control de llamada) y las URL's (también definidas en el WWW) para identificar el contenido WAP en los servidores de información.
Un formato de contenido estándar, basado en la tecnología WWW. Unos protocolos de comunicación estándares, que permitan la comunicación del micro navegador de la terminal móvil con el servidor Web en red.
Veamos ahora un modelo global de funcionamiento de este sistema en la Figura 295.

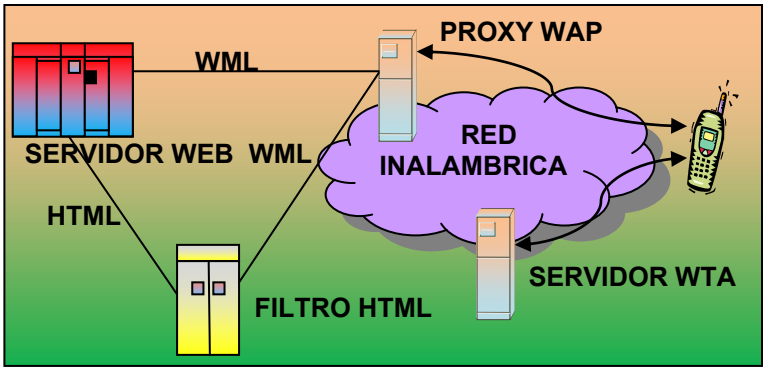


Figura 295

En el ejemplo de la figura 295, nuestra terminal móvil tiene dos posibilidades de conexión: a un proxy WAP, o a un servidor WTA. El primero de ellos, el proxy WAP traduce las peticiones WAP a peticiones Web, de forma que el cliente WAP (la terminal inalámbrica) pueda realizar peticiones de información al servidor Web. Adicionalmente, este proxy codifica las respuestas del servidor Web en un formato binario compacto, que es interpretable por el cliente. Por otra parte, el segundo de ellos, el Servidor WTA está pensado para proporcionar acceso WAP a las facilidades proporcionadas por la infraestructura de telecomunicaciones del proveedor de conexiones de red.

6.6.4.3 MODELO WAP

El modelo de programación WAP es similar al modelo de programación de la Web. Esto brinda muchos beneficios para la comunidad de desarrolladores tales como trabajar con un modelo de programación familiar, de comprobada arquitectura, y con la habilidad en herramientas comunes (tales como servidores Web, herramientas XML, etc.). La optimización y extensiones de este modelo han sido hechas para corresponder a las características del entorno inalámbrico. Donde es posible, los estándares existentes han sido adoptados o han sido usados como punto de partida para la tecnología WAP. El contenido y las aplicaciones WAP son especificados en un bien conocido conjunto de formatos de contenido basado en los que nos son familiares de la Web. El contenido es transportado usando un conjunto de protocolos de comunicación estándar basados en los de la Web. La terminal inalámbrica del usuario es coordinada por un micro navegador análogo al navegador estándar de la Web.

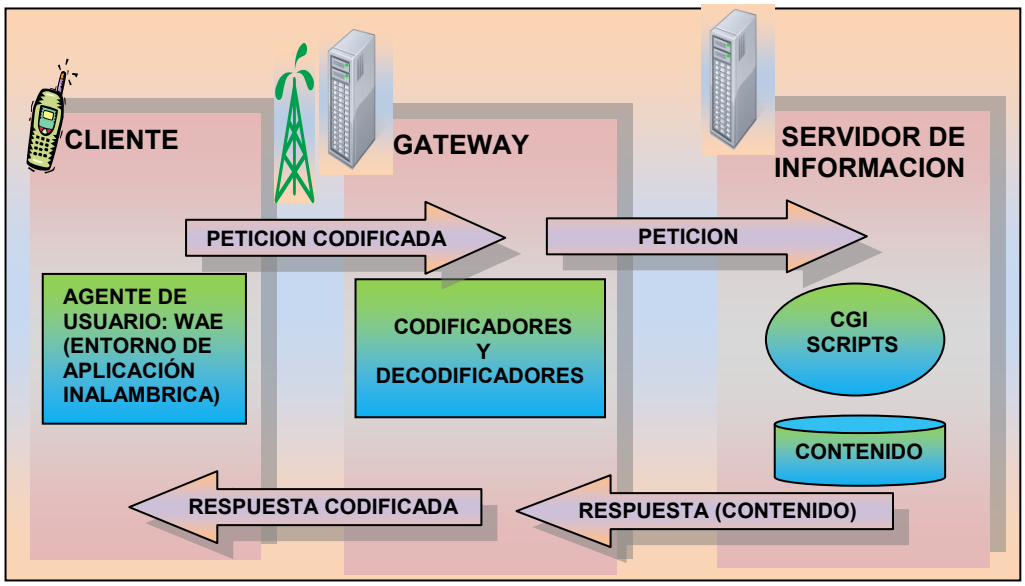


Figura 296 Modelo de programación WAP

WAP define un conjunto de componentes estándar que habilitan las comunicaciones entre la terminal móvil y los servidores de red entre los que se incluyen:

- **Modelo estándar de nombres**: Los antes mencionados URL's son también utilizados para identificar contenido WAP residente en los servidores de origen, y los **URI's (Universal Resource Identifiers, Identificador Universal de Recursos)** de la Web identifican los recursos locales del dispositivo (tales como funciones de control de llamada).
- **Formatos de contenido estándar**: Los formatos de contenido de WAP son basados en la tecnología Web incluyendo marcas, información de calendario, tarjetas para comercio electrónico, imágenes y lenguaje script.
- **Protocolos de comunicación estándar**: Los protocolos de comunicación WAP hacen posible la comunicación entre el navegador de la terminal móvil y el servidor Web en red.

Los tipos de contenido WAP y los protocolos han sido optimizados para el mercado de dispositivos inalámbricos portátiles. WAP utiliza los servidores Proxy para conectar el dominio inalámbrico a la Web. El servidor Proxy WAP típicamente comprende las siguientes funciones:

- **Protocolo de gateway**: Es el encargado del traducir los requerimientos de la pila del protocolo WAP (WSP, WTP, WTLS y WDP) a la pila del protocolo Web (HTTP y TCP/IP).
- **Codificadores y decodificadores de contenido**: Se encargan de traducir el contenido WAP en formatos compactos codificados para reducir él tráfico en la red.

Esta infraestructura garantiza que los usuarios de una terminal móvil puedan buscar una amplia cantidad de aplicaciones y contenido WAP, y que los autores de aplicaciones sean hábiles para construir servicios de contenido y programas que sea adapten a una gran cantidad de terminales móviles. Los servidores Proxy WAP permiten que contenido y aplicaciones sean alojadas sobre servidores Web convencionales y sean desarrollados usando reconocidas tecnologías Web tales como CGI.

Mientras el uso normal de WAP incluye servidor Web, Proxy WAP y usuario final WAP, en la práctica la arquitectura puede soportar otras configuraciones. Por ejemplo es posible crear un servidor Web que contenga el servidor Proxy WAP (o por lo menos desempeña su misma función). Esto puede ser usado para facilitar las soluciones de seguridad de extremo a extremo, o para aplicaciones que requieran mejorar el control de acceso a sus servidores.

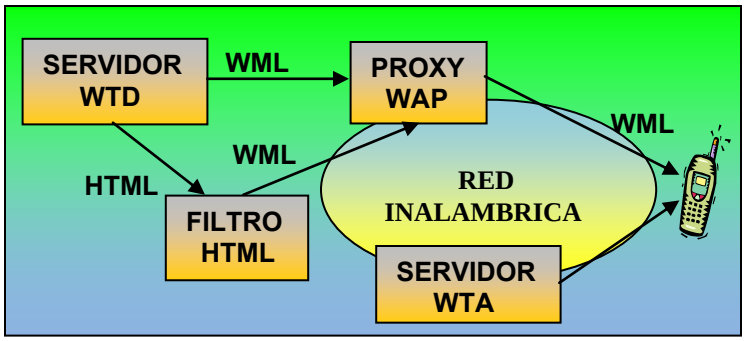


Figura 297 Ejemplo de Red WAP

En el ejemplo el cliente WAP tiene posibilidad de comunicarse con dos servidores a través de la red inalámbrica. La primera posibilidad es el servidor Proxy WAP el cual traduce el requerimiento WAP a un requerimiento Web, permitiendo así al cliente WAP realizar peticiones de información al servidor Web. El Proxy también codifica la respuesta del servidor en un formato compacto binario que es entendible para el cliente. Si el servidor Web proporciona contenido WAP (WML), el Proxy WAP recupera información directamente de él. Pero si la información se encuentra en HTML, es usado el filtro para traducir contenido Web en contenido WAP, es decir, traduce de HTML a WML. El **servidor de Aplicaciones de Telefonía Inalámbrica (WTA)**, el cual es la segunda posibilidad de conexión del terminal móvil, es un ejemplo de un servidor que responde directamente a un cliente WAP. El servidor WTA es usado para proporcionar acceso WAP a clientes soportados en la red de telecomunicaciones del proveedor de telecomunicaciones.

6.6.5 ARQUITECTURA WAP

Una vez introducido el sistema, vamos a ver la arquitectura que le da consistencia. La Arquitectura WAP está pensada para proporcionar un “entorno escalable y extensible para el desarrollo de aplicaciones para dispositivos de comunicación móvil”. Para ello, se define una estructura en capas, en la cual cada capa es accesible por la capa superior así como por otros servicios y aplicaciones a través de un conjunto de interfaces muy bien definidas y especificadas. Este esquema de capas de la arquitectura WAP la podemos ver en la Figura 298. Hagamos un recorrido por estas capas de forma breve, antes de pasar a analizarlas con más profundidad.

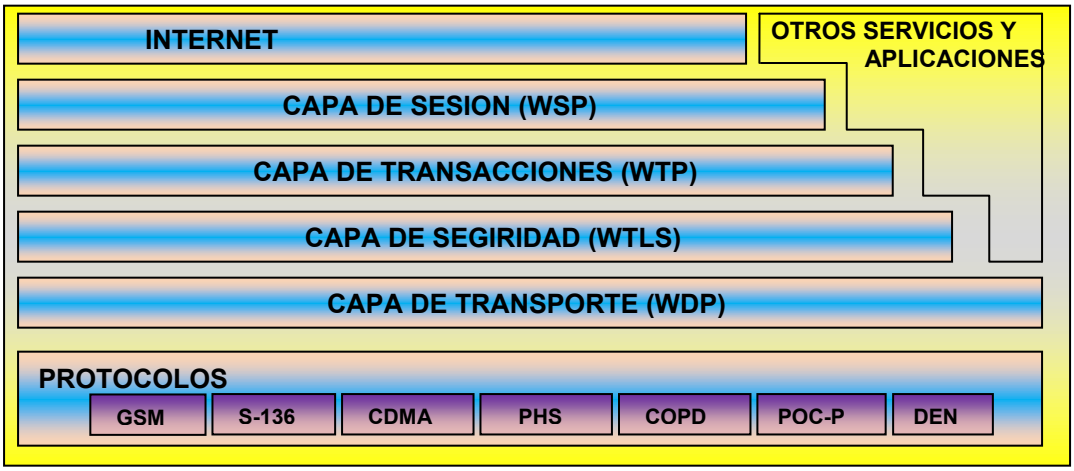


Figura 298

6.6.5.1 CAPA DE APLICACION (WAE)

El **Entorno Inalámbrico de Aplicación (WAE)** es un entorno de aplicación de propósito general basado en la combinación del World Wide Web y tecnologías de Comunicaciones Móviles. Este entorno incluye un micronavegador, del cual ya hemos hablado anteriormente, que posee las siguientes funcionalidades:

- Un lenguaje denominado WML similar al HTML, pero optimizado para su uso en terminales móviles.
- Un lenguaje denominado WML Script, similar al Java Script (esto es, un lenguaje para su uso en forma de Script)
- Un conjunto de formatos de contenido, que son un conjunto de formatos de datos bien definidos entre los que se encuentran imágenes, entradas en la agenda de teléfonos e información de calendario.

6.6.5.2 CAPA DE SESION (WSP).

El **Protocolo Inalámbrico de Sesión (WSP)** proporciona a la Capa de Aplicación de WAP una interfaz con dos servicios de sesión: Un servicio orientado a conexión que funciona por encima de la Capa de Transacciones y un servicio no orientado a conexión que funciona por encima de la Capa de Transporte (y que proporciona servicio de datagramas seguro o servicio de datagramas no seguro). Actualmente, esta capa consiste en servicios adaptados a aplicaciones basadas en la navegación Web, proporcionando las siguientes funcionalidades:

- Semántica y funcionalidades del HTTP/1.1 en una codificación compacta.
- Negociación de las características del Protocolo.
- Suspensión de la Sesión y reanudación de la misma con cambio de sesión.

6.6.5.3 CAPA DE TRANSACCIONES (WTP).

El **Protocolo Inalámbrico de Transacción (WTP)** funciona por encima de un servicio de datagramas, tanto seguros como no seguros, proporcionando las siguientes funcionalidades:

- Tres clases de servicio de transacciones:
  - Peticiones inseguras de un sólo camino.
  - Peticiones seguras de un sólo camino.
  - Transacciones seguras de dos caminos (petición-respuesta)
- Seguridad usuario-a-usuario opcional.
- Transacciones asíncronas.

6.6.5.4 CAPA DE SEGURIDAD (WTLS)

La **Capa Inalámbrica de Seguridad de Transporte (WTLS)** es un protocolo basado en el estándar SSL, utilizado en el entorno Web para la proporción de seguridad en la realización de transferencias de datos. Este protocolo ha sido especialmente diseñado para los protocolos de transporte de WAP y optimizado para ser utilizado en canales de comunicación de banda estrecha. Para este protocolo se han definido las siguientes características:

- **Integridad de los datos**: Este protocolo asegura que los datos intercambiados entre la terminal y un servidor de aplicaciones no ha sido modificada y no es información corrupta.
- **Privacidad de los datos**: Este protocolo asegura que la información intercambiada entre la terminal y un servidor de aplicaciones no puede ser entendida por terceras partes que puedan interceptar el flujo de datos.
- **Autentificación**: Este protocolo contiene servicios para establecer la autenticidad de la terminal y del servidor de aplicaciones.

Adicionalmente, el WTLS puede ser utilizado para la realización de comunicación segura entre terminales, por ejemplo en el caso de operaciones de comercio electrónico entre terminales móviles.

6.6.5.5 CAPA DE TRANSPORTE (WDP)

El **Protocolo Inalámbrico de Datagramas (WDP)** proporciona un servicio fiable a los protocolos de las capas superiores de WAP y permite la comunicación de forma transparente sobre los protocolos portadores válidos. Debido a que este protocolo proporciona una interfaz común a los protocolos de las capas superiores, las capas de Seguridad, Sesión y Aplicación pueden trabajar independientemente de la red inalámbrica que dé soporte al sistema.

El Entorno Inalámbrico de Aplicaciones

El objetivo del Entorno Inalámbrico de Aplicaciones es construir un entorno de aplicación de propósito general, basado fundamentalmente en la filosofía y tecnología del World Wide Web (WWW). Principalmente, se pretende establecer un entorno que permita a los operadores y proveedores de servicios construir aplicaciones y servicios que puedan utilizarse en una amplia variedad de plataformas inalámbricas de forma útil y eficiente. De esta forma, la arquitectura del **Entorno Inalámbrico de Aplicaciones (en adelante WAE)** está enfocado principalmente sobre los aspectos del cliente de la arquitectura del sistema de WAP, esto es, de los puntos relacionados con los agentes de usuario 11. Esto es debido a que la parte que más interesa de la arquitectura es aquella que afecta principalmente a las terminales móviles, esto es, a aquellos puntos en los cuales van a estar ejecutándose los diversos agentes de usuario. Si volvemos sobre la figura 296, vemos que entre los agentes de usuario localizados en el cliente (en la terminal móvil) y los servidores de información se define un nuevo elemento: Los gateways. Su función es codificar y decodificar la información intercambiada con el cliente, para así minimizar la cantidad de datos radiados, así como minimizar el proceso de la información por parte del cliente. Basándonos en esta arquitectura, vamos a profundizar un poco más en los componentes de este Entorno Inalámbrico de Aplicación. Tal y como podemos observar en la figura 299, se divide en dos partes, dos capas lógicas:

- Los Agentes de Usuario, que incluye aquellos elementos como navegadores, agendas telefónicas, editores de mensajes, etc..
- Los Servicios y Formatos, que incluyen todos aquellos elementos y formatos comunes, accesibles a los Agentes de Usuario, tales como WML, WML Script, formatos de imagen, etc.

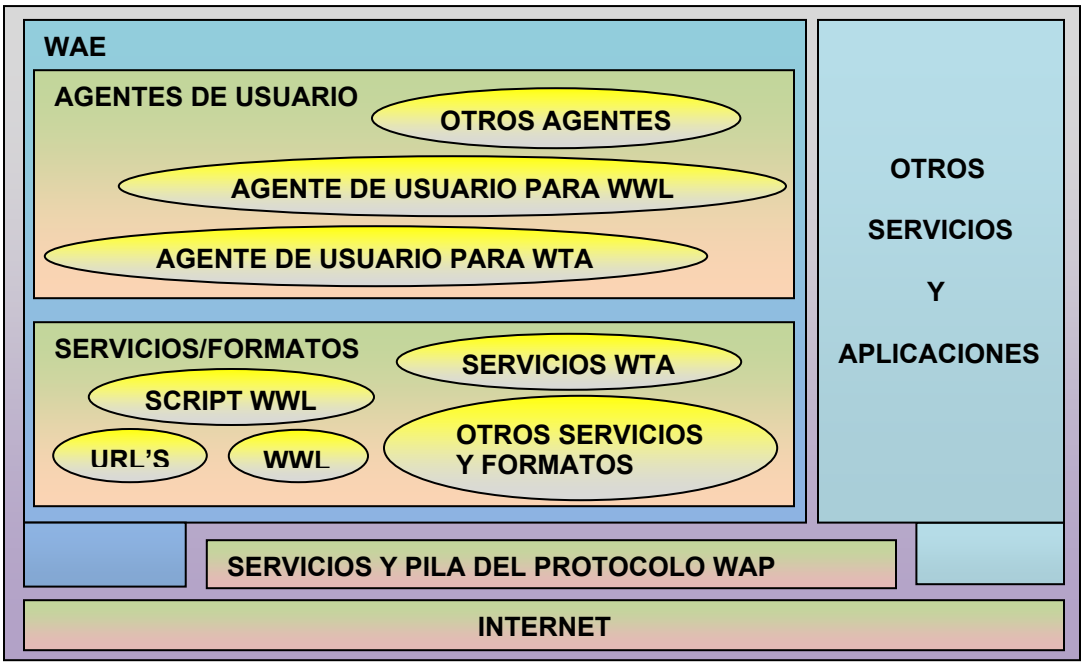


Figura 299

Como se puede ver en la figura 299, dentro de WAE se separan Servicios de Agentes de Usuario, lo que proporciona flexibilidad para combinar varios Servicios dentro de un único Agente de Usuario, o para distribuir los Servicios entre varios Agentes de Usuario. Los dos Agentes de Usuario más importantes son el Agente de Usuario para WML y el Agente de Usuario para WTA. El Agente de Usuario para WML es el Agente de Usuario fundamental en la arquitectura del Entorno Inalámbrico de Aplicación. A pesar de su importancia, este Agente de Usuario no está definido formalmente dentro de esta arquitectura, ya que sus características y capacidades se dejan en manos de los encargados de su implementación. El único requisito de funcionalidad que debe cumplir este Agente de Usuario, es el proporcionar un sistema intérprete a los lenguajes WML y WML Script, de forma que se permita la navegación desde la terminal móvil. Por otra parte, el Agente de Usuario para WTA permite a los autores acceder e interactuar con las características de los teléfonos móviles (p. e. Control de Llamada), así como otras aplicaciones supuestas en los teléfonos, tales como agendas de teléfono y aplicaciones de calendario.

El Protocolo Inalámbrico de Sesión

El Protocolo Inalámbrico de Sesión constituye la capa que se sitúa por debajo de la capa de Aplicación, proporcionando la capacidad necesaria para:

- Establecer una conexión fiable entre el cliente y el servidor, y liberar esta conexión de una forma ordenada.
- Ponerse de acuerdo en un nivel común de funcionalidades del protocolo, a través de la negociación de las posibilidades.
- Intercambiar contenido entre el cliente y el servidor utilizando codificación compacta.
- Suspender y recuperar la sesión.

Hoy por hoy, este protocolo ha sido definido únicamente para el caso de la navegación, definiéndose como WSP/B. Esta implementación está realizada para el establecimiento de una conexión sobre la base de un protocolo compatible con HTTP1.1. De esta forma, se han definido un conjunto de primitivas de servicio para permitir la comunicación entre la capa de sesión integrada dentro del equipo cliente y la capa de sesión integrada en el equipo servidor. Estas primitivas, junto con una pequeña descripción de las mismas, pueden verse en la tabla 37.

NOMBRE DE LA PRIMITIVA	DESCRIPCION
S-Connect	Esta primitiva se usa para iniciar el establecimiento de la conexión y para la notificación de su éxito.
S-Disconnect	Esta primitiva se usa para desconectar una sesión y para notificar al usuario de una sesión que esa sesión no se puede establecer, que ha sido desconectada.
S-Supend	Esta primitiva se usa para solicitar la suspensión de la sesión.
S-Resume	Esta primitiva se utiliza para solicitar que se recupere la sesión utilizando para las direcciones el nuevo identificador de punto de acceso del servicio.
S-Exception	Esta primitiva se usa para notificar aquellos eventos que no están asignados a una transacción en particular, ni provocan la desconexión o la suspensión de la sesión.

S-MethodInvoke	Esta primitiva se utiliza para solicitar una operación que deba ser ejecutada en el servidor.
S-MethodResult	Esta primitiva se utiliza para devolver una respuesta a una petición de operación.
S-MethodAbort	Esta primitiva se utiliza para abortar una solicitud de ejecución de operación, que no haya sido aún completada.
S-Push	Esta primitiva se utiliza para enviar información no solicitada desde el servidor, dentro del contexto de una sesión de forma y sin confirmación.
S-ComfimedPush	Esta primitiva realiza las mismas funciones que la anterior, pero con confirmación.
S-PushAbort	Esta primitiva se utiliza para anular una primitiva anterior del tipo S-Push o SConfirmedPush.

Tabla 37 Primitivas de Inicio de Sesión

Adicionalmente, existen cuatro tipos de cada una de estas primitivas, tal y como puede verse en la tabla 38.

TIPO	ABREVIACION	DESCRIPCION
Request	req	Se utiliza cuando una capa superior solicita un servicio de la capa inmediatamente inferior.
Indication	ind	Una capa que solicita un servicio utiliza este tipo de primitiva para notificar a la capa inmediatamente superior de las actividades relacionadas con su par o con el proveedor del servicio.
Response	res	Este tipo de primitiva se utiliza para reconocer la recepción de la primitiva de tipo Indication de la capa inmediatamente inferior.
Confirme	cnf	La capa que proporciona el servicio requerido utiliza este tipo de primitiva para notificar que la actividad ha sido completada satisfactoriamente.

Tabla 38 Tipos de Primitivas de Servicio

Por último, reseñar que cada una de estas primitivas está perfectamente definida dentro de la especificación, tanto desde el punto de vista del diagrama de tiempos en el que se tienen que invocar las primitivas, como desde el punto de vista de los parámetros intercambiados.

El Protocolo Inalámbrico de Transacción

El Protocolo Inalámbrico de Transacción se establece para proporcionar los servicios necesarios que soporten aplicaciones de "navegación" (del tipo petición/respuesta). Es a este dúo petición/respuesta, lo que vamos a denominar como transacción. Este protocolo se sitúa por encima del Protocolo Inalámbrico de Datagramas y, de forma opcional, de la Capa Inalámbrica de Seguridad de Transporte, que serán estudiados posteriormente. Las características de este protocolo son:

- Proporciona tres clases de servicios de transacción:
  - Clase 0: mensaje de solicitud no seguro, sin mensaje de resultado.
  - Clase 1: mensaje de solicitud seguro, sin mensaje de resultado.
  - Clase2: mensaje de solicitud seguro, con, exactamente, un mensaje de resultado seguro.
- La seguridad se consigue a través del uso de identificadores únicos de transacción, asentimientos, eliminación de duplicados y retransmisiones.

Seguridad opcional usuario a usuario

De forma opcional, el último asentimiento de la transacción puede contener algún tipo de información adicional relacionada con la transacción, como medidas de prestaciones, etc. Se proporcionan mecanismos para minimizar el número de transacciones que se reenvían como resultado de paquetes duplicados. Se permiten las transacciones asíncronas. Al igual que en el protocolo anterior (el protocolo inalámbrico de sesión), en la tabla 39 vamos a ver las primitivas de servicio 14 que sustentan la comunicación entre dos capas de transacciones situadas en dos equipos distintos:

NOMBRE DE LA PRIMITIVA	DESCRIPCION
TR-Invoke	Esta primitiva se utiliza para iniciar una nueva transacción.
TR-Result	Esta primitiva se utiliza para devolver el resultado de transacción iniciada anteriormente.
TR-Abort	Esta primitiva se utiliza para abortar una transacción existente.

Tabla 39 Primitivas de Servicio de Transacción

A modo de ejemplo, vamos a ver en la figura 300 la concatenación de Primitivas de Servicio de Sesión y de Transacción para el caso de una petición-respuesta:

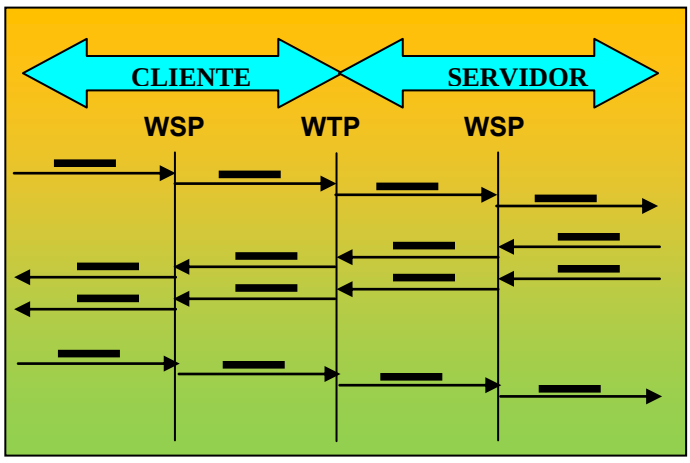


Figura 300

Para finalizar, vamos a detallar un poco más las principales características de este protocolo:

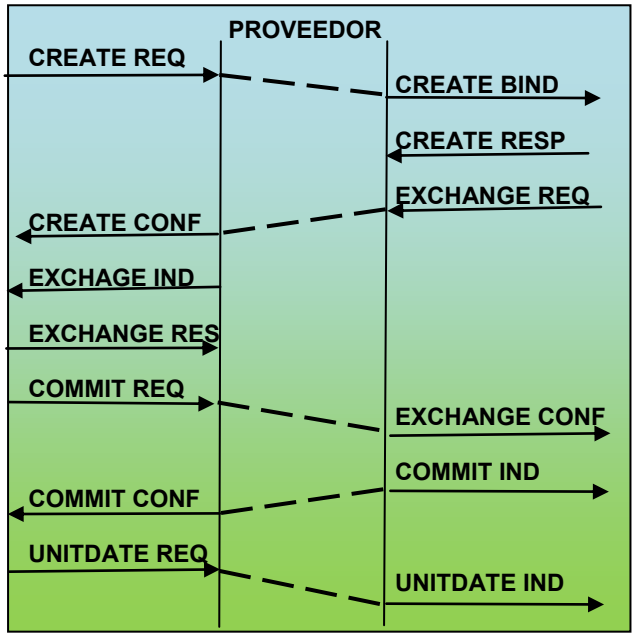
- **Transferencia de Mensajes**: Dentro de este protocolo se distinguen dos tipos de mensajes: mensajes de datos y mensajes de control. Los mensajes de datos transportan únicamente datos de usuario, mientras que los mensajes de control se utilizan para los asentimientos, informes de error, etc. pero sin transportar datos de usuario.
- **Retransmisión hasta el asentimiento**: Esta característica se utiliza para la transferencia fiable de datos desde un proveedor WTP a otro, en caso que haya pérdida de paquetes. A modo de comentario, dejar claro que para reducir lo máximo posible el número de paquetes que se transmiten, este protocolo utiliza asentimiento explícito siempre que sea posible.
- **Asentimiento de usuario**: El Asentimiento de Usuario permite al usuario de este protocolo, confirmar cada mensaje recibido por el proveedor WTP.
- **Información en el Último Asentimiento**: Se permite, así pues, enviar información en el último, y únicamente en el último, asentimiento de una transacción. De esta forma, se puede enviar, por ejemplo, información del rendimiento proporcionado por el sistema durante la transacción realizada, etc.
- **Concatenación y Separación**: Podemos definir concatenación como el proceso de trasmitir múltiples Unidades de Datos del Protocolo (PDU) de WTP en una Unidad de Datos del Servicio (SDU) de la red portadora. Por el contrario, separación es el proceso de separar múltiples PDU's de un único SDU (esto es, el proceso inverso al anterior). El objetivo de estos sistemas es proveer eficiencia en la transmisión inalámbrica, al requerirse un menor número de transmisiones.
- **Transacciones Asíncronas**: Para un correcto funcionamiento del protocolo, múltiples transacciones deben ser procesadas de forma asíncrona, debe ser capaz de iniciar múltiples transacciones antes que reciba la respuesta a la primera transacción.
- **Identificador de la Transacción**: Cada transacción está identificada de forma única por los pares de direcciones de los sockets (Dirección fuente, puerto fuente, dirección destino y puerto destino) y por el Identificador de Transacción (TID), el cual se incrementa para cada una de las transacciones iniciadas. Este número es de 16 bits, utilizándose el bit de mayor orden para indicar la dirección.
- **Segmentación y re-ensamblado (opcional)**: Si la longitud del mensaje supera la Unidad Máxima de Transferencia (MTU 18), el mensaje puede ser segmentado por el WTP y enviado en múltiples paquetes. Cuando esta operación se realiza, estos paquetes pueden ser enviados y asentidos en grupos. De esta forma, el emisor puede realizar control de flujo cambiando el tamaño de los grupos de mensajes dependiendo de las características de la red.

La Capa Inalámbrica De Seguridad de Transporte

La Capa Inalámbrica de Seguridad de Transporte (en adelante WTLS), constituye una capa modular, que depende del nivel de seguridad requerido por una determinada aplicación. Esta capa proporciona a las capas de nivel superior de WAP de una interfaz de servicio de transporte seguro, que lo resguarde de una interfaz de transporte inferior. El principal objetivo de esta capa es proporcionar privacidad, integridad de datos y autentificación entre dos aplicaciones que se comuniquen. Adicionalmente, la WTLS proporciona una interfaz para el manejo de conexiones seguras. Al igual que hemos hecho en los protocolos anteriores, en la tabla 40 vamos a ver las primitivas de servicio 19 que sustentan la comunicación entre dos capas situadas en dos equipos distintos.

NOMBRE DE LA PRIMITIVA	DESCRIPCION
SEC-UnitData	Esta primitiva se utiliza para intercambiar datos de usuario entre los dos participantes. Sólo puede ser invocada cuando existe previamente una conexión segura entre las direcciones de transporte de los dos participantes.
SEC-Create	Esta primitiva se utiliza para iniciar el establecimiento de una conexión segura.
SEC-Exchange	Esta primitiva se utiliza en la creación de una conexión segura si el servidor desea utilizar autentificación de clave pública o intercambio de claves con el cliente.
SEC-Commit	Esta primitiva se inicia cuando el **handshake** se completa y cualquiera de los equipos participantes desea cambiar a un nuevo estado de conexión negociado.
SEC-Terminate	Esta primitiva se utiliza para finalizar la conexión.
SEC-Exception	Esta primitiva se utiliza para informar al otro extremo sobre las alertas de nivel de aviso.
SEC-Create-Request	Esta primitiva se utiliza por el servidor para solicitar al cliente que inicie un nuevo **handshake**.

Tabla 40 Primitivas de Servicio de la Capa de Seguridad



Hemos hablado anteriormente del proceso de establecimiento de una sesión segura o handshake. En la figura 301 podemos ver este intercambio de primitivas:

Figura 301

El Protocolo Inalámbrico de Datagramas.

El Protocolo Inalámbrico de Datagramas (en adelante WDP 21) ofrece un servicio consistente al protocolo (Seguridad, Transacción y Sesión) de la capa superior de WAP, comunicándose de forma transparente sobre uno de los servicios portadores disponibles. Este protocolo ofrece servicios a los protocolos superiores del estilo a direccionamiento por número de puerto, segmentación y reensamblado opcional y detección de errores opcional, de forma que se permite a las aplicaciones de usuario funcionar de forma transparente sobre distintos servicios portadores disponibles. Para ello, se plantea una arquitectura de protocolo como el que se muestra en la figura 302. Al igual que hemos hecho en los protocolos anteriores, en la tabla 41 vamos a ver las primitivas de servicio 22 que se utilizan en este protocolo:

NOMBRE DE LA PRIMITIVA	DESCRIPCION
T-DUnitData	Esta primitiva es utilizada para transmitir datos como datagramas. No requiere que exista una conexión para establecerse.
T-DError	Esta primitiva se utiliza para proporcionar información a la capa superior cuando ocurre un error que pueda influenciar en el servicio requerido.

Tabla 41 Primitivas de Servicio de la Capa de Datagramas

Por último, vamos a ver la arquitectura de este protocolo dentro de la arquitectura global de WAP, para el caso de utilizarse GSM como servicio portador, que es el protocolo que más nos puede interesar por su amplia implantación en los sistemas de comunicaciones móviles telefónicas existentes hoy en día.

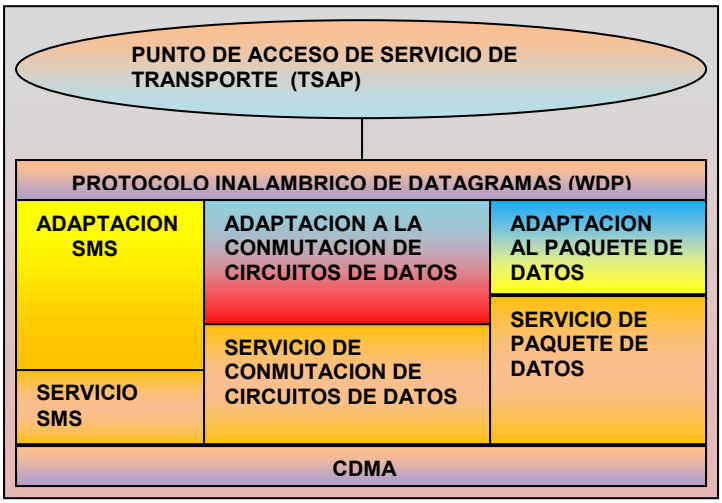


Figura 302

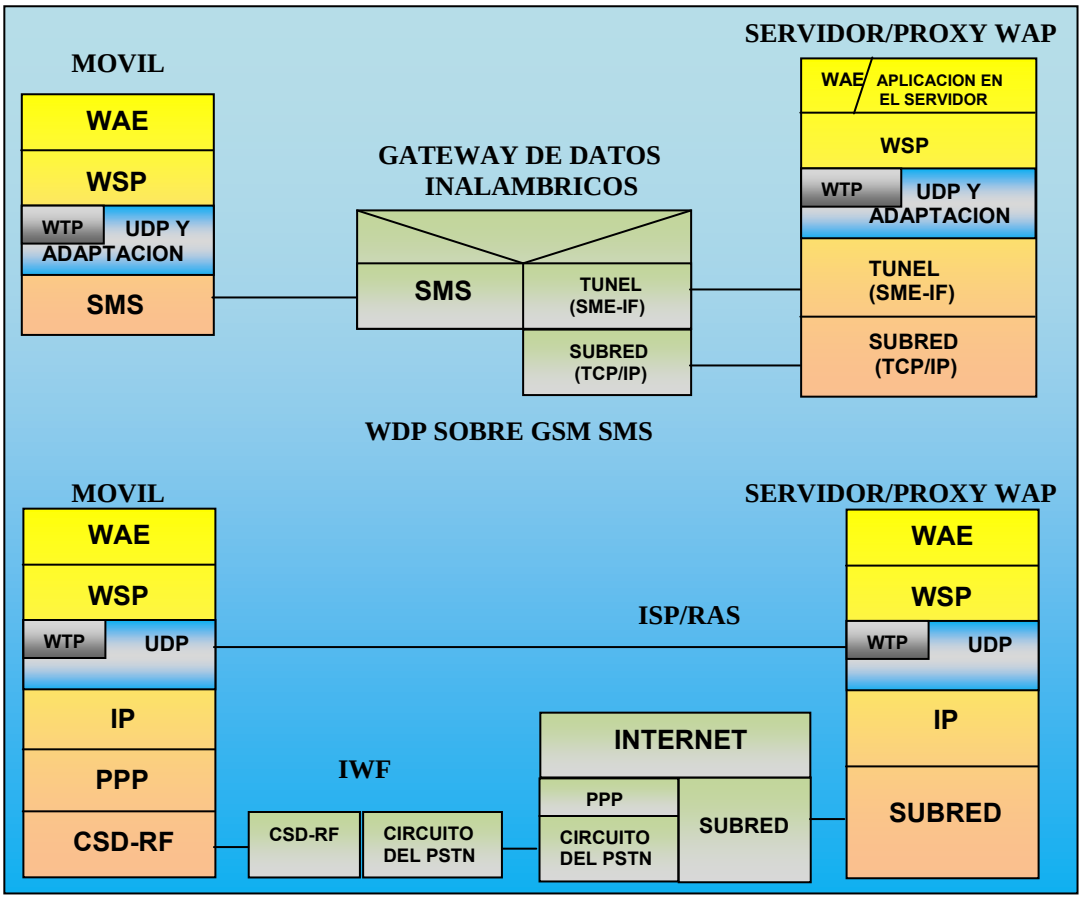


Figura 303

6.6.6 USO Y APLICACIONES DE WAP

La arquitectura por capas de WAP posibilita que otros servicios y aplicaciones utilicen las características de la pila WAP a través de unas bien definidas interfaces. Aplicaciones externas pueden acceder directamente las capas de sesión, transporte, transacción y seguridad. Esto permite que la pila de WAP sea usada para aplicaciones y servicios que no son normalmente especificados por WAP, los cuales son muy valiosos en el mercado inalámbrico. Por ejemplo aplicaciones tales como:

- Aplicaciones telefónicas.
- Correo electrónico.
- Acceso de información de Internet.
- Calendario.
- Libreta de teléfonos.
- Comercio electrónico móvil.

El protocolo WAP está diseñado para operar sobre una variedad de diferentes servicios portadores (o de mensajería) incluyendo:

- Mensajes cortos.
- Llamadas.
- Datos de circuitos conmutados.
- Paquetes de datos.
- Servicios de la banca.
- Noticias.
- Deportes.
- Clima.

- Balance de inventarios.
- Teleservicios.
- Juegos.
- Información geográfica.

Los portadores ofrecen diferentes niveles de calidad de servicio con respecto a la calidad de datos que se puedan transmitir, rate de errores y retrasos. El protocolo WAP está diseñado para compensar o tolerar estas variaciones en el nivel de servicio. Puesto que la capa WDP proporciona la convergencia entre el servicio de portadores y el resto de las capas, WDP especifica claramente los mensajeros que son soportados y las técnicas usadas para permitir que el protocolo WAP corra sobre cualquiera de ellos.

6.6.6.1 APLICACIÓN DE TELEFONIA INALÁMBRICA

La infraestructura WTA soporta las aplicaciones de telefonía inalámbrica que interactúan con dispositivos y redes telefónicas. La infraestructura WTA extiende la infraestructura WAE adicionando:

- Una interfaz a partir de WTA-WML y WML Script que especifica un conjunto de funciones relacionadas con telefonía en el cliente. Esta interfaz es llamada la **Interfaz de Aplicaciones de Telefonía Inalámbrica (WTAI)**.
- Manejo de eventos de red. Esto significa que eventos originados en la red móvil pueden ser detectados por el agente de usuario WTA, y acciones en respuesta a estos eventos pueden ser definidas.
- Un depósito, que permanentemente almacena contenido que los servicios WTA ejecutan. El propósito del depósito es cumplir los requerimientos en tiempo real que son ejecutados por los servicios WTA.
- Un modelo para el estado del agente de usuario WTA y el manejo del contexto WTA.
- Un modelo de seguridad obligatorio.

6.6.6.1.1 VISTAZO GENERAL A LA ARQUITECTURA

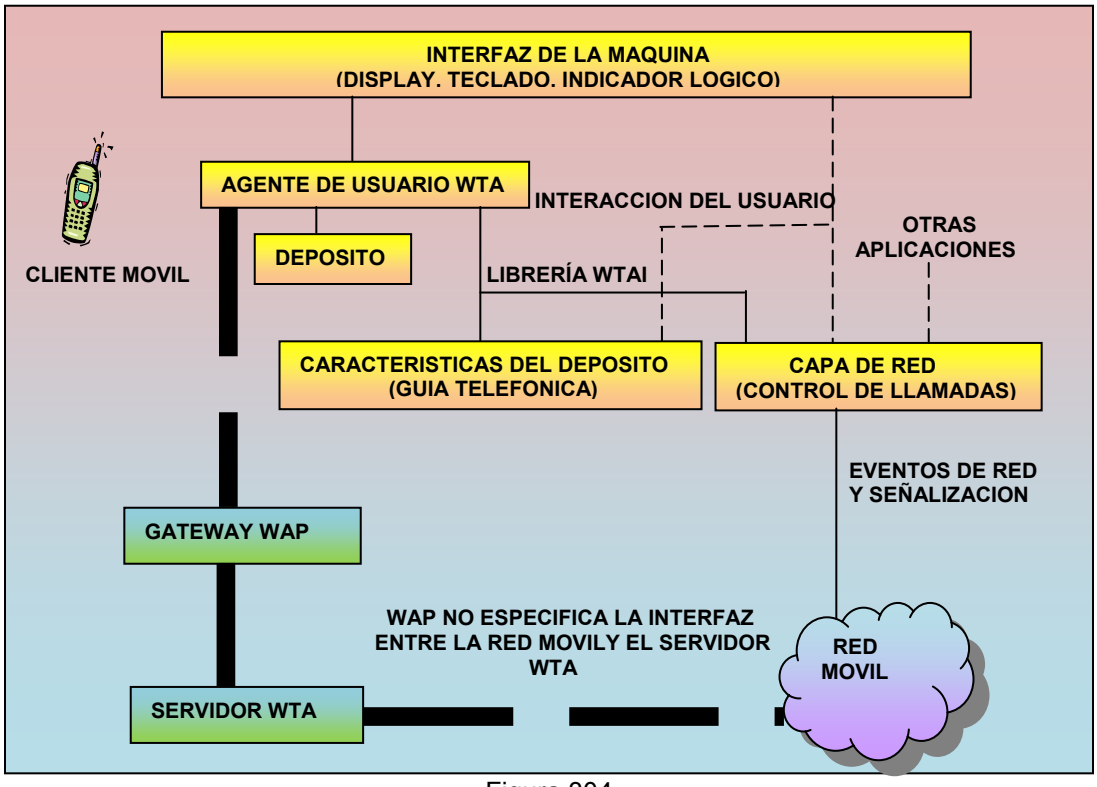


Figura 304

La Aplicación de Telefonía Inalámbrica (Wireless Telephony Application – WTA) es una infraestructura de aplicación en servicios de telefonía. El agente de usuario WTA es una extensión del agente de usuario estándar WML con la capacidad adicional de interconectar los servicios disponibles de la red móvil con los dispositivos de telefonía móvil, por ejemplo, estableciendo y recibiendo llamadas telefónicas. La siguiente figura 304 describe una posible configuración de la estructura WTA. Sin embargo, esta especificación solamente define los componentes contenidos en el cliente.

Es muy importante reconocer la habilidad para soportar funciones simples de telefonía desde adentro de un agente de usuario WAE. Con la perspectiva de la biblioteca especial WTA, ha sido definida la biblioteca pública WTAI. Esta librería contiene funciones que pueden ser llamadas desde cualquier aplicación WAE, figura 305 y proporciona acceso a funciones de funciones de telefonía simples como un asistente al usuario. Por ejemplo, se le permite al autor WML que incluya una función clic en el teléfono dentro del contenido, para ahorrarle al usuario tener que tipear los números usando la interfaz de maquina. Como se menciono anteriormente, la infraestructura de WTA confía en un agente de usuario dedicado en el cliente, el cual se explicara a continuación. El servidor WTA no es especificado por WAP pero posteriormente se hará una apreciación global de este.

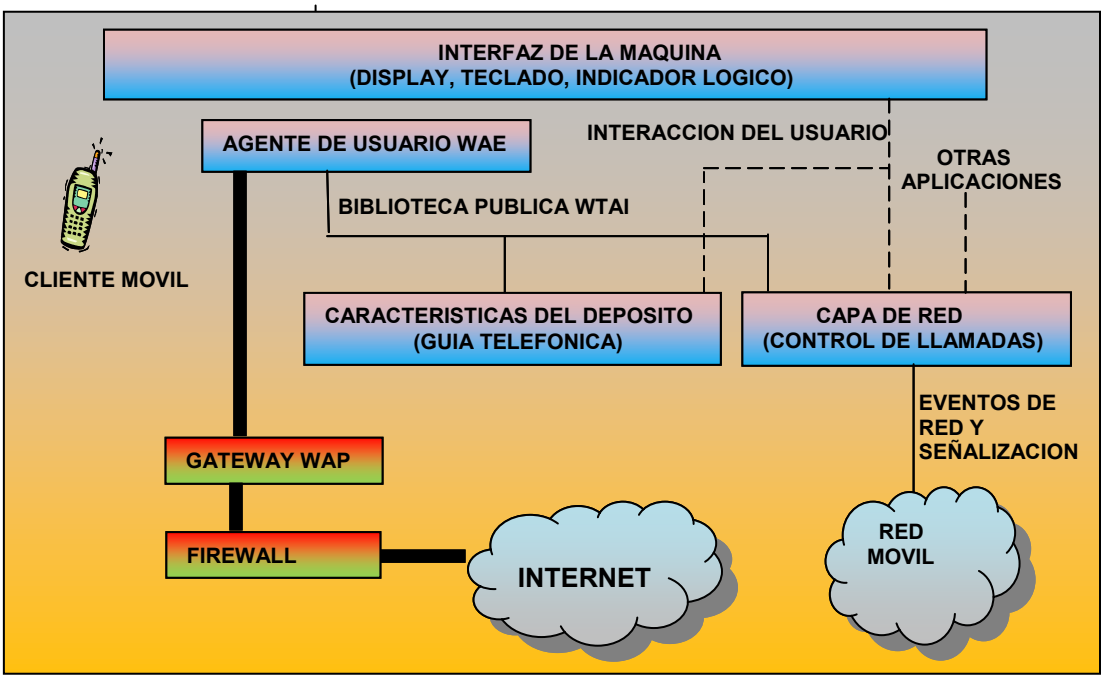


Figura 305

6.6.6.1.2 LOS AGENTES DE USUARIO WTA y WAE

La figura 304 descrita anteriormente, ilustra como el agente de usuario WTA, el deposito (o almacén permanente) y WTAI (la interfaz de aplicaciones de telefonía) interactúan entre si con otras entidades del dispositivo del cliente móvil WTA. El agente de usuario WTA puede recobrar el contenido del depósito mientras que WTAI asegura que el agente de usuario WTA puede interactuar con las funciones de la red móvil (por ejemplo, haciendo llamadas) y características especificas del dispositivo (por ejemplo, manipulando la guía telefónica). El agente de usuario WTA recibe los eventos de la red que pueden ligarse al contenido, de tal manera se hacen posibles las aplicaciones dinámicas en la telefonía. Los eventos de la red que serán disponibles para el agente de usuario WTA son aquellos que resultan de acciones tomadas por los servicios ejecutados sobre

el propio agente de usuario WTA. Los eventos telefónicos iniciados fuera del dispositivo también son pasados al agente de usuario WTA, eventos tales como los mensajes de texto de red que no están dirigidos explícitamente hacia algún otro agente de usuario (por ejemplo eventos pretendidos por SIM). Esto significa, por ejemplo que los eventos de red causados por el agente de usuario WML no afectaran al agente de usuario WTA. La figura 305 ilustra como el agente de usuario WAE y la librería pública WTAI (interfaz de aplicaciones inalámbricas) interactúan recíprocamente entre sí y con otras entidades en un cliente móvil WTA. El agente de usuario WAE sólo recobra contenido a través del gateway WAP y únicamente tiene acceso a las funciones de la librería pública WTAI. Estas funciones muestran la simple operatividad semejante a la capacidad para hacer una llamada, pero no permite completamente el control de la telefonía. Únicamente el agente de usuario WTA esta habilitado para controlar plenamente los dispositivos de telefonía del dispositivo. En particular, el agente de usuario WAE no es capas de recibir y reaccionar a los eventos de texto de la red de telefonía. Nótese que la figura 304 y la figura 305 muestran una separación lógica de los dos agentes de usuario. Ellos podrán coexistir en el mismo dispositivo y es muy probable que se implementen con elementos de código común.

6.6.6.1.3 SERVIDOR WTA

El servidor WTA puede pensarse como un servidor de la red el cual entrega el contenido requerido por el cliente. Un agente de usuario WTA usa URL's para referirse al contenido en el servidor WTA, como un navegador en la Web Internet. Un URL también puede ser usado para referirse a una aplicación en un servidor web (como un CGI Script) el cual es ejecutado en cuanto es llamado. Tales aplicaciones pueden programarse para realizar una gama amplia de tareas, por ejemplo puede generarse el contenido dinámico e interactuar con entidades externas. Un servidor WTA también puede hacer uso de este concepto. Con las aplicaciones referenciadas en un servidor WTA, es posible crear servicios que usan URL's para interactuar con la red móvil y otras entidades (por ejemplo, un sistema de correo de voz). Así el concepto de aplicaciones de referencia en un servidor WTA proporciona un simple pero poderoso modelo de como integrar los servicios de la red móvil con los servicios ejecutados localmente en el cliente WAP.

6.6.6.1.4 SERVICIOS WTA.

Los servicios WTA son los que el usuario finalmente experimenta desde que se esta utilizando la infraestructura WTA. Un servicio WTA aparece al cliente en forma de diferentes formatos de contenido, por ejemplo WTA-WML, WML Script, etc. El agente de usuario WTA ejecuta el contenido que persistentemente almacenado en el depósito del cliente o el contenido recobrado de un servidor WTA. La infraestructura también le permite al agente de usuario WTA actuar en eventos de la red móvil como podría ser el caso de recibir una llamada.

6.6.6.1.5 INICIACION DE SERVICIOS WTA.

El agente de usuario WTA esencialmente, ejecuta el contenido dentro del límite de un contexto conocido. El término servicio se usa para definir la magnitud de un contexto y su contenido asociado. La iniciación de un nuevo contexto es definida como el comienzo de un servicio. La terminación de un contexto define el fin de un servicio. La figura 306 ilustra las posibles maneras de iniciar un servicio WTA en el agente de usuario WTA.

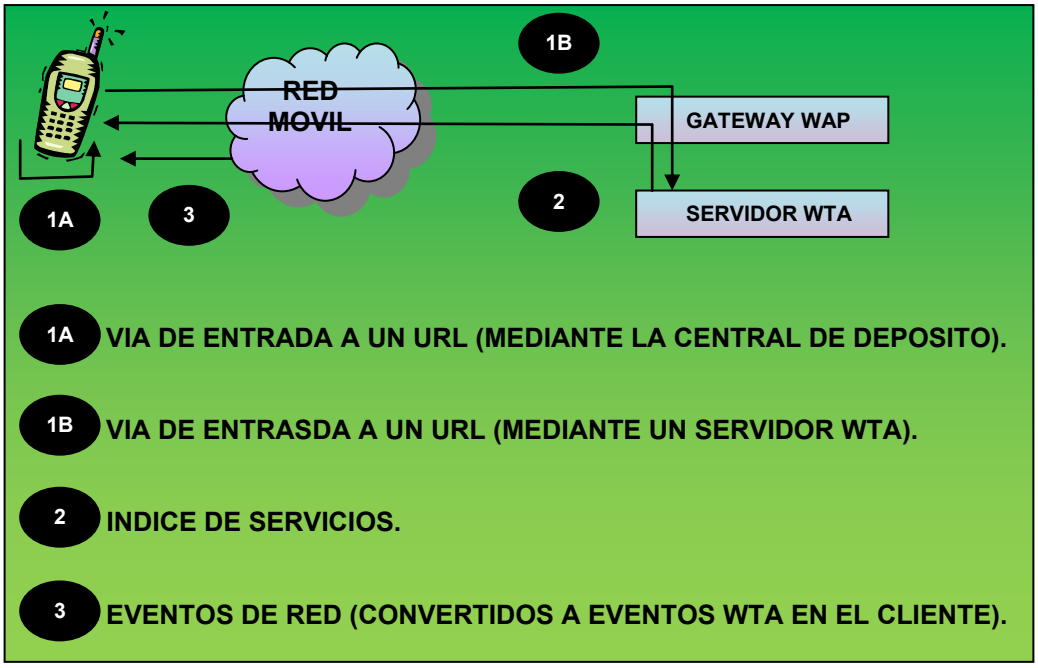


Figura 306

6.6.6.1.6 ACCESO A LA CENTRAL DE DEPÓSITO

El depósito es un modulo de almacenamiento permanente dentro de la terminal móvil, la cual almacena los requerimientos persistentes que pueden ser usados para así suprimir la demanda de acceso a la red cuando se están cargando y ejecutando frecuentemente los servicios WTA. El depósito también se encarga del problema de como un desarrollador de servicios WTA asegura que los eventos WTA críticos en el tiempo se ejecuten oportunamente. El depósito se encarga de dos problemas específicos:
Como los desarrolladores de servicios WTA preprograman los dispositivos con el contenido
Como los desarrolladores de servicios WTA mejoran los tiempos de respuesta de un servicio WTA

6.6.6.1.7 COMO ACCEDER A LA CENTRAL DEL DEPÓSITO

La central de almacenamiento podrá ser accedida por un servicio usando uno de los siguientes métodos:

- Un evento WTA puede ser asociado con un canal. Cuando un evento WTA es detectado, el agente de usuario invoca un URL específico para asociarlo al canal.
- El usuario final podrá acceder a los servicios almacenados en el depósito a través de una aplicación que depende de la representación (por ejemplo un menú conteniendo los nombres de los canales) de los servicios tolerados (los canales especificados explícitamente como accesibles al usuario) en la central de almacenamiento o depósito.
- Una URL puede ser determinado por el agente de usuario (suministrado en el contenido o entregado por un servicio de indicación (SI)). El contenido de esta URL puede ser recuperado del depósito.

Solamente las aplicaciones WTA (esto es, contenido cargado o de otra manera recibido desde el servidor WTA) pueden acceder al depósito.

6.6.6.1.8 REQUERIMIENTOS DE SEGURIDAD EN WTA.

Un servicio WTA puede invocar funciones WTAI que permitan el acceso a las funciones locales en el cliente móvil. Dado que estas funciones hacen posibles cosas tales como por ejemplo

establecer llamadas y accesos para los usuarios locales a las guías telefónicas, se puede garantizar que solamente los servicios WTA son autorizados a ser ejecutados.

2.5.1.9 DELEGACION DE SEGURIDAD

Esta dentro del interés de cada proveedor de telefonía móvil proporcionar un nivel de seguridad aceptable en la red. El proveedor de servicios de telefonía móvil confiable puede escoger:

- Ejecutar todos los servicios WTA por si mismo (no aceptar otros proveedores),
- Delegar la administración de los servicios WTA a una tercera parte.

6.6.6.1.10 CONTROL DE ACCESO

El protocolo de datagramas inalámbrico (WDP) suministra un método para separar los servicios WTA de un servicio WAE común, mediante el uso de números de puerto predeterminado. La figura 307 ilustra la configuración obligatoria. Una sesión WTA, establecida por el agente de usuario WTA deberá utilizar uno de los puertos dedicados en el gateway. El agente de usuario WTA no debe recobrar el contenido WTA fuera de la sesión WTA. El contenido recibido por fuera de la sesión WTA, y las indicaciones de servicio dirigidas al agente de usuario WTA pero entregadas fuera de la sesión WTA, deberá ser descartado.

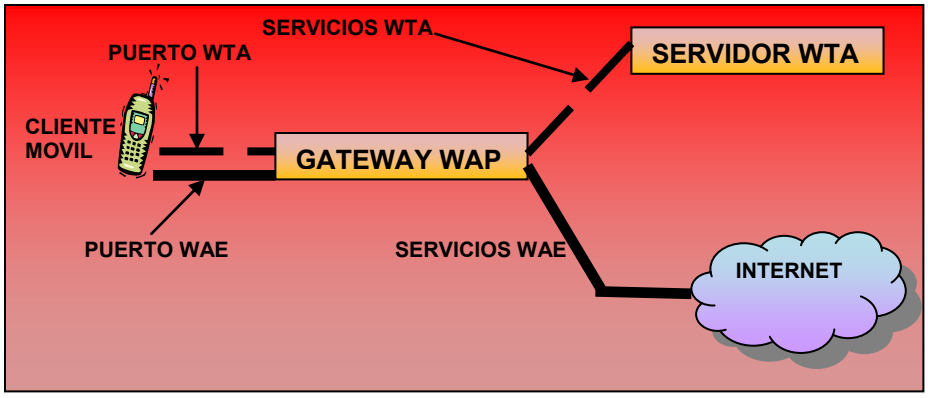


Figura 307

6.6.6.1.11 PERMISOS DEL USUARIO

Los permisos de usuario serán dados para todas las funciones WTAI (públicas y no públicas) realizadas por los ejecutables. Un ejecutable es cualquier entidad que llame funciones WTAI. Si una función WTAI es invocada y el usuario no concede el permiso, la invocación será devuelta inmediatamente sin efecto cualquiera y sin cambio alguno dentro del dispositivo como resultado del intento de ejecución, como si la función WTAI no hubiese sido invocada. En este caso el WML Script de la función WTAI debe retornar un valor inválido y la URI de la función WTAI debe de retornar una cadena de caracteres vacía. El usuario concede permiso para una función específica WTAI llamada por un ejecutable. En general solamente la acción de un único permiso será soportada por las funciones públicas WTAI. Cada una de las funciones públicas WTAI especificara los tipos de permisos que esta soporta.

6.6.6.1.12 MODELO DE SEGURIDAD WTA.

En el modelo de seguridad WTA cualquier entidad puede convertirse en proveedor de servicios WTA siendo aprobada para acceder un gateway confiable. El control de acceso del gateway confiable por los servidores WTA debe ser implementado usando soluciones de seguridad existentes figura 308.

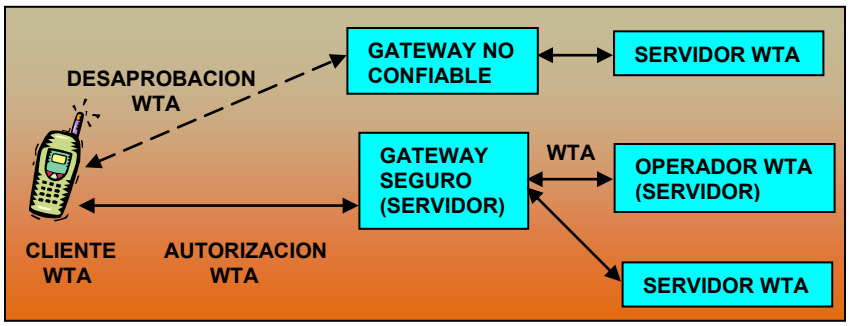


Figura308

Para proporcionar la seguridad a WTA, un gateway WAP puede controlar el acceso entre el agente de usuario WTA y el servidor WTA. El gateway WAP comprobara que los proveedores de contenido pull/push WTA estén autorizados.

6.6.6.1.13 INFRAESTRUCTURA DE SEGURIDAD DISPONIBLE

Para WTA es obligatorio tener un mecanismo de seguridad. Hasta que un modelo de contenido firmado sea disponible, la seguridad entre el cliente y el punto de conexión final. WTLS se asegura usando WTLS clase 2 de uso obligado de autenticación de certificados de servidor. Para los servicios WTA (no públicos) el uso de una sesión WTLS es obligatorio. Usando WTLS, cualquier servicio WTA puede ser entregado por los proveedores de servicios de telefonía confiable (o una entidad delegada por ellos) a través de un camino seguro desde el gateway al cliente. El gateway WAP para servidores de seguridad WTA se deja a la implementación. Para conexiones sobre Internet, SSL/TLS puede ser usado.

6.6.7 EL DEPÓSITO

El depósito se usa para guardar el contenido WTA persistente. Este proporciona un mecanismo que asegura un manejo oportuno del contenido relacionado con los servicios WTA (por ejemplo los servicios WTA iniciados por eventos WTA) y tiene las siguientes características:

- El depósito contiene un conjunto de canales y recursos.
- Los recursos son datos que han sido descargados con WSP (como una baraja WML) y que son almacenados con su meta datos y su localización (URL).
- Un canal es un recurso que incluye un conjunto de enlaces a recursos. Los canales cuentan con una identidad y frescura.
- Los canales en el depósito cuentan con un tiempo de vida de frescura, fuera del cual se consideran desactualizados. Los canales viejos (desactualizados) son removidos automáticamente por el agente de usuario. Los recursos están sujetos a la remoción automática del depósito si no son relacionados por un canal.
- Si el depósito contiene un canal que no esta desactualizado, esto garantiza que el depósito contiene todos los recursos nombrados por el canal. La carga y descarga de un canal es una operación automática en la que el agente de usuario no reconocerá la presencia del canal hasta que todo el contenido en el canal halla sido almacenado en el depósito exitosamente.
- Una etiqueta puede asociarse con un canal para dar una descripción textual del servicio indicado por el canal.

Los recursos en el depósito pueden ser referenciados por más de un canal. Un recurso esta presente en el depósito si uno o más canales lo referencian. La figura 309 muestra un ejemplo de como pueden compartirse los recursos almacenados en el depósito.

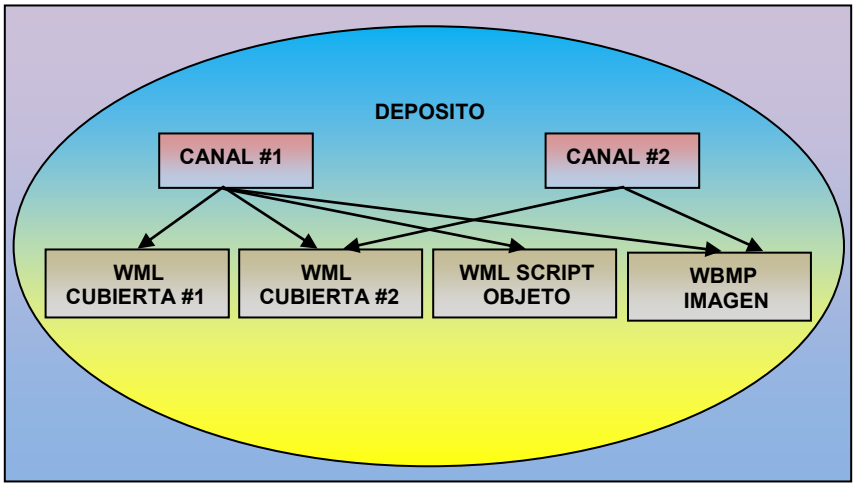


Figura 309

6.6.8 CARGA DEL CANAL

El canal puede ser empujado dentro del depósito o cargado dentro de este en el momento que el agente de usuario lo quiera recuperar. Los canales son identificados particularmente por el valor del atributo channelid. Si el channelid de un nuevo canal tiene un valor el cual es idéntico al de un canal que a sido cargado con anterioridad, la información del canal nuevo toma precedencia sobre la información anterior (sobre escribe). En el caso que ambos elementos del canal viejo y nuevo contengan eventos globales comprometidos, los viejos eventos podrán ser remplazados por los nuevos, siempre y cuando el valor del atributo eventid sea idéntico. Si el atributo eventid de un nuevo elemento del canal tiene un valor el cual es idéntico al de un canal que ha sido previamente cargado, el nuevo canal remplaza al anterior siempre y cuando los valores del atributo channelid del nuevo y del viejo canal sean idénticos. Esto implica que los eventos globales viejos comprometidos anteriormente son remplazados. La instalación de un canal involucra los siguientes pasos:

1.-Siempre carga un recurso señalado por un canal excepto cuando el recurso ya existe en el depósito y tanto el recurso almacenado e indicado son igualmente frescos.

- Si la carga de todos los recursos “exitosos” y una URL “exitosa” es especificada por el canal, un mensaje es enviado al servidor (empleando la URL exitosa). La petición de la URL “exitosa” asegura al servidor que el canal esta próximo a ser activado. La respuesta a la solicitud de la URL “exitosa” puede contener un mensaje al usuario final con la información sobre el nuevo servicio.
- Por encima de una recepción “exitosa” de respuesta a una URL “exitosa”, o si no existe una URL “exitosa” para el canal, este es activado (se hace visible al agente de usuario WTA). El canal es guardado en el depósito. Todos los nuevos recursos son guardados en el depósito. Todos los recursos son actualizados con los nuevos atributos como lo indicado por el canal.

2. De otra manera, si la carga falla por cualquier razón (incluyendo que la URL “exitosa” no pueda ser accedida) el canal (junto con algún nuevo recurso) es descartado. Si el canal previo tiene la misma identificación (desactualizada o no), este (y los recursos indicados) debe ser inalterado.

- Si el canal tiene el atributo “fallido”, la URL “fallida” debe ser solicitado. La solicitud para el URL “fallido” informa al servidor que la instalación del canal fallo. Si el mensaje de respuesta fallo al ser entregado entonces el agente de usuario debe proceder como si el URL “fallido” no existiese en el canal.
- Si la URL “fallida” no existe en el canal, el agente de usuario debe presentar un mensaje apropiado de error al usuario final por ejemplo “fallo la instalación del canal”.

6.6.8.1 DESCARGA DEL CANAL

Cargando un canal vació se realiza la descarga del canal. Para descargar un canal con una cierta identidad, se debe cargar un canal vació con la misma identidad, posteriormente se procede a remover el canal vació del depósito.

6.6.8.2 ALMACEN GC.

Es ocasionalmente necesario buscar espacio en el depósito. Esto debe hacerse mediante el siguiente proceso:

- Remover todos los canales vacíos.
- Remover todos los canales que estén desactualizados (viejos).
- Remover todos los recursos que no estén referenciados por un canal.

6.6.8.3 INSTALACIÓN DEL CANAL

Un cliente que soporta el formato de contenido del canal debe ser capaz de instalar un canal en cualquier momento. El canal debe ser procesado tan pronto como el cliente este desocupado (no este ejecutando ningún servicio, por ejemplo). Los canales pueden ser cargados en el depósito usando cualquier mecanismo de transferencia de contenido estándar apropiados para el uso de tipos específicos de redes y portadores. Los métodos de descarga del canal pueden incluir:

- Retornando el canal como parte de una respuesta a la solicitud del URL estándar (método GET o POST).
- Empujando el canal a cualquier dispositivo directamente o usando una indicación de servicio (SI).

6.6.8.4 TERMINACIÓN DEL CANAL INSTALADO

Cuando todos los recursos han sido cargados y el canal este listo para ser activado entonces la URL “exitosa” es solicitada del servidor. La respuesta le dice al cliente que el servidor ha sido informado acerca de los servicios que están actualizados. Entonces el cliente activa el canal (se hace visible para el agente de usuario). Si ocurre cualquier error durante el proceso de instalación del canal, la instalación debe ser terminada. El contenido indicado por la URL “fallida” deberá ser cargado. Si el URL “fallido” no esta presente en el canal, o la respuesta para este falla, el cliente deberá notificarle al usuario final con un apropiado mensaje de error.

Ejemplo de instalación de un canal

En esta sección se dan dos ejemplos de cómo la instalación de un canal puede verse. El proceso de instalación será ilustrado (por razones prácticas) desde el punto donde el canal ya ha sido introducido en el cliente. El primer ejemplo nos presenta la instalación exitosa del canal. La figura 310 muestra algunas posibles situaciones cuando un canal no puede ser instalado debido a una condición de error.

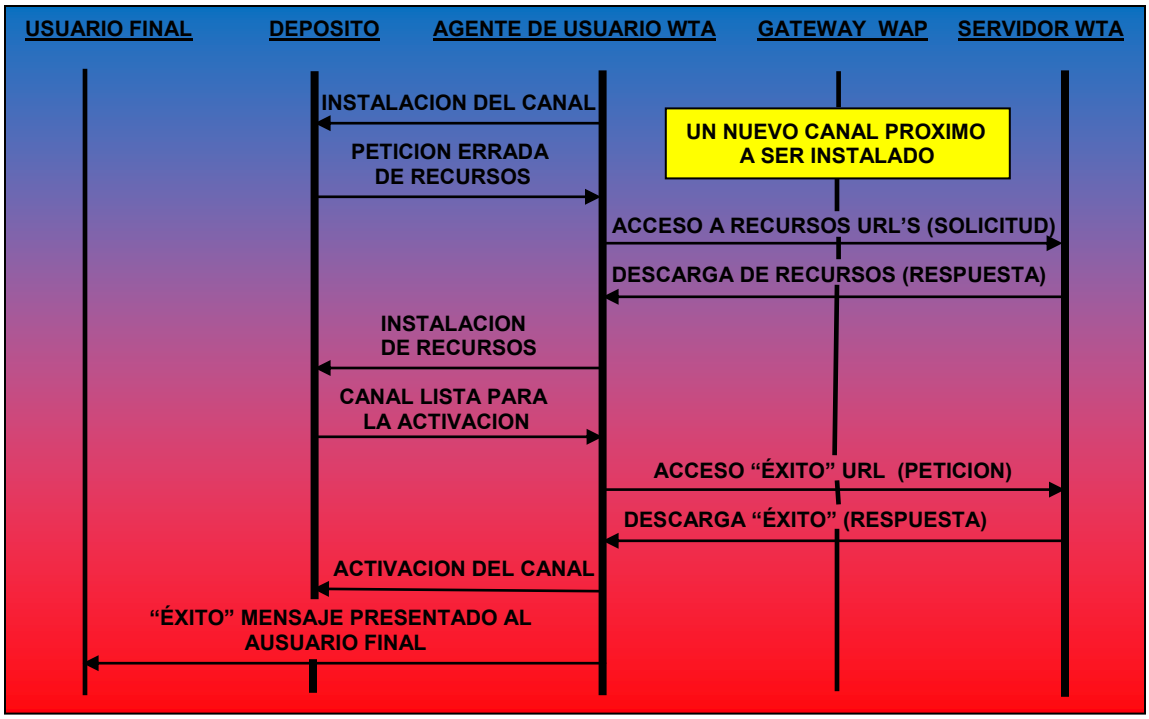


Figura 310

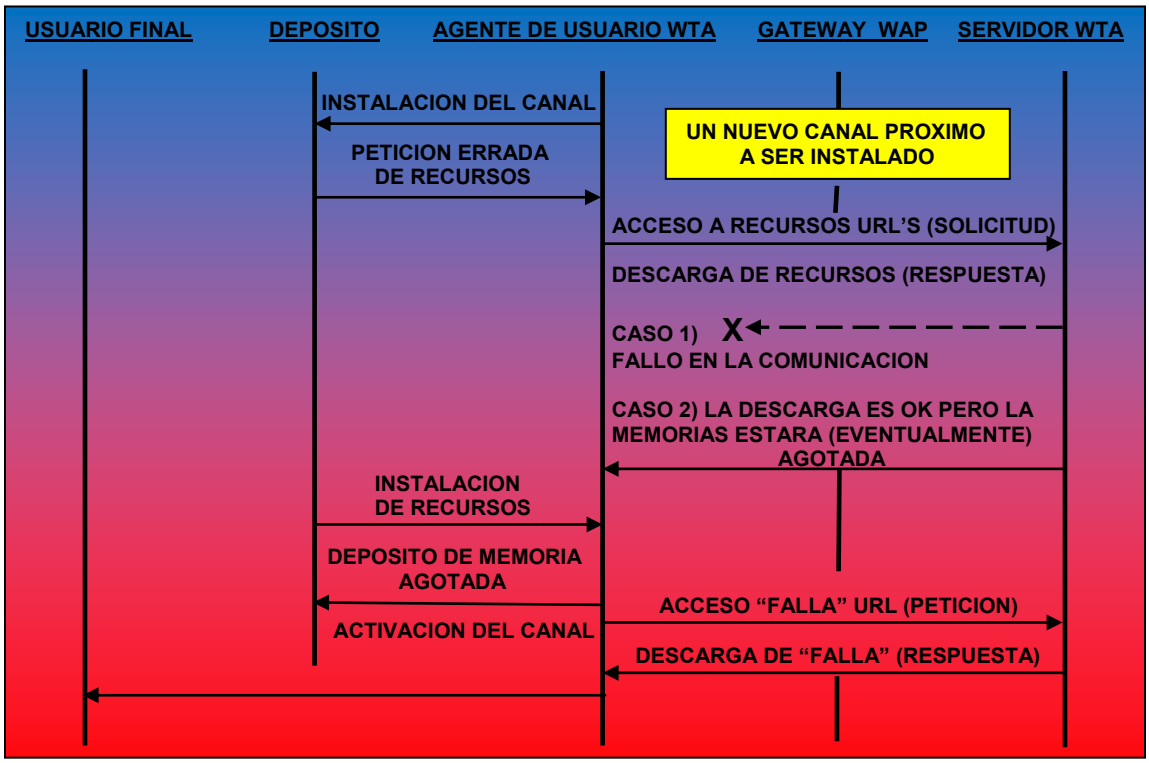


Figura 311

6.6.9 POLITICAS DE ACCESO AL DEPÓSITO

El depósito es programado (por el desarrollador del servicio WTA) para contener los recursos que en otros casos pueden necesitar ser recuperados desde la red. Los recursos en el depósito (no incluyen los canales) son almacenados junto con su URL original. Esto implica que una implementación debe de verificar el depósito para un recurso específico previamente a requerirlo de la red.

6.6.10 SERVICIOS Y BENEFICIOS

El protocolo WAP soporta la fusión de dos tecnologías poderosas: Internet y telefonía móvil. Esta reunión de tecnologías permite ofrecer una gran cantidad de nuevos servicios inalámbricos para uso personal y de negocios. WAP ofrece una nueva dimensión a Internet "La movilidad". Con un teléfono móvil o con una agenda electrónica que soporte la tecnología WAP podrás adquirir boletos, ordenar una pizza o revisar tus cuentas bancarias en cualquier momento. En tu trabajo, en el deportivo o de vacaciones. La información estará ahí para cuando tú la necesites. Podrás buscar información, noticias, las condiciones del clima, tipos de cambio y más para mantenerte actualizado. También podrás tener acceso a aplicaciones de entretenimiento como juegos o chats. Pero WAP no sólo consiste en hacer a Internet móvil. También habrá servicios como bajar agendas telefónicas completas o el manejo de las llamadas entrantes y salientes que harán de la telefonía móvil un medio aún más fácil de usar. WAP es un estándar global desarrollado para poder ofrecer los servicios de Internet a los usuarios móviles. A pesar de que WAP está basado en la tecnología de Internet, WAP e Internet se encuentran lado a lado. Una persona o una empresa que tiene un Sitio de Internet puede hacer disponible la información para un usuario móvil mediante la transformación de páginas de Internet a página de WAP.

Beneficios

Usuarios

WAP ha sido diseñado para proporcionar servicios de valor añadido al usuario. Debido a su diseño e implementación WAP proporciona:

- Los teléfonos celulares son las herramientas dominantes de las comunicaciones y al mismo tiempo, Internet es una plataforma privilegiada para la información. Al adoptar un protocolo común, el usuario final es el que más se beneficiará ya que se le proporcionarán más servicios de valor agregado, los cuales serán de fácil acceso y fáciles de utilizar directamente desde cualquier dispositivo inalámbrico. A su vez, los servicios orientados hacia la telefonía serán más fáciles de entender y utilizar.
- Todas las ventajas de Internet
- Una interfaz de usuario estándar.
- Manejo sencillo de servicios de telefonía.
- Accesos a redes de empresas y contenidos de Internet en cualquier sitio.
- Servicios totalmente nuevos como los servicios dependientes de la localización.
- Personalización de los servicios simplificada.
- Gran disponibilidad de unidades

Operadores

Los operadores pueden diferenciarse de sí mismos al lanzar servicios especiales, como por ejemplo, servicios bancarios, compra-venta de acciones y servicios de directorio. Adicionalmente, el protocolo permite personalizar diferentes menús dentro de los teléfonos celulares. Esta personalización se podrá efectuar en el aire. Esto incrementará los ingresos y adquirir nuevos clientes, mientras que al mismo tiempo reducirá los costos excesivos. La industria de las telecomunicaciones podrá evitar costos e inversiones solapados, si existe una plataforma abierta, común y una herramienta para la mensajería inalámbrica. WAP es un paso importante en la

evolución de los servicios de datos inalámbricos/ mensajería, lo cual aumentará el uso de datos en las redes inalámbricas.

- Nuevas fuentes de ingresos.
- Mayor satisfacción y lealtad del cliente.
- Formato y protocolos estandarizados.
- Soporte de una amplia gama de tipos de terminal móvil.
- Tecnología de larga longevidad que admite GPRS y UMTS.
- Flexibilidad.
- Solución completa de WAP que incluye la integración de la red.
- Personalización del servicio con un aspecto típico agradable.

Desarrolladores de aplicación y contenido

Ya que WAP fue desarrollado por una organización independiente, los desarrolladores estarán en el mismo nivel, tanto los unos como los otros. Ellos pueden crear o escribir una única aplicación que correrá en todas las redes de los operadores, los protocolos de transporte y los dispositivos inalámbricos. Por primera vez, los desarrolladores pueden obtener acceso unificado a toda la comunidad global de usuarios. Esto significa que la unión que proporciona Internet al mundo en línea, puede ahora ofrecerse y hacerse disponible para la comunidad inalámbrica. Las aplicaciones pueden desarrollarse beneficiándose totalmente de la interfaz del usuario final, debido a que el navegador WAP en cada dispositivo inalámbrico será capaz de controlar como el contenido se mostrará y visualizará. Además, los desarrolladores no tienen por que preocuparse ya que WAP es un estándar abierto con una ruta de migración hacia el futuro.

Servicios

WAP mejorará muchas de las aplicaciones disponibles hoy en día, al igual que dará pie a una gama de nuevos servicios innovadores de valor agregado. Las aplicaciones posibles están solamente limitadas por la imaginación. Los tipos de aplicaciones que se beneficiarán de WAP incluyen:

- Servicio al cliente y aprovisionamiento
- Notificación de mensajes y administración de llamadas correo electrónico
- Servicios de telefonía de valor agregado
- Servicios de mapas y ubicación
- Alertas y advertencias en cuanto al tiempo y el tráfico servicios de noticias, deportes e información
- Comercio electrónico, transacciones de Bolsa y servicios bancarios
- Servicios de libreta telefónica y directorio
- Aplicaciones de Intranet corporativo

WAP viajero

Un ejemplo donde WAP puede agregar valor es en la industria de viajes y turismo. Con la creciente competencia, la globalización y los cambios en las preferencias de los clientes, se presentan nuevos retos. Las aerolíneas luchan por asegurar la lealtad de los clientes, mientras reducen los costos de los pasajes. Las compañías de transporte público también valoran la lealtad, y buscan la reducción de costos de "taquilla de información". La tecnología WAP ayuda a enfrentar tales retos al ofrecer una gama de servicios de bajo costo a través de Internet. Una nueva generación de viajeros equipados con celulares que quieren hacer arreglos y reservar boletos, cuando y donde sea más conveniente. Los viajeros podrán tener acceso a una información completa relacionada a viajes y transporte, pues las formas electrónicas inteligentes, requerirán sólo un mínimo de información, pudiéndose verificar automáticamente los posibles errores que puedan contener las entradas de datos efectuadas por el usuario antes de que la solicitud sea enviada a las diferentes compañías de servicios.

Es un hecho. Las comunicaciones nos unen cada vez más. Ya Internet lo logró, y la tercera generación de celulares promete hacerlo aún más. ¿Desaparecerán las PC's para dar paso a estos teléfonos inteligentes que nos permitirán comprar hasta un boleto para entrar al cine? Muchos dicen que no, otros ya lo ven como un hecho. Sea como sea, nos acercamos cada vez más a un mundo inalámbrico. Ya existe un protocolo que permitirá la sincronización entre todos los dispositivos que conocemos como PDA's, e incluso los teléfonos celulares. Se trata de Bluetooth. La meta es unificar todos los componentes de red personal, hasta los electrodomésticos, en un sistema que facilite la interconexión entre cada uno de ellos. Una microred de 30 metros, 2.5 GHz de velocidad, operando con direcciones definidas, es uno de los sistemas que se estudian. Ya Nokia, Ericsson, IBM y 3Com ya desarrollaron productos que soporten el protocolo. Se especula que el gran boom de esta onda inalámbrica será el comercio móvil o el m-commerce. Ya el e-commerce lo es en Internet, así que sólo basta esperar para ver cómo hará su entrada este nuevo modelo de negocios. En un abrir y cerrar de ojos cambiaremos el "click" por el "send".

6.6.11 HERRAMIENTAS

Dentro de las herramientas internas de WAP se encuentra las siguientes componentes en su arquitectura y son; las Terminales, Gateway y el Servidor el cual utiliza un lenguaje de marcación llamado **WML** para su funcionamiento.

- **Terminales**: para poder acceder y visualizar las diferentes páginas de forma remota se dispone de una terminal adecuada. Este tipo de terminal puede ser un teléfono móvil que soporte WAP; PDA's ó handhelds conectados a alguna tarjeta que permita enviar y recibir datos vía radio. Las terminales presentan las siguientes características:
  Lleva incorporado un microbrowser, que es el que realiza la traducción de las paginas WML, y las presenta en pantalla. Interpreta los hipervínculos mediante los que el usuario quiere saltar a otras páginas. Se encarga de generar la secuencia de acciones que lleva consigo un posible código WML Script. Por tanto es el encargado de que podamos realizar la navegación a través de la terminal móvil. El estándar permite un alto grado de libertad a la hora de implantar los micronavegadores. Esta variabilidad implica diferencias en la presentación de las páginas. No todas las terminales se ajustan al estándar, lo que hace difícil el desarrollo de aplicaciones válidas para cualquier equipo. La pantalla tiene limitaciones debido a su reducido tamaño, a su resolución y a la calidad. Ello destierra el uso de imágenes en color o con gran resolución. No se ha logrado facilitar la configuración de la terminal para el acceso a la red basada en WAP ya que:
  - Es Complejo de modificar por el usuario.
  - Las configuraciones para roaming es diferente de la configuración para otro país.
  - La interfaz de usuario presenta ciertas características a la hora de diseñar aplicaciones WAP. Bien sea la baja reusabilidad del teclado, el número de botones, el número de líneas y caracteres que pueden visualizarse sin realizar un scroll por la página, etc.
  - Presenta una amplia interoperabilidad con otros servicios y portadores.

- El **gateway** es el punto de entrada para los usuarios móviles a Internet, proporcionando la correspondencia de protocolo IP y WAP, codificando y decodificando para conseguir una transferencia de datos eficiente y un acceso por móvil. Los gateway presentan las siguientes características:
  - Adapta los protocolos WML (ligero) y HTML (web), descodificando los datos provenientes de la terminal y codificando aquellos que vienen del servidor o traduciendo los contenidos de HTML a WML si es necesario.
  - Puede presentar interoperabilidad ineficiente con terminales y aplicaciones. No siempre adapta los contenidos del mismo modo.
  - Garantiza la conexión segura.
  - No existe interconexión de gateways.
  - Costo: es el de una llamada de datos (circuitos conmutados)

- Asume la responsabilidad de realizar el auto-provisioning, que consiste en que un usuario no necesite estar dado de alta para acceder al servicio WAP. Basta con que llame para que la primera vez se conecte, y el sistema lo registre.
- Se encarga de interpretar las URL's y redireccionar las peticiones de los usuarios.

- El **Servidor** presenta las siguientes características:
  - Almacena los contenidos que se ofrece en la web.
  - Los contenidos almacenados pueden estar en formato HTML o WML, en función del interés del proveedor de contenidos y del proveedor de servicios que estén disponibles en WAP o únicamente en acceso a la Web.
  - Estable su plan de negocio sobre la publicidad buscando generar el máximo tráfico posible a través de sus páginas.
  - Las solicitudes procedentes de los dispositivos móviles se envían en forma de comandos del lenguaje de marcación inalámbrico (WML) al gateway. La solicitud de WML se convierte al lenguaje de marcación de hipertexto (HTML) y se envía a través de http al servidor de aplicaciones de Internet.
  - El lenguaje WML, conforme al ya existente XML, se basa en etiquetas y se diseño para trabajar sobre un hardware con serias limitaciones en sus prestaciones, un ancho de banda pequeño y terminales móviles con escasa capacidad de entrada y salida.
  - Estructura los datos en cartas, que corresponde en principio a lo que se presenta en pantalla, agrupadas en barajas. La idea es que la terminal en sí sea transparente a WML, para darles más posibilidades de desarrollo a los fabricantes y en sus prestaciones su característica esencial será la de ser muy ligero, texto e imágenes, entrada de datos, lista de opciones, códigos, comandos del tipo Get, Uso de varios idiomas, Gestión de Estado y Contexto, que permita pasar de una baraja a otra las variables más importantes, sustituir variables y gestión del Cache y adaptarse a las restricciones de presentación y ejecución de instrucciones del usuario.
  - Por lo tanto las herramientas externas utilizadas por un teléfono móvil con WAP son las siguientes, tabla 42.

Teléfonos Móviles con WAP
Comunicación sin cable
Cobertura limitada a cada Compañía
Buzón de mensajes
Pago fijo de renta mensual
identificador de llamadas
Operabilidad sencilla
Mayor seguridad

Tabla 42

6.6.12 MERCADOS POTENCIALES

La comunicación móvil y la comunicación de datos son dos de las áreas de crecimiento más rápido en la industria de las comunicaciones. En particular la comunicación de datos móviles, que incluye Internet inalámbrica, lleva bastante ímpetu. Los medios de comunicación están manteniendo un ojo vigilante en la evolución de datos inalámbricos, y operadores y distintos tipos de empresas han puesto la comunicación de datos inalámbricos a la cabeza de su orden del día. La comunicación de datos inalámbricos combina la comunicación móvil y la comunicación de datos dando fácil acceso a los consumidores a información pertinente en Internet o intranets por teléfonos móviles, buscapersonas u otros dispositivos inalámbricos. Los operadores ven la comunicación de datos inalámbricos como una oportunidad de crear servicios innovadores por encima de redes e inversiones existentes. El hacer esto les dará un medio de diferenciarse por ejemplo para reforzar su imagen comercial, atraer nuevos abonados y aumentar el volumen de

tráfico por abonado. Las empresas están mirando cada vez más por maneras de aumentar la productividad de los empleados. Los datos inalámbricos permitirían que los profesionales tengan acceso a datos empresariales, tales como correo electrónico, estado de la producción, listas de precios, y otra información crítica para hacer negocios mientras que estén fuera de la oficina. Segmentos verticales específicos, tales como instituciones financieras, han expresado interés en datos inalámbricos como una manera de distribuir servicios. En este contexto los datos inalámbricos podrían mejorar su imagen total y aumentar la disponibilidad de servicios por un canal de distribución de bajo costo y en rápido crecimiento. Estas necesidades e iniciativas han creado "tecnologías ojeadoras por teléfono", tales como el Protocolo de Aplicaciones Inalámbricas, o WAP.

6.6.12.1 NUEVAS FUNCIONES COMERCIALES PARA OPERADORES

El mercado de Internet móvil esta siendo formado por el cruce y la fusión de las industrias de las telecomunicaciones inalámbricas y de Internet. En esta esfera, que todavía esta muy caracterizada por la transición, se cambian las reglas del juego y se han alterado varias cadenas de valores tradicionales. Por lo tanto, y al entrar en esta esfera, son muchos los jugadores que se sienten poco seguros de su función. Al evaluar cuidadosamente la situación se han identificado un número de modelos comerciales emergentes que los operadores pueden adoptar para posicionarse en este mercado turbulento. A pesar de que los modelos comerciales de Internet móvil son similares a los de Internet, se han identificado algunas diferencias:

- La función de portales a Internet móvil es más destacada que la de portales a Internet tradicional.
- Las clases emergentes de servicio tendrán mas impacto en el éxito o el fracaso de Internet móvil que las tecnologías habilitadoras de movilidad.
- Internet móvil representa una oportunidad importante para el comercio electrónico (e-commerce).

Gracias a sus importantes ventajas, tales como grandes bases de clientes, puertas entre redes móviles e Internet, sistemas de facturación y de cuentas, y control de terminales y redes móviles, están bien posicionados los operadores inalámbricos para tener éxito en la industria emergente de los datos inalámbricos (figura 312 y tabla 43). Los operadores móviles que eligen de sacar provecho de su posición en la industria emergente abrirán portales que incorporaran el comercio electrónico y centros de comunicación. Al hacer esto y en particular, al añadir servicios habilitados a WAP que cumplen con las necesidades de los usuarios finales los operadores pueden:

- Diferenciarse de la competencia.
- Reducir la agitación, gracias a perfiles de usuario personalizados.
- Mejorar su imagen comercial total.
- Sacar provecho de grandes aumentos en el tráfico de comunicación de datos.

6.6.12.2 UNA APUESTA SEGURA

WAP es una norma abierta que ha sido perfeccionada lo más posible para ambientes móviles con ancho de banda limitado y pantallas pequeñas, haciendo que sea el primer habilitador principal de una instalación realmente amplia de datos inalámbricos. Varias tecnologías están compitiendo para llegar a ser la norma dominante para información inalámbrica y servicios Internet, pero numerosos indicadores hacen pensar que WAP prevalecerá: WAP representa una tecnología superior que ha sido perfeccionada lo más posible para ambientes móviles. WAP ha ganado el apoyo de operadores, suministradores de telecomunicación y comunicación de datos, y una variedad de empresas. Además, WAP no compite directamente con otras tecnologías. Las principales tecnologías que contienden son Windows CE (Microsoft / Wireless Knowledge), Palm VII (Palm Computing), I-Mode (NTT), y el SIM-Toolkit (Schlumberger). El líder indiscutido de hoy entre estos contendientes es I Mode, que ya tiene varios millones de usuarios finales y una amplia cartera de contenido. El objetivo de WAP es de dar una norma abierta para acceso por medio de un dispositivo móvil a Internet o a intranets. Debido a que WAP ha sido perfeccionado lo más posible para ambientes móviles, hace este un uso óptimo de condiciones reducidas, inclusive pantallas pequeñas, memoria de dispositivo limitada y disponibilidad de ancho de banda limitada.

WAP funciona además con redes existentes y será compatible con normas futuras para sistemas inalámbricos de tercera generación y XML/XHTML. El WAP Forum ha establecido relaciones con el Instituto Europeo de Normas de Telecomunicaciones (ETSI), la Fuerza de Tareas de Ingeniería de Internet (IETF), y el Consorcio World Wide Web (W3C). WAP goza del mayor apoyo de todas las tecnologías contendientes. La mayor parte de los jugadores principales en todos los segmentos afectados (fabricantes de microteléfonos, operadores, proveedores de contenido, desarrolladores de aplicación e integradores de sistema) apoyan a WAP. Algunos de los miembros principales del Forum, además de Ericsson, incluyen a Alcatel, AT&T, IBM, Microsoft, Motorola, Nokia, Oracle, Phone.com, T-Mobil, y Sun Microsystems.

6.6.13 RÁPIDA PENETRACIÓN EN EL MERCADO

Se espera que el reciente lanzamiento de varios portales WAP y la entrada al mercado de terminales WAP den a WAP una rápida penetración en el mercado. La penetración en el mercado que se ha pronosticado esta basada en los cálculos de penetración móvil, una esperanza de duración de vida de tres años para teléfonos que no son WAP, una esperanza de duración de vida de dos años para teléfonos WAP, y porcentajes de teléfonos habilitados a WAP que se venden por sistema. Al principio no todos los usuarios de teléfonos habilitados a WAP tendrán abonos WAP activos. Se espera que el porcentaje de usuarios WAP que abonan a servicios financieros basados en WAP sea igual al de usuarios que usan Internet para servicios similares. Se espera que aproximadamente un 50 % de todas las transacciones financieras por medio de WAP sean servidas por un gateway WAP de propiedad de instituciones financieras. Se espera que como un 40 % de todos los usuarios de WAP usen sus teléfonos WAP en el trabajo. Casi un 15 % de los teléfonos WAP que se usan en el trabajo serán servidos por un gateway WAP de propiedad de empresas.

6.6.14 SEGURIDAD WAP.

Seguridad es un concepto que se usa a menudo con escaso rigor. Esto es así porque, en lenguaje natural, el concepto de seguridad es a menudo equivoco. Cuando hablamos de seguridad en tecnologías de información, estamos hablando de muchas cosas a la vez: que nadie nos robe a modifique los datos, que nadie nos suplante, que nadie acceda a donde no debe, etcétera. Los estándares ISO donde se define una arquitectura de seguridad dentro de la que existe una serie de servicios de seguridad. Según esta especificación, para proteger las comunicaciones es necesario dotar a las mismas de los siguientes servicios:

- **Autenticidad de la Entidad par**: Mediante este servicio se verifica la fuente de los datos. La autenticidad puede ser de la entidad origen, de la entidad destino o de ambas a la vez.
- **Control de Acceso**: Este servicio verifica que los recursos son utilizados sólo por quien tiene derecho a hacerlo.
- **Confidencialidad de los datos**: Con este servicio se evita que se revelen, deliberada o accidentalmente, los datos de una comunicación.
- **Integridad de los datos**: Este servicio verifica que los datos de una comunicación no se alteren, esto es, por los datos recibidos por el receptor coincidan con los enviados por el emisor.
- **No repudio**: Proporciona la prueba, ante una tercera parte, de que cada una de las entidades ha participado, efectivamente, en la comunicación. Puede ser de dos tipos:
    - Con prueba de origen o emisor: El destinatario tiene garantía de quien es el emisor concreto de los datos.
    - Con prueba de entrega o receptor: el emisor tiene prueba de que los datos de la comunicación han legado íntegramente al destinatario correcto en un instante dado.

Por tanto, cuando hablemos de seguridad, debemos especificar cuales son los servicios de seguridad que requiere nuestro sistema y como vamos a garantizarlos.

6.6.14.1 LA SEGURIDAD EN INTERNET

En el mundo Internet se utiliza el protocolo **SSL (Secure Soskets Layer**, creado por Netscape Communications), que dispone un nivel seguro de transporte entre el servicio clásico de transporte en Internet (TCP) y las aplicaciones que se comunican a través de él, como garante de la seguridad en el acceso a servicios "delicados", como compra (comercio electrónico) o transacciones bancarias. El modo de funcionamiento de SSL es bastante sencillo y se compone de dos partes diferenciadas:

- **Handshake Protocol** (algo así como el apretón de manos): Se encarga de establecer la conexión, verificando la identidad de las partes (opcionalmente) y determinando los parámetros que se van a utilizar posteriormente (fundamentalmente se trata de acordar cual va ser la clave simétrica que se utilizará para transmitir los datos durante esa conexión, para lo cual se utiliza criptografía de clave pública).
- **Record Protocol**: Comprime, cifra, descifra y verifica la información que se transmite tras el inicio de la conexión (handshake).

No obstante, de lo señalado anteriormente se deduce que SSL, como protocolo de seguridad de transporte sólo proporciona alguno de los servicios de seguridad necesarios:

- **Confidencialidad**: La información que circula entre el cliente (una navegador habitualmente) o el servidor que actúa de frontal del servicio se cifra utilizando criptografía de clave simétrica (con una clave de sesión acordada en el handshake).
- **Autenticación**: Las partes que mantienen la comunicación se autentican mediante certificados basados en criptografía de clave pública. Esto no es siempre así, siendo lo más habitual que sea únicamente el servidor el que se autentica mediante un certificado digital.
- **Integridad**: La integridad de los datos transmitidos se asegura usando códigos de integridad (MAC) cálculos mediante funciones de hash (SHA ó MD5).

El uso de SSL como soporte de compras o transacciones seguras es muy habitual. En el caso de una compra en línea, es habitual facilitar los datos de tarjeta de crédito (número, fecha de caducidad, impresión) sobre una conexión protegida con SSL para su procesado por parte de un TPV virtual proporcionado por un banco. Este modelo adolece de un grave problema. No protege al comercio contra el repudio de la transacción, puesto que no existe forma de demostrar que es el propietario de la tarjeta el que ha efectuado la compra. Para frenar este problema algunas compañías se unieron para crear **SET (Secure Electronic Transactions)** para garantizar la irrenunciabilidad en el pago electrónico utilizando tarjetas de crédito. Otra forma de garantizar la irrenunciabilidad es utilizar SSL como capa de transporte seguro e implementar un protocolo a nivel de aplicación, que mediante firmas digitales, garantice la irrenunciabilidad de las operaciones.

6.6.14.2 LA SEGURIDAD EN EL ENTORNO WAP

El protocolo WAP, prevé mecanismos de seguridad independientes de la red de transmisión que se use, para fomentar el uso del comercio electrónico desde el móvil. Por tanto, podemos operar en nuestra cuenta bancaria, invertir en bolsa en tiempo real o comprar con total seguridad desde nuestro teléfono móvil. Aunque WAP fue diseñado para utilizar cualquier tecnología móvil existente en la actualidad, la más utilizada por WAP en nuestro entorno es GSM. GSM es una tecnología digital de acceso aéreo que incluye mecanismos de cifrado de la comunicación entre el terminal móvil y la BTS (Estación base). Se considera comúnmente que los mecanismos de cifrado de GSM no son suficientes para garantizar la seguridad de cualquier transacción conducida mediante WAP, debido no sólo a la debilidad de los algoritmos como a la porción de camino protegidas (exclusivamente desde la terminal móvil a la BTS). WAP se articula como una arquitectura en capas en la que la capa de trasporte se denomina **WDP (Wireless Datagram Protocol)**, sobre esta capa de transporte se sitúa una capa opcional de seguridad denominada **WTLS (Wireless Transport Layer Security)**. Del mismo modo que TCP/IP se a consolidado un estándar de facto, el ya conocido SSL (Secure Sockets layer), o su evolución **TLS (Transport Layer Security)**, como capa de seguridad entre los protocolos de aplicación (HTTP, FTP, SMTP, etc.) y la capa de

transporte, la especificación WAP ha definido WTLS. Este protocolo se ha diseñado siguiendo una serie de criterios.

- Debe soportar datagramas.
- Debe soportar portadoras de ancho de banda variopinto.
- Debe soportar periodos de latencia, potencialmente largos.
- La capacidad de memoria y procesamiento de las terminales puede ser pequeña.

En definitiva, TLS y WTLS son protocolos equivalentes (en múltiples partes de la especificación de WTLS, se copia literalmente la de TLS), siendo patente que la intención de los autores del protocolo TLS y añadir soporte a datagramas, optimizar el tamaño de los paquetes transmitidos y seleccionar algoritmos rápidos entre los permitidos. En cuanto a su estructura, tanto SSL – TLS como WTLS incluye una fase de handshake en la que se negocian los algoritmos utilizados, se intercambian claves y se verifican certificados, seguida de una fase de registro (en la que garantiza también la integridad de los mensajes intercambiados). Del mismo modo que con SSL – TLS, se han definido las siguientes características:

- **Integridad de los datos**: Se asegura que los datos intercambiados entre la terminal y el gateway WAP no han sido modificados.
- **Confidencialidad de los datos**: Se asegura que la información intercambiada entre la terminal y el gateway WAP no puede ser entendida por terceras partes que puedan interceptar el flujo de datos.
- **Autentificación**: El protocolo contiene servicios para autentificar la terminal y el gateway WAP.

Las implementaciones de WTLS pueden soportar diferentes características, definiéndose las siguientes clases.

- **Clase 1**: Clase básica en la que no existe autentificación ni del cliente (terminal WAP) ni del gateway WAP.
- **Clase 2**: Lo mismo que la clase 1, pero añadiendo autentificación del gateway WAP (este nivel es el equivalente al implementado usualmente con SSL en Internet).
- **Clase 3**: Igual que la clase 2, pero añadiendo autentificación de terminal WAP.

Resumen de las características tabla 43.

Características	Clase 1	Clase 2	Clase 3
Intercambio de cave	Obligatorio	Obligatorio	Obligatorio
Certificados de servidor	Opcional	Obligatorio	Obligatorio
Certificados de cliente	Opcional	Opcional	Obligatorio
Compresión		Opcional	Opcional
Cifrado	Obligatorio	Obligatorio	Obligatorio
MAC	Obligatorio	Obligatorio	Obligatorio
Interfaz con tarjetas Inteligentes		Opcional	Opcional

Tabla 43

Características de las clases

- La v3, pero también certificados WTLS y X.s diferencias que existen entre SSL-TLS y WTLS son:
  - La negociación se hace sobre datagramas WDP (equivalentes a los datagramas de UDP), no sobre conexiones fiables TCP, puesto que no existe TCP en WAP.
  - Se permite una autentificación basada en un secreto compartido. Esto permite que las terminales WAP puedan prescindir de hardware criptográfico.
  - Existen mecanismos de negociación optimizados para mejorar el tiempo de transacción segura en la que el servidor busca el certificado del cliente por su cuenta, sin esperar que dicho certificado viaje a través de la red móvil.

- Criptográficamente las innovaciones son mínimas. La más es que admite la utilización de algoritmos criptográficos basados en curvas elípticas, que ofrecen ventajas en cuanto a memoria y prestaciones. Por lo demás sigue soportando los algoritmos ya conocidos: DH y RSA para intercambio de claves, RC5, DES, 3DES e IDEA para cifrado simétrico y MD5 y SHA para generación de MAC's. Además, la especificación permite el uso de certificados X.968.
- Se puede concluir que WTLS no es más que TLS (o SSL) modificado para permitir la utilización de terminales WA como agentes de usuario. Si bien estas modificaciones lo hacen también más vulnerable, es de prever que posteriores versiones del protocolo lo hagan más fiable y una herramienta totalmente eficaz de seguridad de transporte en el tramo entre la terminal y el gateway.

Los principales gateways WAP soportan WTLS, menos de clase 2 (con autentificación de gateway). Entre ellas se encuentran:

- UP. Link de phone.com
- El gateway WAP de Ericsson
- WAP Server de Nokia
- El gateway WAP de SAS

La primera debilidad que presenta el modelo de seguridad WAP es la existencia de dos zonas de seguridad, fruto de la existencia de dos dominios tecnológicos diferentes. Conectados mediante el gateway WAP, se deduce que mientras que en el dominio WAP existe seguridad en el transporte mediante WTLS, en el dominio TCP/IP esta protección en el transporte se consigue utilizando SSL. El gateway debe ser capaz de hablar WTLS con el dispositivo móvil y SSL con el proveedor de contenidos, la conversión de protocolos no se hace en este nivel de transporte, si no que se hace en un nivel más alto. Esto significa que es preciso un proceso de descifrado y recifrado en el gateway WAP. En la figura 312 hay dos partes diferenciadas en el modelo de seguridad WAP. En la parte derecha del dibujo, el gateway WAP sencillamente usa SSL para establecer comunicación segura con el servidor web, asegurando la privacidad, integridad y autenticidad del servidor.

En la parte de la izquierda, el gateway recoge los mensajes codificados con SSL del servidor web y los transforma para transmitirlo usando WAP y la capa de seguridad WTLS. Las peticiones desde el teléfono hacia el servidor web, recorren el camino inverso, por tanto el gateway actúa de gateway entre las capas WTLS y SSL.

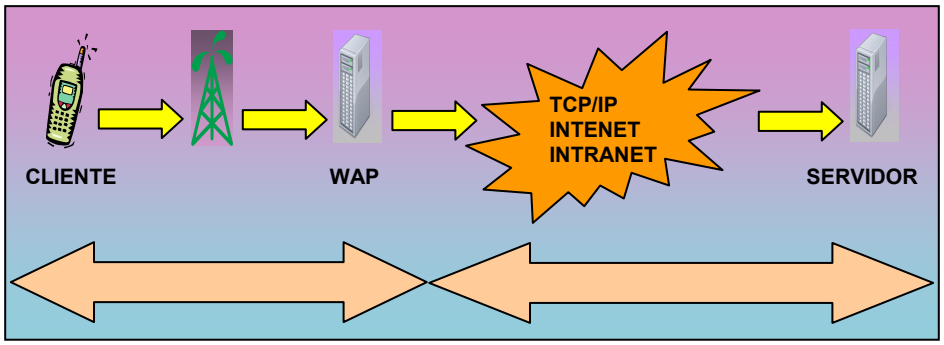


Figura 312

La necesidad de cambio de SSL a WTLS viene impuesta por la naturaleza de las comunicaciones inalámbricas: ancho de banda reducido con alta latencia. Dado que SSL se diseño para ordenadores de escritorio con capacidad superior a la de un teléfono móvil y con mayor ancho de banda y menor latencia. Si se intentara incluir SSL en los teléfonos móviles, esto dispararía los precios de las terminales frenando el crecimiento de la industria WAP. WTLS: Se diseño específicamente para conseguir un nivel de seguridad suficiente, sin necesitar una gran capacidad de proceso. La transformación entre SSL y WTLS tan sólo dura unos milisegundos y

ocurre en la memoria del gateway simultáneamente con otros cientos o miles de peticiones simultáneas, permitiendo una conexión virtual y segura entre los dos protocolos. Los desarrolladores de gateways WAP y los operadores de red, toman todas las medidas posibles para mantener seguro el gateway WAP.

6.6.14.3 MEDIDAS DE SUGURIDAD

El gateway nunca guarda el contenido decodificado en algún tipo de medio secundario. El proceso de decodificación/codificación está desarrollado bajo unos parámetros de seguridad optimizados en velocidad, de forma que el contenido original sea borrado de la memoria volátil del gateway tan pronto como sea posible.

- Restringiendo el acceso físico a la consola gateway.
- Restringiendo el acceso administrativo a direcciones internas al firewall del operador.
- Usando las habituales medidas de seguridad que se aplican para proteger los sistemas de facturación y HLR con el gateway WAP.

6.6.15 EVOLUCIÓN DE WAP

En los últimos años la revolución en el mundo de las telecomunicaciones esta teniendo lugar en dos ámbitos: la telefonía móvil e Internet. Llegado un momento en que parece muy interesante unir ambos ámbitos, y así fue como nació WAP, como un método de acceder a Internet a través de un teléfono móvil. No se puede negar que esta unión ha sido un campo que ha alcanzado un elevadísimo grado de desarrollo tecnológico, y podría decirse que es uno de los tópicos que más investigación genera en el ámbito mundial actualmente. En 1997 pesos pesados en el mundo de las telecomunicaciones tales como Nokia, Motorola, Ericsson y Phone.com se unen para dar origen al WAP forum. La especificación WAP 2.0 o NG (Next Generation) fue aprobada en el año 2001 e incluyó gráficos a color, animaciones, descarga de archivos grandes, servicios de localización inteligente. Además funciones para facturación, tarjetas inteligentes, WAP por Bluetooth, WAP en sistemas inalámbricos de tercera generación, multimedia, y convergencia con XHTML. En pocas palabras podemos caracterizar la evolución de WAP como:

- Un aumento de la funcionalidad de WAP en sistemas actuales inalámbricos de segunda generación, fortaleciendo por ello los sistemas que se usan hoy; y
- Una extensión de las capacidades de WAP de trabajar en conjunción con otras tecnologías, ahora y en el futuro; por ejemplo, búsqueda, Bluetooth, tarjetas inteligentes, etc.

La instalación de soluciones WAP de punto a punto en el año 2001 fue bienvenida y dio lugar a una penetración en el mercado rápida y a gran escala. Estos servicios evolucionaron con la introducción de GPRS, Bluetooth, y la tecnología inalámbrica de tercera generación. Los desarrolladores de aplicación que desarrollan servicios WAP desarrollaron más adelante servicios para EPOC, GPRS, Bluetooth, Parlay, y sistemas de tercera generación. WAP es por eso más que sólo otra tecnología inalámbrica; es el catalizador de Internet móvil. WAP va a llegar a ser un artículo práctico entre los usuarios finales móviles, cambiando de modo significativo la manera en que enfocan y realizan numerosas tareas diarias. Hoy WAP adapta la tecnología existente de Internet al ambiente móvil. Las tecnologías requeridas para construir Internet Móvil estarán avanzando cada día y obteniendo un mayor reconocimiento, gracias a su alta velocidad en el envío de paquetes de datos, transmisión de radio de banda ancha, mayor número de terminales móviles avanzadas y mucha más capacidad y más calidad en la tecnología de redes. Actualmente, sin embargo, existen criticas a WAP por su lenta irrupción en el mercado que se ha propuesto dominar y esto se puede deber a causas como su relativo alto costo, bajo ancho de banda y errores de mentalidad tanto de usuarios como proveedores de contenido WAP que no se acostumbran aún a información especifica y muy reducida, muy diferente a los usuales caudales de bytes que disponemos en la Web.

6.6.16 TENDENCIAS

WAP funciona en cualquier patrón de tecnología móvil, como TDMA, CDMA, GSM, en todas las bandas de frecuencias de banda y, especialmente en los nuevos sistemas 3G. La plataforma es el camino para la oferta de servicios de transmisión de datos de la Web, hasta que la comunicación llegue a su máximo grado de excelencia, o sea, Tercera Generación de las Tecnologías de Comunicación Móviles. WAP es el primer paso en dirección para Internet Móvil y para la Tercera Generación de Tecnologías Móviles. Internet Móvil crea una serie de aplicaciones y servicios que estarán disponibles en cualquier lugar, a cualquier momento. Pero para que WAP se torne realidad, el usuario necesita estar conectado a un WAP gateway, servicio dado por una operadora o un proveedor. La tecnología WAP posibilita, a través de un "micro-browser", la visualización de páginas en la pantalla del teléfono móvil que están programadas en un lenguaje especial, denominado de WML. El WAP es un suceso relativo si comparado con su concurrente japonés I-Mode de la NTT DoCoMo. A pesar de las diferencias tecnológicas, el éxito del I-Mode está probablemente en el modelo de negocio adoptado por la operadora japonesa: un ciclo virtuoso en que cada parte participante recibe una parte justa de la recompensa por el esfuerzo en la creación de contenidos. WAP debe ser visto como uno de los principales elementos dentro de Internet Móvil. Es la llave que abre la puerta a un amplio rango de nuevas aplicaciones móviles basadas en la combinación de las tecnologías móviles e Internet. WAP maneja los diferentes tipos de redes y estándares de terminales móviles, por lo que tiene el potencial de convertirse en un verdadero estándar global. Así que, sin importar las limitaciones de las tecnologías actuales de Internet móvil, los operadores móviles, proveedores de contenido, proveedores de servicios, desarrolladores de aplicaciones y empresas de todo tipo, reconocen el potencial de WAP y buscaran entrar al mercado lo más oportunamente posible.

VII.-ANEXOS

ETHERNET Y FASTETHERNET

A1 INTRODUCCION

Fue a finales de los años 60 cuando la universidad de Hawai desarrolló el método de acceso CSMA/CD, empleado por primera vez en la red de área extendida ALOHA, en la que se basa la Ethernet. En 1972, Ethernet experimentó un fuerte desarrollo en Xerox, donde se conoció como *Experimental Ethernet*. Esta empresa pretendía unir 100 PC's en una distancia de 1 Km. El diseño tuvo mucho éxito y su popularidad creció. Además Xerox también contribuyó al avance del proyecto 802 del IEEE. Más adelante, en 1982, Xerox junto con Intel y Digital Equipment Corporation, sacaron la versión 2.0 de Ethernet. Hoy en día, Ethernet sigue el estándar 802.3 del IEEE.

A1.2 ETHERNET Y EL NIVEL FISICO

- La **velocidad** que desarrolla Ethernet es de 10Mbps, pero la norma 802.3 de IEEE define otras velocidades que van desde 1Mbps hasta 1000Mbps.
- La **codificación** que emplea Ethernet es de tipo Manchester Diferencial.
- El **medio de transmisión** empleado pueden ser varios:
    1. Cable Coaxial: Puede ser fino (thinnet) o grueso (thicknet).
    2. Par Trenzado: No apantallado (UTP), apantallado (STP).
    3. Fibra Óptica: Monomodo, Multimodo o de índice gradual.

Según se emplee un tipo de cable u otro, la **distancia máxima** de un segmento de cable que no pasa por ningún tipo de repetidor será una u otra. Existe una nomenclatura que nos indica la velocidad, el tipo de medio físico empleado, la distancia máxima:

- 10Base2: Nos indica que es una red Ethernet a 10Mbps, con cable coaxial fino (thinnet) y cuya distancia máxima es de 200m (en realidad son 185m, pero por comodidad se representa con un 2). Como máximo se pueden unir 5 segmentos de 200m mediante 4 repetidores. Donde como mucho 3 de esos segmentos pueden llevar estaciones de trabajo, y 2 deben ir sin equipos. A esta especificación se la denomina la regla de diseño 5/4/3/2/1. El número máximo de nodos por segmento es de 30. El nombre de Base se refiere a que se trata de una transmisión en banda base.
- 10Base5: Igual que el anterior pero esta vez se emplea cable coaxial grueso (thicknet), que permite aumentar la distancia máxima hasta 500m. También cumple con la regla de diseño 5/4/3/2/1. El número de nodos por segmento está limitado a 100.
- 10BaseT: La sigla 'T' se refiere a que se emplea par trenzado. Con este tipo de cable es necesario usar un Hub (concentrador) donde se conectarán todas las estaciones de trabajo. De este modo dispondremos de una topología física en estrella, mientras que la lógica sigue siendo en bus. La distancia máxima de un ordenador a cualquiera de los repetidores es de 100m. El máximo número de nodos en una red completa 10BaseT es de 1024. Estas estaciones pueden estar en un mismo segmento o en varios. Como en los otros casos una señal no puede atravesar más de 4 repetidores (Hubs).
- 10BaseF: La notación 'F' indica que el medio de transmisión es fibra óptica. La velocidad es como las anteriores, de 10Mbps. Y la longitud máxima de un vano puede llegar a varios kilómetros.

A1.3 ETHERNET Y EL SUBNIVEL MAC

- La **técnica de acceso** de Ethernet es CSMA/CD. Esta funciona bien cuando el tráfico cursado no es muy elevado. A veces ocurre que el tráfico en una LAN es muy elevado y se producen demasiadas colisiones haciendo que la red no funcione debidamente. Esto se puede solucionar separando la red en dos subredes mediante un bridge. Recordemos que

un Hub no aísla el tráfico, en cambio un bridge si. Otra característica de las redes Ethernet es que por su funcionamiento no puede garantizar un tiempo de acceso. Aunque por esta razón Ethernet no sería adecuada para aplicaciones en tiempo real, puede emplearse para transmitir voz y video cuando la red se sobredimensiona.

- El **Caudal Agregado** de una red Ethernet es del 30%. Esto significa que si todas las estaciones transmitieran a más del 30% de 10Mbps (3.33Mbps) habría demasiadas colisiones y la red se saturaría.
- El **Formato de Trama** del protocolo IEEE 802.3 (trama MAC) consta de los siguientes campos:

7B	**1B**	**6B**	**6B**	**2B**			**4B**
Preámbulo	SFD	DA	SA	Tipo/Longitud	Datos LLC	Relleno	FCS

Formato de la trama IEEE 802.3

1. Preámbulo: Son una serie de ceros y unos alternados que sirven para establecer la sincronización a nivel de bit.
2. Delimitador de comienzo de trama (SFD): Consiste en la secuencia de bits 10101011, que indica el comienzo real de la trama y posibilita al receptor localizar el primer bit del resto de la trama.
3. Dirección de destino (DA): Indica a quien va dirigida la trama. Esta dirección puede ser una única dirección física, una dirección de grupo o una dirección global.
4. Dirección de origen (SA): Especifica la estación que envió la trama.
5. Longitud: Marca la longitud del campo de datos LLC.
6. Datos LLC: Unidad de datos suministrada por LLC.
7. Relleno: Son unos octetos de relleno para asegurar que la trama es lo suficientemente larga como para un correcto funcionamiento de la técnica de detección de colisión.
8. Secuencia de comprobación de trama (FCS): Comprobador de redundancia cíclica de 32 bits (CRC-32). Este campo sirve para detectar errores, pero no para corregirlos.

Las direcciones en Ethernet están formadas por 6 octetos (48 bits). Una posible dirección podría ser, 01:A0:7F:10:04:AC. A continuación mostramos el formato:

1b	**1b**	**22b**	**24b**
Grupo	Global/Local	Fabricante	Nº de serie

Dirección Ethernet

El primer bit indica si el mensaje va destinado a una maquina individual ('0') o a un grupo ('1'). El siguiente sirve para indicar si la dirección es global ('1') o local ('0'). La dirección por defecto que tiene la tarjeta de red (NIC), es una dirección global. A veces nos puede interesar modificarla por alguna razón. Entonces pasa a ser local, pero será responsabilidad nuestra que esta no cree conflicto en nuestra LAN, pues puede haber dos máquinas con la misma dirección. Cuando en el campo de dirección destino aparece todo unos, es decir, FF:FF:FF:FF:FF:FF significa que se está emitiendo para todos los ordenadores conectados a la LAN (*multicast*). El campo de longitud de la trama MAC en la norma 802.3 ya hemos dicho que indica la longitud del campo de datos, que como mucho puede ser de 1500 Bytes. Esta trama luego pasa al subnivel LLC, quien se encarga de multiplexarla al protocolo que corresponda (IP, IPX, ARP, ...) Esta es una pequeña diferencia que existe con la arquitectura Ethernet, pues en este caso el campo de longitud marca el tipo de trama para saber a que protocolo corresponde. Se han reservado una serie de valores que van de 1500 en adelante.

El campo de relleno nos sirve para conseguir un tamaño mínimo de trama (64Bytes). Esto es para que funcione correctamente la detección de colisiones (CD). Supongamos dos equipos A y B

conectados por medio un medio físico. El equipo B manda una trama hacia A, que debido al retardo de propagación del medio no le llega pasado un tiempo 't'. Si justo antes de que le llegue la trama al equipo A, este transmite (pues ve que la línea no está ocupada por ningún otro medio), se produce una colisión. Esta tarda otro tiempo 't' en llegar al equipo B, que si todavía sigue transmitiendo la trama detecta la colisión y volvería a mandar la información. El problema surge cuando el equipo B recibe la colisión una vez que ya ha terminado de transmitir la trama. Esto puede suceder porque la trama sea muy corta, el retardo del medio muy grande (distancias largas) o porque se transmite a mucha velocidad. Por esta razón para una velocidad dada (10Mbps) se fija el retardo máximo (51.2 microseg) y esto fija el tamaño mínimo de la trama (64 Bytes). Con lo que una colisión solo se puede producir en los primeros 64 Bytes de una trama. De este modo quedan relacionados estos tres parámetros. Por ejemplo para transmitir a mayor velocidad, manteniendo el tamaño mínimo de la trama, debe disminuir el retardo del medio (distancia máxima).

Creando una red Ethernet, se podrá transferir archivos entre las diferentes computadoras y servidores, imprimir documentos en impresoras que se encuentren a varios metros de tu escritorio, ejecutar aplicaciones que se encuentren almacenadas en otras computadoras y compartir el acceso a Internet de alta velocidad. Ethernet extiende la accesibilidad y facilita la velocidad de transmisión. Las especificaciones de Ethernet describen como los datos pueden ser enviados entre computadoras en una LAN. Para ser una parte de ésta LAN, cada computadora necesita una interfaz de red que "empaqueta" los datos para que "viajen" a través de la red y un punto de conexión, o puerto, para el cableado especial que conecta todas las PC’s. Este puerto, creado en la placa madre (motherboard) o una tarjeta interfaz de red, envía los datos a la red y recibe la información enviada desde otras computadoras a la red. **Pero Ethernet es más que sólo hardware**. También se dedica a los protocolos de comunicación, o como las computadoras conectadas envían los datos. Las computadoras unidas por Ethernet envían datos paquetes de información. En adición a los datos en sí mismos, cada paquete lleva consigo una dirección de destino y la dirección origen. La interfaz de Ethernet utiliza Carrier Sense Multiple Acces With Collision Detection (Sensor carrier múltiple acceso con detención de colisiones) para enviar los paquetes. Todo esto significa que la computadora primero busca una baja en la actividad antes de enviar la información. Cada vez que un paquete llega a su destino, el emisor recibe una confirmación mientras que la computadora espera para enviar otro paquete. Los dispositivos a través del camino leen las direcciones y pasan los paquetes al siguiente dispositivo cercano. Ocasionalmente, dos dispositivos envían un paquete al mismo momento resultando una "colisión" y la pérdida momentánea de ambos paquetes. Cuando los paquetes colisionan, las PC’s que los enviaron son notificadas de manera instantánea, y cada una elige un intervalo aleatorio para esperar antes de volver a enviarlos. Esto ayuda a prevenir la parálisis de la red.

Pero no necesitas crear una LAN completa para utilizar Ethernet. Si simplemente conectas dos computadoras, podrás crear una red peer-to-peer (procesos distribuidos) mediante un cable crossover entre los puertos de red de las PC’s. Ethernet es muy utilizada para conectar PC’s a dispositivos de Internet de alta velocidad, como por ejemplo cable modem o DSL. Las especificaciones también detallan que tan rápido los datos pueden viajar y que tipos de cables deben ser utilizados. Por mucho tiempo, Ethernet 10Base-T, capaz de pasar 10 megabits de datos por segundo, fue la implementación más rápida y popular. A medida que las personas fueron utilizando Ethernet en redes cada vez más complejas y grandes, y el tamaño de los datos creció, la elección popular comenzó a ser la Ethernet 100Base-T, también conocida como FastEthernet o Ethernet Rápida con una velocidad de transferencia de datos diez veces mayor. Para conseguir más velocidad, FastEthernet utiliza cableado de mayor calidad que envía los paquetes más rápidamente sin perder la señal.

A2 FASTETHERNET

FastEthernet sigue la norma 802.3u (1995). La ventaja de FastEthernet es que es compatible y puede coexistir con redes Ethernet tradicionales. Ya que se mantienen todos los elementos de la norma 802.3 en cuanto a interfaces, estructura, longitud de tramas, detección de errores, método de acceso, etc. Lo único que se modifica es el nivel físico, reduciendo el tiempo de bit en un factor

de 10 (10ns), permitiendo un ancho de banda de 100Mbps. El cableado que se emplea es par trenzado (de categoría 3,4 ó 5) y fibra óptica. En FastEthernet también se dispone de una nomenclatura para designar el medio físico empleado:

- 100BaseT4: Se emplea UTP de categoría 3. De los 4 pares (8hilos) emplea 3 para transmisión a 100Mbps (recordemos que Ethernet es semiduplex) y 1 para detección de colisiones. Se emplea una codificación 8B6T. La longitud máxima es de 100m.
- 100BaseTX: Se usa UTP de categoría 5. Utiliza 2 pares, uno para fordwarding y otro para recepción (100Mbps). La codificación que emplea es 4B5B (compatible con FDDI). La longitud máxima también es de 100m.
- 100BaseFX: Emplea fibra óptica a una velocidad de 100Mbps (full duplex). La longitud máxima es de 2000m.

Las PC's y estaciones de trabajo que cuentan con un alto performance, o las nuevas arquitecturas de redes pueden no satisfacerse por las arquitecturas de 10Mbps. Sus aplicaciones requieren un gran ancho de banda para mover sus grandes cantidades de datos a través de una red de una manera rápida. Para aquellas empresas con instalaciones Ethernet, es preferible el incrementar la velocidad de su red a 100 Mbps que el invertir en una nueva tecnología LAN. Esta preferencia provocó que se especificara una Ethernet de mayor velocidad que operara a 100Mbps. (Desarrollo de FastEthernet). **En julio de 1993**, un grupo de compañías de redes se juntaron para formar la alianza de FastEthernet. Este grupo incorporó un bosquejo de la especificación 802.3u 100BaseT del IEEE, y aceleró la aceptación de dicha especificación en el mercado. La especificación final del 802.3u fue aprobada en Junio de 1995. Dentro de otros **objetivos** de esta alianza se tiene:

- Mantener el CSMA/CD (Ethernet transmission protocol Carrier Sense Multiple Access Collision Detection).
- Soportar los esquemas populares de cableado. (por ejemplo 10BaseT).
- Asegurar que la tecnología FastEthernet no requerirá cambios en los protocolos de las capas superiores, ni en el software que corre en las estaciones de trabajo LAN. No se necesita realizar cambios para el software de SNMP (Simple Network Managment Protocol) ni para las Management Information Bases (MIB's).
- **El objetivo principal de la alianza es el de asegurar que se pueda pasar del Ethernet tradicional a FastEthernet, manteniendo el protocolo tradicional de transmisión de Ethernet.**

A2.1 TOPOLOGIA

La topología que se utilizada es la de estrella en la cual cada usuario se conecta a un repetidor central o Hub. Cada grupo de trabajo forma una LAN separada (también conocido como collision domain). Y estos collision domains son fácilmente conectados por switches, puentes o ruteadores. El grupo de trabajo de la topología de estrella de FastEthernet puede estar configurado con un máximo de dos repetidores. Existen repetidores de Clase I que transmiten (o repiten) la señal de la línea de entrada de un puerto a los demás. No pueden existir en cascada. El de tipo Clase II repite inmediatamente las señales de la línea de entrada sin conversiones. Aquí se conectan medios de transmisión idénticos. a diferencia del nivel I Para 100BaseTX y 100BaseT4 la distancia máxima de un Hub a una estación de trabajo es de 100m. FastEthernet ofrece tres opciones de medio de transmisión:

Nombre	Sistema de Comunicación	Tipo Cable/Categoría
100Base-T4	half-duplex. Debido a que utiliza 3 pares para transmitir y recibir.	4 pares de UTP Categoría 3, 4, 5. Los datos son transmitidos en 3 pares (cada uno a 33 Mbps) utilizando codificación 8B/6T, la cual permite frecuencias menores y decrementa las emisiones electromagnéticas. Y el cuarto par es para detectar colisiones.
100Base-TX	half o full-duplex	Dos pares de UTP categoría 5 o STP Tipo I half

		duplex. Un par para transmisiones (con una frecuencia de operación de 125 MHz a 80% de eficiencia para permitir codificación 4B5B). Y el otro par para detectar colisiones y recibir. Utiliza un esquema de codificación MLT-3, también utilizado en ATM.
100Base-FX	half o full-duplex	Fibra óptica de 62.5 (core)/125 (cladding) -micron multimodo. Capaz de sostener un throughput de 100 Mbps en distancias mayores a 100m. Utiliza un fibra para transmisiones y la otra para detección de colisiones y para recibir.

	Longitud máxima por segmento	número Máximo de repetidores
100 Base-TX	100m (328 ft)	2
100 Base-T4	100m (328 ft)	2
100Base-FX	412m (1351ft)	2

Tabla 44 Ventajas adicionales de FastEthernet.

A2.2 FULL-DUPLEX

La tecnología full-duplex permite transmisiones a 200 Mbps porque provee comunicación bidireccional a 100 Mbps, además incrementa la distancia máxima que es soportada por las fibras ópticas entre dos dispositivos DTE (Data Terminal Equipment).

Physical Sublayer Option	Cable Specifcation	Length (meters)
100BaseTX	UTP Categoría 5, dos pares. STP Tipo 1 y 2, dos pares	100 half/full duplex. 100 half/full duplex
100BaseT4	UTP Categorías 3,4,5, cuatro pares	100 half/full duplex
100BaseFX	62.5/125 Fibra óptica multimodo	400 half duplex. 2000 full duplex

La comunicación full-duplex es implementada deshabilitando la detección de colisiones y las funciones de loopback, las cuales son necesarias para una comunicación eficiente en una red compartida; por lo tanto sólo los switches pueden ofrecer full-duplex si por tanto es más eficiente si esos switches se conectan en la conexión backbone.

B1 TOKEN RING

El problema con Ethernet es que la distribución del acceso al medio es aleatoria, por lo que puede ser injusta, perjudicando a una computadora durante un periodo de tiempo. En algunos casos es muy importante garantizar un acceso igualitario al medio, de modo de garantizar que siempre podremos transmitir, independientemente de la carga. Por razones de justicia en el acceso, típicamente estas redes se organizan en anillo, de modo de que el Token pueda circular en forma natural. El Token es un paquete físico especial, que no debe confundirse con un paquete de datos. Ninguna estación puede retener el Token por más de un tiempo dado (10 ms). Intenta aprovechar el ancho de banda a un 100%.

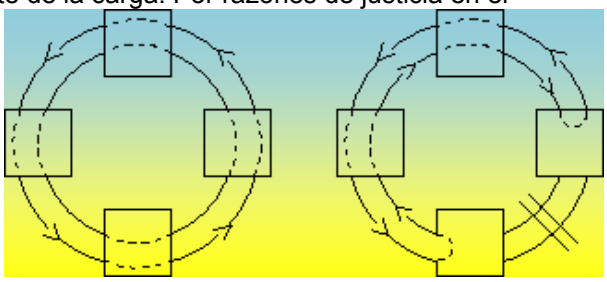


Figura 313

Las redes Token Ring originalmente fueron desarrolladas por IBM en los años 70's. Este fue el primer tipo de Red de Area Local de la tecnología IBM (LAN) Las especificaciones de IEEE 802.5 son casi idénticas en cuanto a compatibilidad con las redes de IBM's Token Ring. En base a las especificaciones de esta red se modeló el estándar IEEE 802.5. El término Token Ring es generalmente usado para referirnos a ambas redes, IBM's Token Ring e IEEE 802.5.

B1.1 COMPARACION TOKEN RING/IEEE802.5

Redes Token Ring e IEEE 802.5 son básicamente compatibles, a pesar que las especificaciones difieran relativamente de menor manera. Las redes IBM's Token Ring se refiere a las terminales conectadas a un dispositivo llamado **Multistation Access Unit (MSAU),** mientras que IEEE 802.5 no especifica un tipo de topología. Otras diferencias existentes son el tipo de medio, en IEEE 802.5 no se especifica un medio, mientras que en redes IBM Token Ring se utiliza par trenzado. En la siguiente figura 314 se muestran algunas características y diferencias de ambos tipos de red:

	TOKEN RING IBM	IEEE802.5
VELOCIDAD DE TRANSMISION	4.16Mbps	4.16Mbps
ESTACIONES/ SEGMENTOS	250 STP 70 UTP	250
TOPOLOGIA	ESTRELLA	NO ESPECIFICADO
MEDIO	PAR TRENZADO	NO ESPECIFICADO
SEÑALIZACION	BANDA BASE	BANDA BASE
METODO DE ACCESO	TOKEN PASSING	TOKEN PASSING
CODIFICACION	MANCHESTER	MANCHESTER

Figura 314

Las redes basadas en ***Token Passing*** basan el control de acceso al medio en la posesión de un Token (paquete con un contenido especial que le permite transmitir a la estación que lo tiene). Cuando ninguna estación necesita transmitir, el Token va circulando por la red de una a otra estación. Cuando una estación transmite una determinada cantidad de información debe pasar el Token a la siguiente. Cada estación puede mantener el Token por un periodo limitado de tiempo. Las redes de tipo Token Ring tienen una topología en anillo y están definidas en la especificación IEEE 802.5 para la velocidad de transmisión de 4Mbps. Existen redes Token Ring de 16Mbps, pero no están definidas en ninguna especificación de IEEE. Los grupos locales de dispositivos en una red Token Ring se conectan a través de una unidad de interfaz llamada MAU. La MAU contiene un pequeño transformador de aislamiento para cada dispositivo conectado, el cual brinda protección similar a la de Local Talk. El estándar IEEE 802.5 para las redes Token Ring no contiene ninguna

referencia específica a los requisitos de aislamiento. Por lo tanto la susceptibilidad de las redes Token Ring a las interferencias puede variar significativamente entre diferentes fabricantes.

B2 FUNCIONAMIENTO: TOKEN PASSING

Si una estación que posee el Token y tiene información por transmitir, esta divide el Token, alterando un bit de éste (el cuál cambia a una secuencia de start-of-frame), abre la información que se desea transmitir y finalmente manda la información hacia la siguiente estación en el anillo. Mientras la información del frame es circulada alrededor del anillo, no existe otro Token en la red (a menos que el anillo soporte uno nuevo), por lo tanto otras estaciones que deseen transmitir deberán esperar **es difícil que se presenten colisiones**. La información del frame circula en el anillo hasta que localiza la estación destino, la cual copia la información para poderla procesar. La información del frame continúa circulando en el anillo y finalmente es borrada cuando regresa a la estación desde la cual se envió. La estación que mandó puede checar en el frame que regresó si encontró a la estación destino y si entregó la información correspondiente (Acuse de recibo). A diferencia de las redes que utilizan CSMA/CD (como Ethernet), las redes Token Passing están caracterizadas por la posibilidad de calcular el máximo tiempo que pueden permanecer en una terminal esperando que estas transmitan.

B2.1 MAU

La MAU es el circuito usado en un nodo de red para acoplar el nodo al medio de transmisión. Este aislamiento es la clave para la inmunidad de los sistemas en red ante las interferencias. La implementación y la calidad del aislamiento proporcionado varía entre diferentes topologías de red. Estas diferencias son descritas a continuación:

Conexión de cableado Local Talk/Token Ring/AUI

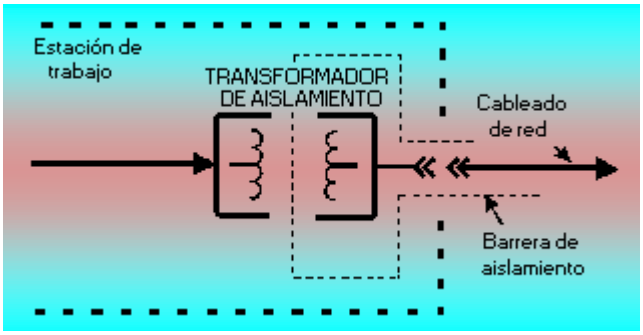


Figura 315

B2.2 CONEXIONES AUI

Casi todas las tarjetas Ethernet proveen una conexión AUI de 15 pines que puede ser usada para conectar un usuario a un Hub local o a una MAU. Esta conexión no da aislamiento o protección contra sobretensiones. El aislamiento hacia el cableado principal de la red lo brinda el Hub. Esta situación se muestra en la figura 315 y difiere de los arreglos LocalTalk y Token Ring principalmente en que el segmento de cable desprotegido es frecuentemente más largo en el caso de las conexiones AUI y en que el Hub en el cual termina la conexión puede tener una tierra diferente a la del equipo del usuario. El equipo del usuario es muy susceptible a daño a través de la conexión AUI. Estas últimas operan a distancias tan grandes como 100 metros, pero nunca deben ser usadas a esas distancias sin extremas precauciones. Cuando se conecten usuarios a un Hub usando un cable AUI, observe las siguientes reglas:

- Siempre asegúrese de que todos los usuarios conectados al Hub y el Hub mismo estén conectados en tomacorrientes que estén cableados al mismo tablero de distribución. Esto evita que ocurran altos voltajes de tierra intersistema.

- Mantenga la longitud del cableado por debajo de los 10 metros. Si es posible, haga que todos los usuarios alimentados desde el Hub y el mismo Hub se alimenten desde el mismo no break.

B2.3 CONEXIONES FISICAS

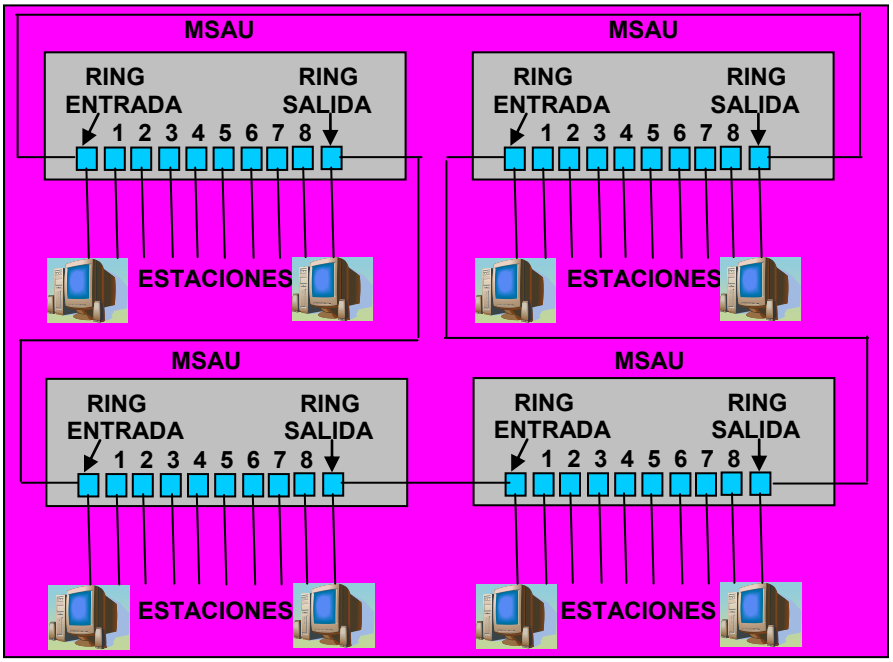


Figura 316

Las estaciones en redes IBM Token Ring se conectan directamente a MSAU's, las cuales pueden ser cableadas a través del anillo (como se muestra en la figura 316). Los Patch cables sirven para interconectar las MSAU's. Los Lobe cables conectan a las estaciones con las MSAU's.

B2.4 PRIORIDADES

Las redes Token Ring utilizan un sofisticado sistema de prioridad que permite designarles a los usuarios un tipo de prioridad en base a su uso de la red. Los frames en redes Token Ring tienen dos campos que controlan la prioridad: el campo de prioridad y un campo reservado. Solo las estaciones que posean un valor de prioridad igual o mayor al contenido en el Token pueden seccionar éste. Una vez que el Token está seccionado y la información del frame cambiada, sólo las estaciones con una prioridad mayor a la que transmitió el Token puede reservar el Token para la siguiente pasada a través de la red. Cuando el siguiente Token es generado, este incluye la prioridad más grande anteriormente reservada por la estación. Después de que se efectuó su entrega la estación que mandó debe regresar la prioridad del Token a como lo había encontrado.

B2.5 MANEJO DE MECANISMOS DE FALLA

Las redes Token Ring emplean varios mecanismos para detectar y corregir las fallas en la red. Por ejemplo: se selecciona una estación en una red Token Ring para que trabaje como monitor de la red. Esta estación que puede ser cualquiera de la red, centraliza los recursos en base a tiempos y sistemas de mantenimiento para las estaciones. Una de estas funciones es remover los constantes frames que circulan en el anillo. Cuando un dispositivo que envía falla, este frame puede continuar circulando en el anillo, esto previene a otras estaciones de transmitir en ese momento. El monitor detecta dichos frames y los remueve del anillo generando uno nuevo. Un algoritmo de Token llamado beaconing detecta y trata de reparar ciertos errores en la red. A veces,

una estación detecta un problema serio con la red (como un cable dañado o desconectado), esta envía un frame de reemplazo. El frame de reemplazo define una falla en el dominio donde reside la estación que detectó el problema, y enseguida viene un proceso de autoreconfiguración donde intervienen los nodos cercanos al problema y automáticamente lo soluciona.

B2.6 FORMATO DEL FRAME

Las redes Token Ring definen dos tipos de frames: **Token** y **data/command** frames. Ambos formatos se muestran en la figura 317 siguiente:

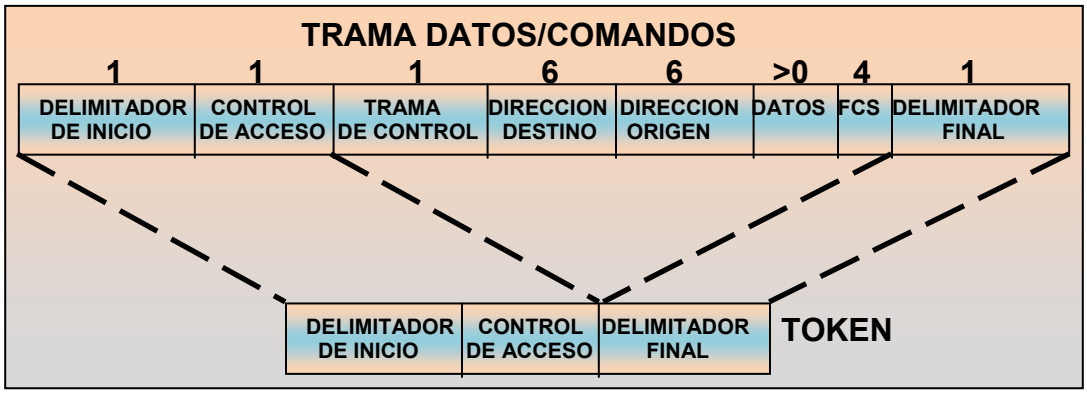


Figura 317

B2.7 TOKENS

Los Tokens son de 3 bytes de longitud y consisten en **un delimitador de inicio**, **un byte de control de acceso** y **un delimitador final**. El delimitador de inicio alerta a cada estación de la llegada de un Token (o data/command frame). Este campo incluye señales que distinguen este byte del resto del frame por una violación al esquema usado en el frame. El byte de control de acceso contiene los campos de prioridad y reservación, como un Token bit (usado para diferenciar un Token del frame data/command) y un monitor bit (usado por el monitor activo para determinar cuando un frame está circulando en el anillo a baja velocidad). Finalmente, las señales finales de delimitación señalan el final del Token o data/command frame. Aquí también están contenidos bits que muestran si el Token está dañado.

B 2.8 DATA/COMMAND FRAMES

Los Data/command frames varían en tamaño, dependiendo del tamaño del campo de datos. Los Data/command frames llevan información hacia protocolos de otro nivel.; Los frames de command contienen información de control y no contienen datos para llevar a otros protocolos. En los Data/command frames, hay un byte de frame control después del byte de control de acceso. El byte de frame control indica cuando el frame contiene datos o información de control. Seguido del byte de frame control hay dos campos de direcciones los cuáles identifican las estaciones destino y fuente. El campo de datos se encuentra después de los campos de direcciones. La longitud de este campo está limitado por el ring Token holding time, el cual define el máximo tiempo que una estación puede tener el Token. Seguido del campo de datos está el campo de frame check sequence (FCS). Este campo es llenado por la terminal fuente con un valor calculado dependiendo del contenido del frame. La estación de destino recalcula este valor para determinar si el frame tuvo algún daño durante el tiempo que se movió, si es así, el frame es descartado. Como en el Token, el delimitador completa el data/command frame.

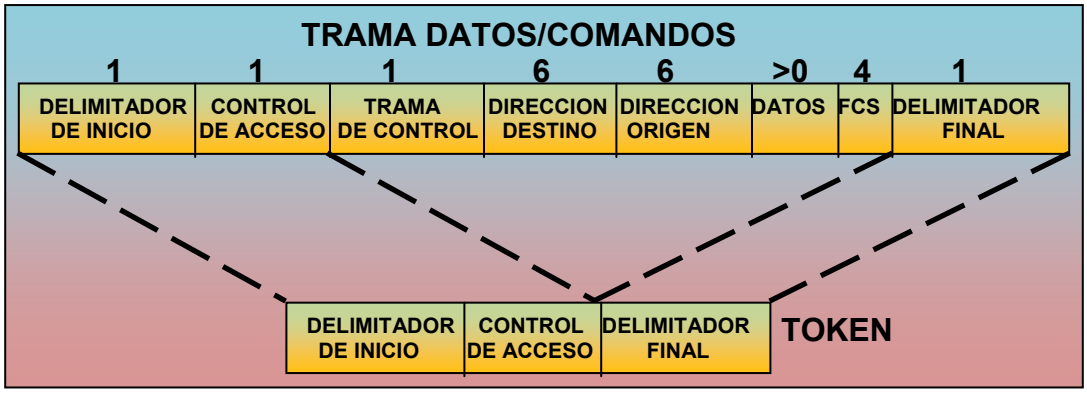


Figura 318

B3 TERMINOLOGIA TOKEN RING

- **Adaptadores Token Ring** Las tarjetas Token Ring están disponibles en modelos de 4 Mbits/sec y 16 Mbits/sec model. Si una tarjeta de 16 Mbits/sec es usada en una red de 4 Mbits/sec, ésta opera a 4 Mbits/sec. Verificar que se usen tarjetas de 16 Mbits/sec en su red respectiva.
- **Multistation Access Units (MAU)** Un conector MAU conecta 8 o más Estaciones de Trabajo usando algún tipo de cable de red como medio. Se pueden interconectar más de 12 dispositivos MAU.
- **Token Ring Adapter Cables** Cables Token Ring cables típicamente tienen conectores de 9 pines como terminales para conectar una tarjeta de red a un tipo especial, un conector especial que se conecta al MAU. La longitud del cable no debe excederft de longitud pero se pueden utilizar patch cables para extenderlos hasta 150ft.
- **Patch Cables** Los Patch cables extienden la distancia de una workstation hacia un dispositivo MAU. En los sistemas IBM, debe de ser del tipo 6 para una longitud arriba de 150ft. Ya que este tipo de cable tiene el potencial suficiente para soportar grandes distancias.
- **Conectores** Tipo 1 los usa IBM en sus sistemas de cableado conectores de datos tipo A que son hermafroditas.
- **Media Filters** Cuando se usa par trenzado tipo 3, se requiere un filtro de medios para las workstations. Este convierte los conectores de cable y reduce el ruido.
- **Patch Panels** Un patch panel se usa para organizar el cable con los MAU. Un conector estándar de teléfono se usa para conectar el patch panel al bloque de punchdown.
- **Maximum Stations and Distances** El número máximo de estaciones en un anillo es de 260 para cable blindado (STP) y 72 para UTP. La distancia máxima que puede haber entre un conector MAU y una estación es de 101 metros (330 f) tomando en cuenta que el cable es continuo de un sólo segmento, si se tienen que unir los segmentos se debe utilizar un patch cable, la distancia máxima de un MAU hacia la workstation es de 45 metros (150ft). La longitud total de la red LAN puede variar según las conexiones de las estaciones.

IPv6

C1.-INTRODUCCION

El protocolo **IPv6** es una nueva versión de IP (*Internet Protocol*). Diseñado por Steve Deering de Xerox PARC y Craig Mudge, IPv6 está destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados. Pero el nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionará a futuras celdas telefónicas y dispositivos móviles con sus direcciones propias y permanentes. A día de hoy se calcula que las dos terceras partes de las direcciones que ofrece IPv4 ya están asignadas. IPv4 posibilita 4,294,967,296 (2^{32}) direcciones de red diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos a cada vehículo, teléfono, PDA, etcétera. En cambio, IPv6 admite 340,282,366,920,938,463,463,374,607,431,768,211,456 (2^{128} o 340 sextillones de direcciones, cerca de 3.4×10^{20} 340 trillones de direcciones por cada pulgada cuadrada, 6.7×10^{17} o 670 mil billones de direcciones/mm^2 de la superficie de La Tierra). En esta versión se mantuvieron las funciones del IPv4 que son utilizadas, las que no son utilizadas o se usan con poca frecuencia, se quitaron o se hicieron opcionales, agregándose nuevas características.

Propuesto por el *Internet Engineering Task Force* en 1994 (cuando era llamado "IP Next Generation" o IPng), la adopción de IPv6 por parte de Internet es menor, la red todavía está dominada por IPv4. La necesidad de adoptar el nuevo protocolo debido a la falta de direcciones ha sido parcialmente aliviada por el uso de la técnica NAT. Pero NAT rompe con la idea originaria de Internet donde todos pueden conectarse con todos y hace difícil o imposible el uso de algunas aplicaciones P2P, de voz sobre IP y de juegos multiusuario. Un posible factor que influya a favor de la adopción del nuevo protocolo podría ser la capacidad de ofrecer nuevos servicios, tales como la movilidad, Calidad de Servicio (QoS), privacidad, etc. Otra vía para la popularización del protocolo es la adopción de este por parte de instituciones. El gobierno de los Estados Unidos ha ordenado el despliegue de IPv6 por todas sus agencias federales. IPv6 es la segunda versión del Protocolo de Internet que se ha adoptado para uso general. También hubo un IPv5, pero no fue un sucesor de IPv4; mejor dicho, fue un protocolo experimental orientado al flujo de streaming que intentaba soportar voz, video y audio.

C1.2 DIRECCIONAMIENTO

El cambio más grande de IPv4 a IPv6 es la longitud de las direcciones de red. Las direcciones IPv6, definidas en el RFC 2373 y RFC 2374, son de 128 bits; esto corresponde a 32 dígitos hexadecimales, que se utilizan normalmente para escribir las direcciones IPv6. En muchas ocasiones las direcciones IPv6 están compuestas por dos partes lógicas: un prefijo de 64 bits y otra parte de 64 bits que corresponde al identificador de interfaz, que casi siempre se genera automáticamente a partir de la dirección MAC de la interfaz a la que está asignada la dirección.

C1.2.1 NOTACION PARA LAS DIRECCIONES

Las direcciones identifican interfaces individuales o conjuntos de interfaces. Al igual que en IPv4 en los nodos se asignan a interfaces. Se clasifican en tres tipos:

- ***Unicast*** identifican a una sola interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección.
  [RFC 2373] [RFC 2374]
- ***Anycast*** identifican a un conjunto de interfaces. Un paquete enviado a una dirección anycast, será entregado a alguna de las interfaces identificadas con la dirección del conjunto al cual pertenece esa dirección anycast. [RFC 2526]
- ***Multicast*** identifican un grupo de interfaces. Cuando un paquete es enviado a una dirección multicast es entregado a todas las interfaces del grupo identificadas con esa

dirección. En el IPv6 no existen direcciones broadcast, su funcionalidad ha sido mejorada por las direcciones multicast. [RFC 2575]

Existen tres formas de representar las direcciones IPv6 como strings de texto.

- x:x:x:x:x:x:x:x donde cada x es el valor hexadecimal de 16 bits, de cada uno de los 8 campos que definen la dirección. No es necesario escribir los ceros a la izquierda de cada campo, pero al menos debe existir un número en cada campo. Ejemplos:
  FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
  1080:0:0:0:8:800:200C:417A

- Como será común utilizar esquemas de direccionamiento con largas cadenas de bits en cero, existe la posibilidad de usar sintácticamente ***::*** para representarlos. El uso de :: indica uno o más grupos de 16 bits de ceros. Dicho símbolo podrá aparecer una sola vez en cada dirección. Por ejemplo:

1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A	unicast address
FF01:0:0:0:0:0:0:101	FF01::101	multicast address
0:0:0:0:0:0:0:1	::1	loopback address
0:0:0:0:0:0:0:0	::	unspecified addresses

- Para escenarios con nodos IPv4 e IPv6 es posible utilizar la siguiente sintaxis: x:x:x:x:x:x:d.d.d.d, donde x representan valores hexadecimales de las seis partes más significativas (de 16 bits cada una) que componen la dirección y las d, son valores decimales de los 4 partes menos significativas (de 8 bits cada una), de la representación estándar del formato de direcciones IPv4.
  Ejemplos:

0:0:0:0:0:0:13.1.68.3	::13.1.68.3
0:0:0:0:0:FFFF:129.144.52.38	::FFFF:129.144.52.38

C1.2.2 REPRESENTACION DE LOS PREFIJOS DE LAS DIRECCIONES

Los prefijos de identificadores de subredes, routers y rangos de direcciones IPv6 son expresados de la misma forma que en la notación CIDR utilizada en IPv4. Un prefijo de dirección IPv6 se representa con la siguiente notación:
dirección-ipv6/longitud-prefijo,
donde: ***dirección-ipv6***: es una dirección IPv6 en cualquiera de las notaciones mencionadas anteriormente.
longitud-prefijo: es un valor decimal que especifica cuantos de los bits más significativos, representan el prefijo de la dirección.

C1.2.2.1 DIRECCIONES GLOBAL UNICAST

Formato de las direcciones global unicast

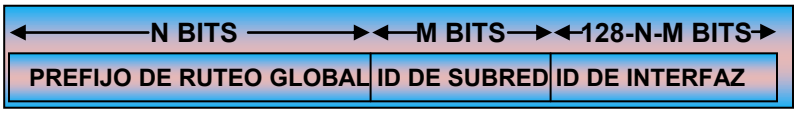


Figura 318

- **Prefijo de ruteo global**: es un prefijo asignado a un sitio, generalmente está estructurado jerárquicamente por los RIR's e ISP's.
- **Identificador de Subred**: es el identificador de una subred dentro de un sitio. Está diseñado para que los administradores de los sitios lo estructuren jerárquicamente

- **Identificador de Interfaz**: es el identificador de una interfaz. En todas las direcciones unicast, excepto las que comienzan con el valor binario 000, el identificador de interfaz debe ser de 64 bits y estar construido en el formato Modified EUI-64. El formato para este caso es el siguiente:

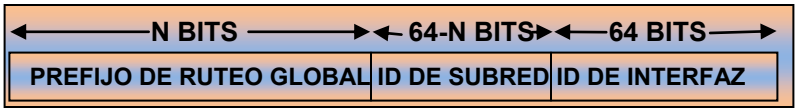


Figura 319

El siguiente es un ejemplo del formato de direcciones global unicast bajo el prefijo 2000::/3 administrado por el IANA

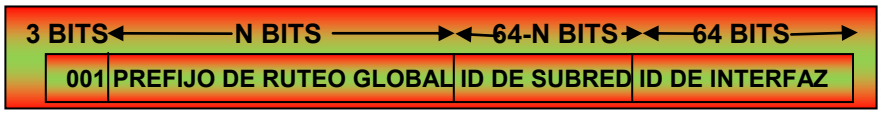


Figura 320

La asignación del espacio de direcciones IPv6 global unicast está accesible en IPv6 GLOBAL UNICAST ADDRESS ASSIGNMENTS Los tipos de direcciones IPv6 pueden identificarse tomando en cuenta los primeros bits de cada dirección.

- :: La dirección con todo ceros se utiliza para indicar la ausencia de dirección, y no se asigna ningún nodo.
- ::1 La dirección de loopback es una dirección que puede usar un nodo para enviarse paquetes a sí mismo (corresponde con 127.0.0.1 de IPv4). No puede asignarse a ninguna interfaz física.
- ::1.2.3.4 La dirección IPv4 compatible se usa como un mecanismo de transición en las redes duales IPv4/IPv6. Es un mecanismo que no se usa.
- ::ffff:0:0 La dirección IPv4 mapeada se usa como mecanismo de transición en terminales duales.
- fe80:: El prefijo de *enlace local* (*link local*) específica que la dirección sólo es válida en el enlace físico local.
- fec0:: El *prefijo de emplazamiento local* (*site-local prefix*) específica que la dirección sólo es válida dentro de una organización local. El RFC 3879 lo declaró obsoleto, estableciendo que los sistemas futuros no deben implementar ningún soporte para este tipo de dirección especial. Se deben sustituir por direcciones Local IPv6 Unicast.
- ff00:: El prefijo de multicast. Se usa para las direcciones multicast.

Hay que resaltar que no existen las direcciones de difusión (broadcast) en IPv6, aunque la funcionalidad que prestan puede emularse utilizando la dirección multicast FF01::1, denominada *todos los nodos* (*all nodes*) El formato ::ffff:1.2.3.4 se denomina *dirección IPv4 mapeada*, y el formato ::1.2.3.4 *dirección IPv4 compatible*. Las direcciones IPv4 pueden ser transformadas fácilmente al formato IPv6. Por ejemplo, si la dirección decimal IPv4 es 135.75.43.52 (en hexadecimal 874B2B34), puede ser convertida a 0000:0000:0000:0000:0000:0000:874B:2B34 o ::874B:2B34. Entonces, uno puede usar la notación mixta dirección IPv4 compatible, en cuyo caso la dirección debería ser ::135.75.43.52. Este tipo de dirección *IPv4 compatible* casi no está siendo utilizada en la práctica, aunque los estándares no la han declarado obsoleta.

C1.3 PAQUETES

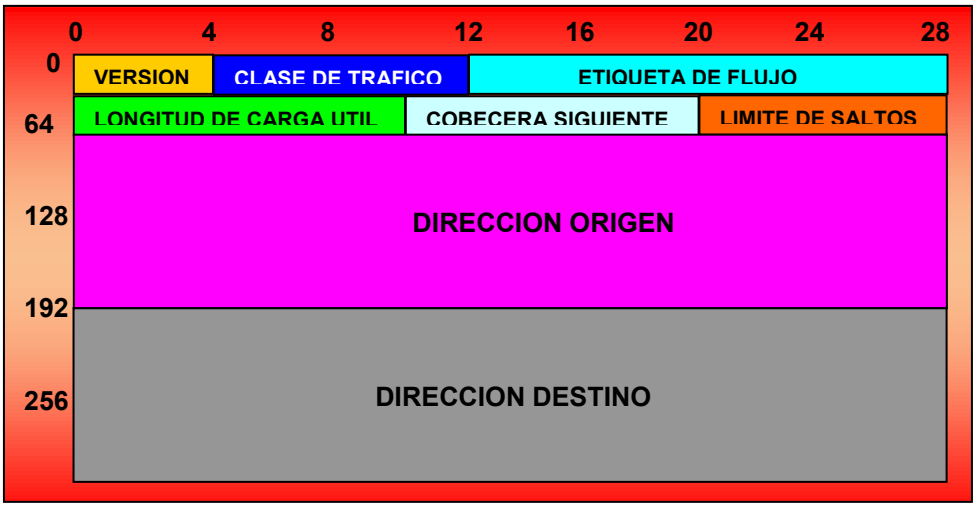


Figura 321 Estructura de la cabecera de un paquete IPv6

- *Versión* Campo de 4 bits, contiene el número de versión del Protocolo Internet (IP) en nuestro caso la 6.
- *Clase de Tráfico (Prioridad del paquete)* Es un campo de 4 bits. Se usa para distinguir entre paquetes a cuyos orígenes se les puede controlar el flujo y aquellos a los que no. Los valores 0 a 7 son para transmisiones capaces de reducir su velocidad en caso de un congestionamiento. Se muestran los siguientes valores de prioridad:
  - 0 - tráfico sin caracterizar
  - 1 - tráfico como las News de la red
  - 2 - datos de transferencia sin atender como e-mail
  - 3 - reservado
  - 4 - volumen de transferencia atendido como FTP
  - 5 - reservado
  - 6 - tráfico interactivo como telnet
  - 7 - tráfico de control de Internet como SNMP

  Los valores que van desde 8 hasta 15 se usan para tráfico de tiempo real cuya tasa de envío es constante aún si se están perdiendo todos los paquetes mandados, un ejemplo de este tipo de tráfico son los videos o audio. Dentro de cada grupo, los paquetes de número más bajo son menos importantes que los paquetes de número alto.
- *Etiqueta de flujo* Campo de 24 bits. Es un campo aún experimental. Se usará en un principio para permitir a un origen y a un destino establecer una pseudoconexión con unas determinadas propiedades y requisitos. Un ejemplo sería el de video en tiempo real.
- *Longitud de carga útil* Campo de 16 bits. Define la longitud del paquete que sigue a la cabecera (que inicialmente ocupa 40 bytes). El nombre del campo se cambió de longitud total en el IPv4 porque el significado cambió ligeramente: los 40 bytes de la cabecera ya no se cuentan como parte de la longitud. Si su valor es cero, indica que el tamaño de la carga vendrá especificado como Carga Jumbo, en una opción salto a salto.
- *Cabecera Siguiente* Campo de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente después de la primera cabecera (si es que hubiere más). Por ejemplo, puede ser una cabecera TCP, de encaminamiento, o de fragmentación y sus combinaciones.
- *Límite de Saltos* Campo de 8 bits. Este campo se usa para evitar que los paquetes vivan eternamente. En la práctica es igual que el campo de IPv4 TTL (time to live, tiempo de vida). Se decrementa de uno en uno en cada nodo que procesa el paquete. Si el límite es cero, el paquete se descarta.
- *Dirección de Origen* Campo de 128 bits, que contiene la dirección origen.
- *Dirección de Destino* Campo de 128 bits, que contiene la dirección origen.

C1.3.1 CABECERAS EXTENDIDAS

En IPv6, diferente información es codificada en cabeceras separadas, entre la cabecera IPv6 y la cabecera del nivel superior. Existen una serie de cabeceras extendidas, cada una identificada con un valor en el campo *cabecera siguiente*. Un paquete IPv6 puede contener ninguna, una o más cabeceras extendidas. Con la única excepción de las opciones salto a salto, las cabeceras extendidas no son examinadas ni procesadas hasta que el paquete llega a su destino. En las opciones *salto a salto*, hay información que es necesario procesar a lo largo del camino del datagrama, incluyendo los nodos origen y destino, cuando esta cabecera está presente, debe situarse inmediatamente después de la cabecera IPv6. Las cabeceras extendidas deben de ser procesadas en el orden en que aparezcan, el receptor no puede buscar una cabecera en concreto y procesarla antes que las anteriores. Si en el procesamiento de las cabeceras, un nodo se encuentra con un valor en *cabecera siguiente* que le es desconocido, el paquete debe ser descartado, y un nivel superior (ICMP), se encargará de enviar un error al origen. Cada cabecera extendida debe tener una longitud en octetos múltiplo de 8, para mantener la alineación a 8 octetos a cabeceras posteriores. La implementación de IPv6 incluye soporte para las siguientes opciones extendidas:

- ***Cabecera de opciones de salto a salto (Hop-by-Hop)***: Transporta información opcional, contiene los datos que deben ser examinados por cada nodo (cualquier sistema con IPv6) a través de la ruta de envío de un paquete. Su código es 0.
- ***Cabecera de encaminamiento (Routing)***: Se utiliza para que un origen IPv6 indique uno o más nodos intermedios que se han de visitar en el camino del paquete hacia el destino. Encaminamiento desde la fuente. El código que utiliza es 43.
- ***Cabecera de fragmentación (Fragment)***: hace posible que el origen envíe un paquete más grande de lo que cabría en la MTU de la ruta (unidad máxima de transferencia). Hay que tener en cuenta que al contrario que en IPv4, en IPv6 la fragmentación de un paquete sólo se puede realizar en los nodos origen. El código empleado en esta cabecera es 44.
- ***Cabecera de autenticación (Authentication Header)***: nos sirve para proveer servicios de integridad de datos, autenticación del origen de los datos, antireplay para IP. El código de esta cabecera es 51.
- ***Cabecera de encapsulado de seguridad de la carga útil (Encapsulating Security Payload)***: permiten proveer servicios de integridad de datos. El código al que hace referencia esta cabecera es el 50.
- ***Cabecera de opciones para el destino (Destination Options)***: se usa para llevar información opcional que necesita ser examinada solamente por los nodos destino del paquete. Esta cabecera utiliza el código 60.
- ***No Next Header***: Indica que no hay más cabeceras Utiliza el código 59

C1.3.1.1 ORDEN DE LAS CABECERAS

Cuando existe más de una cabecera extendida en el mismo paquete, es recomendable que éstas aparezcan en el siguiente orden:

- Cabecera IPv6.
- Opciones salto a salto.
- Opciones en destino. Para opciones que deban ser procesadas por el destino final y por los destinos marcados en la cabecera de enrutamiento.
- Enrutamiento.
- Fragmentación.
- Autenticación.
- Opciones de seguridad para la carga.
- Opciones en destino. Para opciones que sólo deban ser procesadas por el destino final.
- Cabecera del nivel superior.

Cada cabecera debe aparecer tan sólo una vez, con la excepción de las opciones de destino, que pueden aparecer dos veces, en el orden indicado anteriormente. Si la cabecera del nivel

superior es otra cabecera IPv6, ésta irá seguida de sus propias cabeceras, ordenadas de la forma indicada. Los nodos que soporten IPv6, deben aceptar y procesar las cabeceras en cualquier orden en que aparezcan, y también si aparecen dos o más veces, a excepción de las opciones salto a salto, que deben aparecer inmediatamente después de la cabecera IPv6. De todos modos, se recomienda que los nodos que envíen paquetes IPv6 sigan el orden recomendado.

C1.3.2 FRAGMENTACION

Al contrario que en IPv4, el fragmentado de un paquete sólo lo puede llevar a cabo el origen, con lo que se obvia el flag no fragmentable, de IPv4. La fragmentación de un datagrama IP es necesaria cuando el tamaño de un datagrama resulta intratable para alguna de las redes que debe atravesar para llegar a su destino. Para cada paquete que deba ser fragmentado, el origen le asigna un identificador (Cabecera de fragmento), este identificador debe ser diferente del de cualquier otro paquete enviado recientemente con las mismas direcciones origen y destino. La Cabecera de fragmento es utilizada por el origen del paquete IPv6 para enviar paquetes cuyo tamaño excede el mínimo MTU (Maximum Transmission Unit) en el camino del paquete. El paquete original se diferencia en dos partes, fragmentable y no fragmentable. La parte no fragmentable consiste en la cabecera IPv6 y las cabeceras extendidas que deban ser procesadas por los nodos intermedios en el camino del paquete. La parte fragmentable consta del resto de cabeceras extendidas, de la cabecera del nivel superior y de la carga. El paquete original se descompone en fragmentos cuya longitud debe estar alineada a 8 octetos (excepto el último). La parte no fragmentable del paquete original se copia a todos sus fragmentos, cambiando el campo longitud de la carga a la longitud de cada fragmento y el campo cabecera siguiente a 44 (valor que identifica a una cabecera de fragmento). Cada fragmento está compuesto por:

- La parte no fragmentable del paquete original.
- La cabecera de fragmento.
- El fragmento propiamente dicho.

En destino, el paquete original es construido según las siguientes normas:

- Los fragmentos del paquete original deben contener los mismos valores en los campos Dirección Origen, Dirección Destino e Identificador de Fragmento.
- El campo cabecera siguiente de la cabecera IPv6 se obtiene del campo cabecera siguiente de la cabecera de fragmento del primer fragmento.
- El campo tamaño de la carga del datagrama original se calcula en base al tamaño de la parte no fragmentable, al tamaño y offset de fragmento del último fragmento.

En el proceso de reensamblado, pueden producirse los siguientes errores:

- Si se ha recibido un número de fragmentos insuficientes para recomponer el paquete original pasados 60 segundos desde el primer fragmento recibido, se abandona el proceso y se descartan todos los fragmentos recibidos. Si se recibió el primer fragmento (offset de fragmento = 0), se envía un mensaje ICMP de error al origen.
- Si la longitud de un fragmento en octetos no es múltiplo de 8 y no es el último fragmento, se descarta el fragmento y se envía un mensaje ICMP de error al origen.

Si la longitud y el offset de fragmento de un fragmento determinan que la longitud de la carga del paquete original es mayor de 65,535 octetos, se descarta el fragmento y se envía un mensaje ICMP de error al origen.

C1.4 IPv6 Y EL SISTEMA DE NOMBRES DE DOMINIO

Las direcciones IPv6 se representan en el Sistema de Nombres de Dominio (DNS) mediante registros *AAAA* (también llamados registros de *quad-A*, por tener una longitud cuatro veces la de los registros A para IPv4). El concepto de AAAA fue una de las dos propuestas al tiempo que se estaba diseñando la arquitectura IPv6. La otra propuesta utilizaba registros *A6* y otras innovaciones como las etiquetas de cadena de bits (*bit-string labels*) y los registros *DNAME*. Mientras que la idea de AAAA es una simple generalización del DNS IPv4, la idea de A6 fue una revisión y puesta a

punto del DNS para ser más genérico, y de ahí su complejidad. El RFC 3263 recomienda utilizar registros AAAA hasta tanto se pruebe y estudie exhaustivamente el uso de registros A6. El RFC 3364 realiza una comparación de las ventajas y desventajas de cada tipo de registro. El almacenamiento actual de direcciones de Internet en el Domain Name System (DNS) de IPv4 no se puede extender fácilmente para que soporte direcciones IPv6 de 128 bits, ya que las aplicaciones asumen que a las consultas de direcciones se retornan solamente direcciones IPv4 de 32 bits. El 20 de Julio de 2004 la ICANN anunció que los servidores raíz de DNS de Internet habían sido modificados para soportar ambos protocolos, IPv4 e IPv6.

C1.5 IPSEC

C1.5.1 EL PROBLEMA DE LA SEGURIDAD EN INTERNET

De forma recurrente vemos cómo se achaca a Internet el hecho de ser un medio de comunicación inseguro. Este es un tema con muchas aristas y que debe ser examinado en cada una de sus partes. Sin embargo, el problema de seguridad en el nivel de red sigue sin ser tenido en cuenta y comienza a producirse una serie de ataques cada vez más sofisticados y basados en la suplantación de la identidad de máquinas conectadas a la red, dando la posibilidad de violar un acceso prohibido o dando la posibilidad de escudriñar (o desviar) la información a intrusos. Como respuesta surgen mecanismos de barrera como los cortafuegos, pero los protocolos siguen sin incorporar medidas específicas de seguridad. Pero esto es sólo una parte del problema. La seguridad integral comprende servicios tanto de confidencialidad como de autentificación, integridad y no rechazo para los que se requieren técnicas criptográficas que están sujetas a diferentes normativas de exportación y uso en determinados países, lo que hace complicado su uso generalizado en un medio que se tiene por libre (en cuanto a la naturaleza de la información intercambiada y su formato) y homogéneo (en cuanto al tipo de protocolos/aplicaciones empleados). Se corre el peligro de fracturar la Internet en zonas donde se puedan intercambiar información de forma segura y otras en que no, bien por considerarse tecnología de uso militar, bien por el derecho que se guardan algunos gobiernos a poder intervenir –e interpretar- las comunicaciones de sus ciudadanos.

C1.5.2 SEGURIDAD EN IPv6

La seguridad es una de las grandes ventajas que presenta IPv6. El nuevo protocolo de comunicación incluye, de forma obligatoria e intrínseca en su núcleo, la especificación de seguridad IPSec. IPv6 recoge todo lo bueno como lo malo de IPv4 y lo mejora. En el caso de la seguridad, el nuevo protocolo utiliza también IPSec como lo hace IPv4, pero con la diferencia de que en este deja de ser algo opcional para pasar a ser obligatorio. Con IPv6 todo el tráfico de la red va a ser autenticado, vamos a saber quien es el origen, quien el destino, realizando un mejor y más exhaustivo seguimiento de la información y su envío.

C1.5.3 CALIDAD DE SERVICIO (QoS)

En otro orden de cosas, estamos asistiendo al nacimiento de servicios de transmisión de información en tiempo real dentro de Internet. Ipv6 proporciona una mejor plataforma para crear y soportar muchos de los nuevos servicios imaginados, especialmente aquellos que combinan diferentes tipos de medios, como videotelefonía y mensajería multimedia. Y estos diferentes servicios exigen diferentes requerimientos sobre la red y el sistema subyacente. Si se producen retardos en el flujo de datos en el correo, no tiene demasiada importancia, pero si surgen interrupciones significativas en el flujo de datos de una videollamada, la comunicación se haría imposible. Por tanto, un defecto claro de IPv4 es la falta de caracterización de los distintos flujos de información que viajan por la red. El advenimiento de nuevos servicios multimedia en tiempo real presenta una clara limitación al uso de la Internet tal y como la concebimos actualmente en contraposición a otro tipo de tecnologías orientadas a la conexión como ATM que parecen más adecuadas para este tipo de servicios. Pero gracias a IPv6, se mejoran sensiblemente este tipo de transmisiones, ya que en el nuevo formato proporciona una verdadera calidad de servicio mediante

la inclusión de dos campos en la cabecera: La clase de tráfico, que distingue los diferentes tipos de datagramas según la clase de servicio, y la etiqueta de flujo, que permite diferenciar y asignar distintos estados a distintos flujos originados por la misma fuente. IPSec es un grupo de extensiones de la familia del protocolo IP. IPSec provee servicios criptográficos de seguridad. Estos servicios permiten la autenticación, integridad, control de acceso, y confidencialidad. IPSec provee servicios similares a SSL, pero a nivel de redes, de un modo que es completamente transparente para sus aplicaciones y mucho más robusto. Es transparente porque sus aplicaciones no necesitan tener ningún conocimiento de IPSec para poder usarlo. Puede crear túneles cifrados (VPN's), o simple cifrado entre ordenadores. Debido a que dispone de tantas opciones, IPSec es más bien complejo. Además, se puede utilizar cualquier protocolo IP sobre IPSec. De un modo lógico.

C1.5.4 SERVICIOS OFRECIDOS POR IPSEC

El protocolo de Internet actual (IP), también conocido como IPv4, no provee por sí mismo de ninguna protección a sus transferencias de datos. IPSec intenta remediarlo. Estos servicios vienen tratados como dos servicios distintos, pero IPSec ofrece soporte para ambos de un modo uniforme.

- **Confidencialidad** Asegura que sea difícil para todos comprender qué datos se han comunicado, excepto para el receptor, de manera que nadie vea las contraseñas cuando ingrese en una máquina remota a través de Internet.
- **Integridad** Garantiza que los datos no puedan ser cambiados en el camino. En el caso de una línea que lleve datos sobre facturación, será imprescindible que las cantidades y cifras de contabilidad son las correctas, y que no han podido ser alteradas durante el tránsito.
- **Autenticidad** Firma los datos de modo que otros puedan verificar que es realmente el remitente quien los envió, asegurando así su autenticidad.
- **Protección a la réplica** Asegura que una transacción sólo se puede llevar a cabo una vez, a menos que se autorice una repetición de la misma.

C1.5.5 PROTOCOLOS USADOS POR IPSEC

IPSec provee confidencialidad, integridad, autenticidad, y protección a la réplica a través de dos nuevos protocolos. Estos protocolos se llaman "Cabecera de Autenticación" (AH, "Authentication Header") y "Cargo de Seguridad Encapsulado" (ESP, "Encapsulated Security Payload"). AH provee autentificación, integridad, y protección a la réplica (pero no confidencialidad). Su principal diferencia con ESP es que AH también asegura partes de la cabecera IP del paquete (como las direcciones de origen o destino). ESP puede proveer autenticación, integridad, protección a la réplica, y confidencialidad de los datos (asegura todo lo que sigue a la cabecera en el paquete).

C1.6 DESPLIEGUE DE IPv6

C1.6.1 MECANISMOS DE TRANSICION A IPv6

Ante el agotamiento de las direcciones IPv4, el cambio a IPv6 ya ha comenzado. Se espera que convivan ambos protocolos durante 20 años y que la implantación de IPv6 sea paulatina. Existe una serie de mecanismos que permitirán la convivencia y la migración progresiva tanto de las redes como de los equipos de usuario. En general, los mecanismos de transición pueden clasificarse en tres grupos:

- **Pila dual** La pila dual hace referencia a una *solución de nivel IP con pila dual* (RFC 2893), que implementa las pilas de ambos protocolos, IPv4 e IPv6, en cada nodo de la red. Cada nodo de pila dual en la red tendrá dos direcciones de red, una IPv4 y otra IPv6.
    1. **A favor**: Fácil de desplegar y extensamente soportado.
    2. **En contra**: La topología de red requiere dos tablas de encaminamiento y dos procesos de encaminamiento. Cada nodo en la red necesita tener actualizadas las dos pilas.
- **Túneles** Los túneles permiten conectarse a redes IPv6 "saltando" sobre redes IPv4. Estos túneles trabajan encapsulando los paquetes IPv6 en paquetes IPv4 teniendo como

siguiente capa IP el protocolo número 41, y de ahí el nombre *proto-41*. De esta manera, se pueden enviar paquetes IPv6 sobre una infraestructura IPv4. Hay muchas tecnologías de túneles disponibles. La principal diferencia está en el método que usan los nodos encapsuladores para determinar la dirección a la salida del túnel.

- **Traducción** La traducción es necesaria cuando un nodo que sólo soporta IPv4 intenta comunicar con un nodo que sólo soporta IPv6. Los mecanismos de traducción se pueden dividir en dos grupos basados en si la información de estado está guardada:
    1. **Con estado**: NAT-PT RFC 2733, TCP-UDP Relay RFC 3142, Socks-based Gateway RFC 3089
    2. **Sin estado**: Bump-in-the -Stack, Bump-in-the API RFC 276

Actualmente el protocolo IPv6 está soportado en la mayoría de los sistemas operativos modernos, en algunos casos como una opción de instalación. Linux, Solaris, Mac OS, NetBSD, OpenBSD, FreeBSD, Windows (2000, XP y Vista de forma nativa) y Symbian (dispositivos móviles) son sólo algunos de los sistemas operativos que pueden funcionar con IPv6.

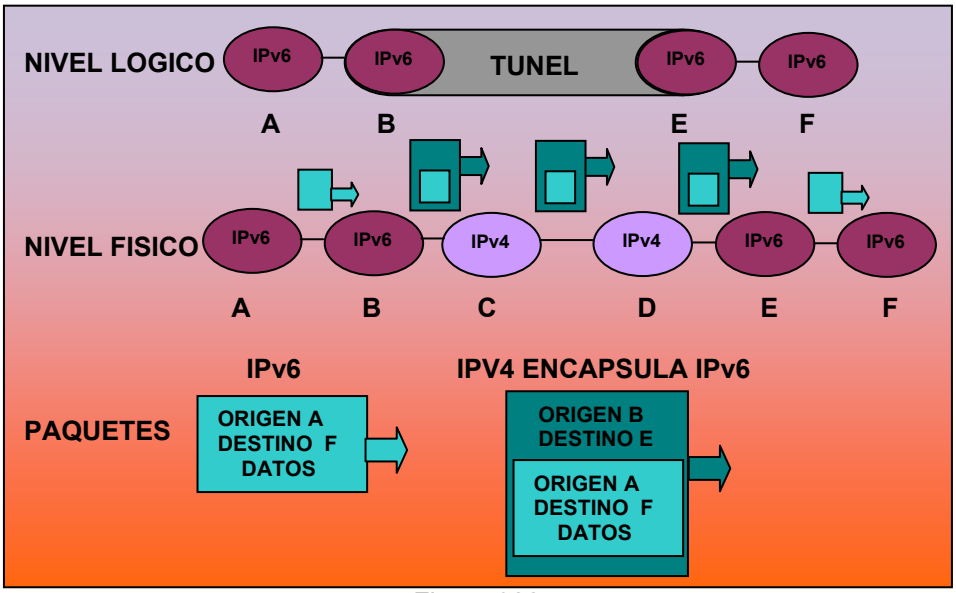


Figura 322

C1.6.2 VENTAJAS

- **Capacidad extendida de direccionamiento** IPv6 incrementa el tamaño de dirección IP de 32 bits a 128 bits, para dar soporte a más niveles de direccionamiento jerárquico, un número mucho mayor de nodos direccionables, y una autoconfiguración más simple de direcciones. La escalabilidad del enrutamiento multicast se mejora agregando un campo "ámbito" a estas direcciones. Y se define un nuevo tipo de dirección llamada "dirección envío a uno de", usado para enviar un paquete a cualquiera de un grupo de nodos.
- **Simplificación del formato de cabecera** Algunos campos de la cabecera IPv4 se han sacado o se han hecho opcionales, para reducir el costo del procesamiento de los paquetes y para ahorrar ancho de banda.
- **Soporte mejorado para las extensiones y opciones** Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un reenvío más eficiente, límites menos rigurosos en la longitud de opciones, y mayor flexibilidad para introducir nuevas opciones en el futuro.
- **Capacidad de etiquetado de flujos** Una nueva capacidad se agrega para permitir el etiquetado de paquetes que pertenecen a "flujos" de tráfico particulares para lo cual el remitente solicita tratamiento especial, como la calidad de servicio no estándar o el servicio en "tiempo real".

- **Capacidades de Autentificación y Privacidad** IPv6 incluye la especificación de extensiones que proveen autenticación, integridad, y (opcionalmente) confidencialidad de los datos.

C1.6.3 DESVENTAJAS

- La necesidad de extender un soporte permanente para IPv6 a través de todo Internet y de los dispositivos conectados a ella.
- Para estar enlazada al universo IPv6 durante la fase de transición, todavía se necesita una dirección IPv4 o algún tipo de NAT (Compartición de direcciones IP) en los routers (IPv6<-->IPv4) que añaden complejidad y que significa que el gran espacio de direcciones prometido por la especificación no podrá ser inmediatamente usado.
- Problemas restantes de arquitectura, como la falta de acuerdo para un soporte adecuado de IPv6 multihoming.
- Las direcciones IPv6 son mucho más largas que las direcciones IPv4, y, por lo tanto, más difíciles de memorizar.

VOZ SOBRE IP

D1 CONCEPTOS

D1.1 INTRODUCCION

El crecimiento y fuerte implantación de las redes IP, tanto en local como en remoto, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que permitan la calidad en redes IP, han creado un entorno donde es posible transmitir telefonía sobre IP lo que no significará en modo alguno la desaparición de las redes telefónicas modo circuito, sino que habrá, al menos temporalmente, una fase de coexistencia entre ambas. Primero se explican los conceptos fundamentales de esta tecnología, los inicios de la misma, así como las ventajas y desventajas que presenta la Voz Sobre IP. Después se trata sobre la seguridad en la tecnología Voz Sobre IP, las amenazas que poseen las redes bajo esta tecnología , así como los medios de defensa que existen para proteger la red IP. Y por último se expone el presente y futuro de la tecnología de Voz Sobre IP, las empresas relacionadas con la misma, de igual forma se expone las predicciones del mercado de esta tecnología. Como tecnología, la Voz sobre IP (VoIP) lleva varios años de presencia en el mercado. Sin embargo, no ha sido hasta la emergencia de nuevos e innovadores servicios basados en esta tecnología que la integración de voz y datos se ha hecho realidad, lo que, para las empresas, ha significado un ahorro de costos y unas comunicaciones más eficientes y efectivas.

D1.2 DEFINICION

Los productos de telefonía por Internet se denominan: Telefonía IP (IP telephony) Voz sobre Internet -Voice over the Internet (VOI)- o Voz sobre IP -Voice over IP (VOIP).

Figura 323

La Voz sobre IP (VoIP, Voice over IP) es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos. La Telefonía IP es una aplicación inmediata de esta tecnología, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando una PC, gateways y teléfonos estándares. En general, servicios de comunicación (voz, fax, aplicaciones de mensajes de voz) que son transportados vía redes IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional. La VoIP (Voz sobre IP) esta sigla designa la tecnología empleada para enviar información de voz en forma digital en paquetes discretos a través de los protocolos de Internet, en vez de hacerlo a través de la red de telefonía habitual. La industria de Voz sobre IP se encuentra en una etapa de crecimiento rápido. La evolución del uso de Voz sobre IP vendrá con la evolución de la infraestructura y de los protocolos de comunicación. En el año 2010, una cuarta parte de las llamadas mundiales se basarán en IP. A lo largo del tiempo, las aplicaciones de voz y datos han requerido redes distintas que usan tecnologías diferentes.

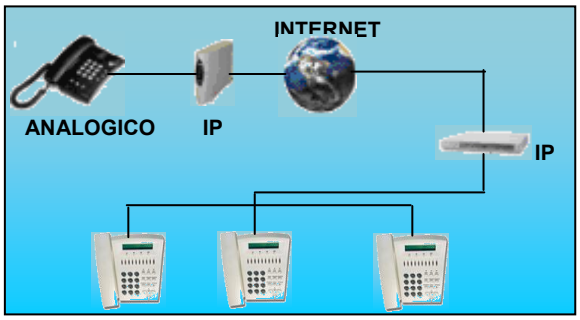


Figura 324

Sin embargo, últimamente se han realizado numerosos esfuerzos para encontrar una solución que proporcione un soporte satisfactorio para ambos tipos de transmisión sobre una sola red. La Voz sobre IP es una tecnología de telefonía que puede ser habilitada a través de una red de datos de conmutación de paquetes. La ventaja real de esta tecnología es la transmisión de voz de forma gratuita, ya que viaja como datos.

La tecnología VoIP puede revolucionar las comunicaciones internas al ofrecer:

- Acceso a las redes corporativas desde pequeñas sedes a través de redes integradas de voz y datos conectadas a sucursales.
- Directorios corporativos basados en la Intranet con servicios de mensajes y números personales para quienes deben desplazarse.
- Servicios de directorio y de conferencias basadas en gráficos desde el sistema de sobremesa.
- Redes privadas y gateways virtuales gestionados para voz que sustituyen a las Redes Privadas Virtuales (VPN).
- VoIP (Voz sobre IP) brinda nuevas oportunidades para quienes sean capaces de preverlas y actúen con la rapidez suficiente para superar la confusión que envuelve esta extraordinaria tecnología.

D1.3 COMO SE USA LA VoIP

Es importante conocer como se usa esta tecnología, básicamente hay que comprar un dispositivo que visualmente es una cajita negra que se conecta por un lado al aparato telefónico y por el otro a la PC, aunque también hay disponibles teléfonos IP. Por supuesto se necesita instalar un software para que dicho dispositivo funcione. Hay dos posibilidades de conexión:

- Una de las partes tiene VoIP y la otra no.
- Ambas partes tienen VoIP.

Si ambas partes tienen VoIP la llamada es totalmente gratuita, pues se llama de VoIP a VoIP; sólo tiene que discar el número telefónico y nada más. Si sólo quien llama tiene VoIP entonces hace uso de una tarjeta que se compra online (en línea). La mencionada tarjeta no es una tarjeta de plástico o de cartón como las que se venden en los comercios, más bien es una tarjeta virtual que se compra y carga por Internet. Es necesario aclarar que se puede instalar un VoIP aunque tenga una central telefónica y más de una línea de teléfono, pues se puede designar una línea para que trabaje directamente con VoIP, sin perjuicio de seguir utilizándola normalmente. El VoIP es una buena alternativa para quien tiene oficinas en el exterior y hace llamadas de larga distancia diariamente o de mucha duración.

D1.4 ELEMNTOS DE VoIP

El modelo de Voz sobre IP está formado por tres principales elementos:

- **El cliente.** Este elemento establece y termina las llamadas de voz. Codifica, empaqueta y transmite la información de salida generada por el micrófono del usuario. Asimismo, recibe, decodifica y reproduce la información de voz de entrada a través de los altavoces o audífonos del usuario. Cabe destacar que el elemento cliente se presenta en dos formas básicas: la primera es una suite de software corriendo en una PC que el usuario controla mediante una interfaz gráfica (GUI); y la segunda puede ser un cliente "virtual" que reside en el gateway.
- **Servidores.** El segundo elemento de la VoIP está basado en servidores, los cuales manejan un amplio rango de operaciones complejas de bases de datos, tanto en tiempo real como fuera de él. Estas operaciones incluyen validación de usuarios, tasación, contabilidad, tarificación, recolección, distribución de utilidades, enrutamiento, administración general del servicio, carga de clientes, control del servicio, registro de usuarios y servicios de directorio entre otros.
- **Gateways.** El tercer elemento lo conforman los gateways de VoIP, los cuales proporcionan un puente de comunicación entre los usuarios. La función principal de un gateway es proveer las interfaces con la telefonía tradicional apropiada, funcionando como una

plataforma para los clientes virtuales. Estos equipos también juegan un papel importante en la seguridad de acceso, la contabilidad, el control de calidad del servicio (QoS; Quality of Service) y en el mejoramiento del mismo.

D1.5 CARACTERISTICAS DE VoIP

Por su estructura el estándar proporciona las siguientes características:

- Permite el control del tráfico de la red, por lo que se disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento de las redes de datos.
- Proporciona el enlace a la red telefónica tradicional.
- Al tratarse de una tecnología soportada en IP presenta las siguientes ventajas adicionales:
  - Es independiente del tipo de red física que lo soporta. Permite la integración con las grandes redes de IP actuales.
  - Es independiente del hardware utilizado.
  - Permite ser implementado tanto en software como en hardware, con la particularidad de que el hardware supondría eliminar el impacto inicial para el usuario común.

Figura 325

D1.6 PROTOCOLOS DE VoIP

Hoy en día, existen dos protocolos para transmitir voz sobre IP, ambos definen la manera en que los dispositivos de este tipo deben establecer comunicación entre sí, además de incluir especificaciones para codecs (codificador-decodificador) de audio para convertir una señal auditiva a una digitalizada compresa y viceversa.

- **H.323**
  H.323 es el estándar creado por la Unión Internacional de Telecomunicaciones (ITU) que se compone por un protocolo sumamente complejo y extenso, el cual además de incluir la VoIP, ofrece especificaciones para vídeoconferencias y aplicaciones en tiempo real, entre otras variantes.
- **Session Initiation Protocol (SIP)**
  Session Initiation Protocol (SIP) fue desarrollado por la IETF (Internet Engineering Task Force) específicamente para telefonía IP, que a su vez toma ventaja de otros protocolos existentes para manejar parte del proceso de conversión, situación que no se aplica en H.323 ya que define sus propios protocolos bases.

D1.7 EL ESTANDAR DE VoIP

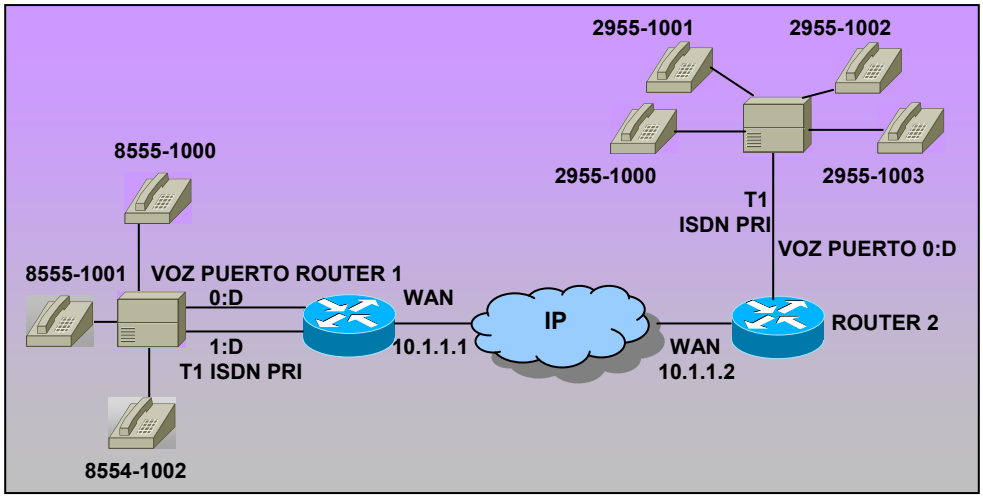


Figura 326 Ejemplo de red con conexión de centralitas a routers CISCO que disponen de soporte VoIP

Es innegable la implantación definitiva del protocolo IP desde los ámbitos empresariales a los domésticos y la aparición de un estándar, el VoIP, no podía hacerse esperar. La aparición del VoIP junto con el abaratamiento de los DSP's (Procesador Digital de Señal), los cuales son claves en la compresión y descompresión de la voz, son los elementos que han hecho posible el despegue de estas tecnologías. Para este auge existen otros factores, tales como la aparición de nuevas aplicaciones o la apuesta definitiva por VoIP de fabricantes como Cisco Systems o Nortel-Bay Networks. Por otro lado los operadores de telefonía están ofreciendo o piensan ofrecer en un futuro cercano, servicios IP de calidad a las empresas. Por lo dicho hasta ahora, vemos que nos podemos encontrar con tres tipos de redes IP:

- **Internet**. El estado actual de la red no permite un uso profesional para el tráfico de voz.
- **Red IP Pública**. Los operadores ofrecen a las empresas la conectividad necesaria para interconectar sus redes de área local en lo que al tráfico IP se refiere. Se puede considerar como algo similar a Internet, pero con una mayor calidad de servicio y con importantes mejoras en seguridad. Hay operadores que incluso ofrecen garantías de bajo retardo y/o ancho de banda, lo que las hace muy interesante para el tráfico de voz.
- **Intranet**. La red IP implementada por la propia empresa. Suele constar de varias redes LAN (Ethernet conmutada, ATM, etc.) que se interconectan mediante redes WAN tipo Frame-Relay/ATM, líneas punto a punto, RDSI para el acceso remoto, etc. En este caso la empresa tiene bajo su control prácticamente todos los parámetros de la red, por lo que resulta ideal para su uso en el transporte de la voz.

A finales de 1997 el VoIP Forum del IMTC ha llegado a un acuerdo que permite la interoperabilidad de los distintos elementos que pueden integrarse en una red VoIP. Debido a la ya existencia del estándar H.323 del ITU, que cubría la mayor parte de las necesidades para la integración de la voz, se decidió que el H.323 fuera la base del VoIP. De este modo, el VoIP debe considerarse como una clarificación del H.323, de tal forma que en caso de conflicto, y a fin de evitar divergencias entre los estándares, se decidió que H.323 tendría prioridad sobre el VoIP. El VoIP tiene como principal objetivo asegurar la interoperabilidad entre equipos de diferentes fabricantes, fijando aspectos tales como la supresión de silencios, codificación de la voz y direccionamiento, estableciendo nuevos elementos para permitir la conectividad con la infraestructura telefónica tradicional. Estos elementos se refieren básicamente a los servicios de directorio y a la transmisión de señalización por tonos multifrecuencia (DTMF). El VoIP/H.323 comprende a su vez una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación:

- **Direccionamiento**:
    1. RAS (Registration, Admision and Status). Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través de el Gatekeeper.
    2. DNS (Domain Name Service). Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS.
- **Señalización**:
    1. Q.931 Señalización inicial de llamada.
    2. H.225 Control de llamada: señalización, registro y admisión, y paquetización/ sincronización del stream (flujo) de voz.
    3. H.245 Protocolo de control para especificar mensajes de apertura y cierre de canales para streams de voz.

- **Compresión de voz**:
    1. Requeridos: G.711 y G.723.
    2. Opcionales: G.728, G.729 y G.722.
- **Transmisión de voz**:
    1. UDP. La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.
    2. RTP (Real Time Protocol). Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.
- **Control de la transmisión**:
    1. RTCP (Real Time Control Protocol). Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.

D1.8 PILA DE PROTOCOLOS EN VoIP

Hasta ahora hemos visto la posibilidad de utilizar nuestra red IP para conectar las centralitas a la misma, pero el hecho de que VoIP se apoye en un protocolo de nivel 3, como es IP, nos permite una flexibilidad en las configuraciones que en muchos casos está todavía por descubrir. Una idea que parece inmediata es que el papel tradicional de la centralita telefónica quedaría distribuido entre los distintos elementos de la red VoIP. En este escenario, tecnologías como CTI (computer-telephony integration) tendrán una implantación mucho más simple. Será el paso del tiempo y la imaginación de las personas involucradas en estos entornos, los que irán definiendo aplicaciones y servicios basados en VoIP. Actualmente podemos partir de una serie de elementos ya disponibles en el mercado y que, según diferentes diseños, nos permitirán construir las aplicaciones VoIP. Estos elementos son:

- Teléfonos IP.
- Adaptadores para PC.
- Hubs Telefónicos.
- Gateways (pasarelas RTC/IP).
- Gatekeeper.
- Unidades de audioconferencia múltiple. (MCU Voz)
- Servicios de Directorio.

Las funciones de los distintos elementos son fácilmente entendibles a la vista de la figura anterior, si bien merece la pena recalcar algunas ideas.

- El Gatekeeper es un elemento opcional en la red, pero cuando está presente, todos los demás elementos que contacten dicha red deben hacer uso de él. Su función es la de gestión y control de los recursos de la red, de manera que no se produzcan situaciones de saturación de la misma.
- El Gateway es un elemento esencial en la mayoría de las redes pues su misión es la de enlazar la red VoIP con la red telefónica analógica o RDSI. Podemos considerar al

Gateway como una caja que por un lado tiene una interfaz LAN y por el otro dispone de uno o varios de las siguientes interfaces:

1. FXO. Para conexión a extensiones de centralitas ó a la red telefónica básica.
2. FXS. Para conexión a enlaces de centralitas o a teléfonos analógicos.
3. E&M. Para conexión específica a centralitas.
4. BRI. Acceso básico RDSI (2B+D).
5. PRI. Acceso primario RDSI (30B+D).
6. G703/G.704. (E&M digital) Conexión especifica a centralitas a 2Mbps.

Los distintos elementos pueden residir en plataformas físicas separadas, o nos podemos encontrar con varios elementos conviviendo en la misma plataforma. De este modo es bastante habitual encontrar juntos Gatekeeper y Gateway. También podemos ver cómo Cisco ha implementado las funciones de Gateway en el router. Un aspecto importante a resaltar es el de los retardos en la transmisión de la voz. Hay que tener en cuenta que la voz no es muy tolerante con estos. De hecho, si el retardo introducido por la red es más de 300 milisegundos, resulta casi imposible tener una conversación fluida. Debido a que las redes de área local no están preparadas en principio para este tipo de tráfico, el problema puede parecer grave. Hay que tener en cuenta que los paquetes IP son de longitud variable y el tráfico de datos suele ser a ráfagas. Para intentar obviar situaciones en las que la voz se pierde porque tenemos una ráfaga de datos en la red, se ha ideado el protocolo RSVP, cuya principal función es trocear los paquetes de datos grandes y dar prioridad a los paquetes de voz cuando hay una congestión en un router. Si bien este protocolo ayudará considerablemente al tráfico multimedia por la red, hay que tener en cuenta que RSVP no garantiza una calidad de servicio como ocurre en redes avanzadas tales como ATM que proporcionan QoS de forma estándar. Podemos resumir diciendo que VoIP es una tecnología que tiene todos los elementos para su rápido desarrollo. Como muestra podemos ver que compañías como Cisco, la han incorporado a su catálogo de productos, los teléfonos IP están ya disponibles y los principales operadores mundiales, están promoviendo activamente el servicio IP a las empresas, ofreciendo calidad de voz a través del mismo. Por otro lado tenemos ya un estándar que nos garantiza interoperabilidad entre los distintos fabricantes. La conclusión parece lógica: hay que estudiar como podemos implantar VoIP en nuestra red.

D1.9 ARQUITECTURA DE RED

El propio estándar define tres elementos fundamentales en su estructura:

- **Terminales:** Son los sustitutos de los actuales teléfonos. Se pueden implementar tanto en software como en hardware. Algunos ejemplos de Hardware: Teléfono IP Video Teléfono IP

Figura 327

- **Gatekeepers:** Son el centro de toda la organización VoIP, y serian el sustituto para las actuales centralitas. Normalmente implementadas en software, en caso de existir, todas las comunicaciones pasarían por él.
- **Gateways:** Se trata del enlace con la red telefónica tradicional, actuando de forma transparente para el usuario.

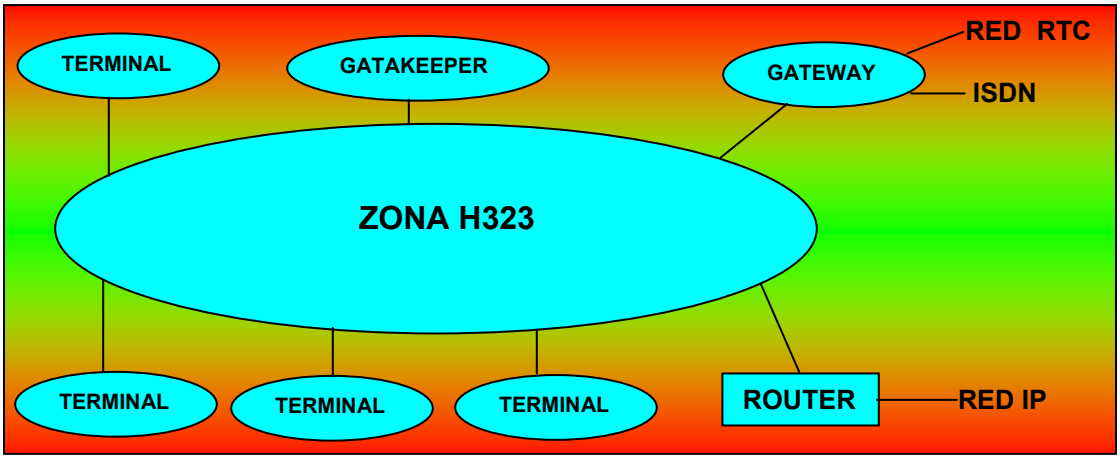


Figura 328

Con estos tres elementos la estructura de la red quedaría como muestra la figura 328 adjunta: El Gateway sirve de enlace entre la RTC/RDSI y la zona H.323 (VoIP). A su vez existe un Gatekeeper que realiza el control de llamadas y la gestión del sistema de direccionamiento. El router permitiría enlazar con otras redes H.323 sin necesidad de utilizar la RTC, resultando todas las llamadas a zonas H.323 totalmente gratuitas, con la ventaja de ahorro de costos que esto supone para las empresas.

D1.10 CALIDAD DEL SERVICIO (QoS)

- **Anchos de Banda:** En la tabla 45 adjunta se muestra la relación existente entre los distintos algoritmos de compresión de voz utilizados y el ancho de banda requerido por los mismos:

VoCodecs	Ancho de Banda (BW)
G.711 PCM	64kbps
G.726 ADPCM	16, 24, 32, 40kbps
G.727 E-ADPCM	16, 24, 32, 40kbps
G.729 CS-ACELP	8kbps
G.728 LD-CELP	16kbps
G.723.1 CELP	6.3 / 5.3kbps

Tabla 45 Ancho de Banda requerido por los VoCodecs actuales

- **Retardo:** Una vez establecidos los retardos de tránsito y el retardo de procesado la conversación se considera aceptable por debajo de los 150 ms.
- **Calidad de servicio:** Este es el principal problema que presenta hoy en día la implantación tanto de VoIP como de todas las aplicaciones de VoIP. Garantizar la calidad de servicio sobre una red IP, en base a retardos y ancho de banda, actualmente no es posible, es por eso que se presentan diversos problemas en cuanto a garantizar la calidad del servicio. La calidad de servicio se está logrando en base a los siguientes criterios:
    1. La supresión de silencios, otorga más eficiencia a la hora de realizar una transmisión de voz, ya que se aprovecha mejor el ancho de banda.
    2. Compresión de cabeceras aplicando los estándares RTP/RTCP.
    3. Priorización de los paquetes que requieran menor latencia. Las tendencias actuales son: **CQ** (**Custom Queuing**). Asigna un porcentaje del ancho de banda disponible. **PQ** (**Priority Queuing**). Establece prioridad en las colas. **WFQ** (**Weight Fair Queuing**). Se asigna la prioridad al tráfico de menos carga. **DiffServ**: Evita tablas de encaminados intermedios y establece decisiones de rutas por paquete.

4. La implantación de IPv6 que proporciona mayor espacio de direccionamiento y la posibilidad de tunneling.

D1.11 APLICACIONES DE VoIP

VoIP proporcionaría a las delegaciones de una misma empresa, comunicaciones gratuitas entre ellas, con el ahorro de costos que esto supondría. No solo entre sus delegaciones, sino entre proveedores, intermediarios y vendedores finales, las comunicaciones se podrían realizar de forma completamente gratuita. Además, la red de comunicaciones de la empresa se vería enormemente simplificada, ya que no habría que cablear por duplicado la red, debido a que se aprovecharía la red de datos para voz. Entre las aplicaciones para las que esta tecnología que supondrán una gran cantidad de ventajas podemos citar:

- **Centros de llamadas por el WEB:** Partiendo de una tienda que ofrece sus productos on-line, los visitantes de la Web no sólo tendrán acceso a la información que la Web les proporciona, sino que además podrían establecer comunicación directa con una persona del departamento de ventas sin necesidad de cortar la conexión. Esta cualidad reduciría el enorme temor del usuario a hacer sus compras por Internet por primera vez. Al establecer una conversación directa, le da una confianza que a la postre supondrá una mejora en su relación con el e-commerce.
- **Multiconferencia:** Con los datos de ancho de banda requeridos actualmente (de 8 a 16kbps por llamada), se podrían establecer de 15 a 30 comunicaciones simultáneas con una línea ADSL estándar, que podría satisfacer los requerimientos de una mediana empresa.
- **Posibilidad de usar Push 2 Talk:** De esta forma, con el simple gesto de pulsar un botón se establece comunicación directa con la persona que lo ha elaborado.

D1.12 INICIOS DE LA TECNOLIGIA DE VoIP

D1.12.1 INICIOS

La VoIP inicialmente se implementó para reducir el ancho de banda mediante compresión vocal, aprovechando los procesos de compresión diseñados para sistemas celulares en la década de los años 80. En consecuencia, se logró reducir los costos en el transporte internacional. Luego tuvo aplicaciones en la red de servicios integrados sobre la LAN e Internet. Con posterioridad se migró de la LAN (aplicaciones privadas) a la WAN (aplicaciones públicas).

D1.12.2 EL MERCADO DE SERVICIOS DE VoIP: ES TAN SOLO EL COMIENZO

Evolución del mercado de la Voz sobre IP	
1995	Año del aficionado
1996	Año del cliente
1997	Año del gateway
1998	Año del gatekeeper
1999	Año de la aplicación

Tabla 46

A fines de 1996, la VoIP aún era considerada una especie de "radio de aficionados" en Internet, una aplicación para un pequeño grupo de amateurs que poseían estaciones de trabajo con PC

ataviadas con configuraciones elaboradas de parlantes, micrófonos y shareware de VoIP. La calidad era terrible, no existían normas, y para poder hablar con alguien era necesario llamar primero por teléfono de la manera tradicional para averiguar si estaban conectados.

D1.12.3 LAS PRIMERAS BARRERAS

A pesar de que en ese año (1996) proliferó el software nuevo de VoIP para clientes, la falta de normas y la necesidad de utilizar una tosca PC como dispositivo de usuario final desalentaron a los primeros posibles seguidores que esperaban calidad y eficiencia así como originalidad. La tecnología de VoIP para el mercado empresarial era prácticamente inexistente y los primeros gateways (dispositivos de acceso que pasan las llamadas hacia y desde Internet u otras redes IP, que permiten utilizar teléfonos convencionales) estaban muy lejos de la "clase carrier". Pero no cabe duda de que las cosas hayan cambiado. Varios años de investigación y desarrollo intensos en todas las áreas de las industrias de las redes y las telecomunicaciones dieron lugar a un mercado en el cual las grandes empresas telefónicas tradicionales no sólo reconocen que la telefonía sobre IP es viable sino que también la están adoptando. Hoy en día, la telefonía sobre IP no constituye una simple fuente potencial de ingresos para los proveedores de servicios de todas las formas y tamaños; los analistas y los actores industriales la consideran cada vez más el nuevo paradigma de las comunicaciones de voz y datos del próximo siglo.

D1.12.4EL MERCADO DECIDE

Al lograr normas de interoperabilidad y la existencia de gateways de clase carrier disponibles, los proveedores de equipos y servicios por igual pueden concentrarse en desarrollar las aplicaciones de valor agregado que se necesitan para llevar la demanda de la telefonía sobre IP más allá de su uso inicial como una alternativa de bajo costo ante los servicios tradicionales de larga distancia.

D1.12.5 COMPARACION VoIP Y TELEFONIA TRADICIONAL

VoIP es transmitir Voz utilizando IP. Si bien es una tecnología novedosa, tiene muchas características similares y otras diferentes a las de la telefonía tradicional.
Por eso, a continuación se explica brevemente el esquema de una red telefónica tradicional, y luego las coincidencias y diferencias con la tecnología de VoIP.

D1.12.6 TELEFONIA TRADICIONAL

El servicio telefónico es, junto con la red eléctrica, uno de los más confiables que conocemos y usamos, ya que todo es muy redundante y está pensado para funcionar siempre. Una central telefónica está diseñada para minimizar los tiempos de interrupción del servicio. Es una tecnología en que la interfaz es muy importante, la gente la conoce, espera que cuando levanta el teléfono se escuche el tono, y si no es el mismo que el que esperaba escuchar, molesta; además es muy universal y difundida. Todo esto se tiene en cuenta a la hora de prestar el servicio telefónico.

D1.12.6.1 ARQUITECTURA DE UNA CENTRAL TELEFONICA

Todos tenemos un teléfono en nuestra casa. Y, en general, sabemos que el cable del teléfono tiene una conexión (RJ-11) parecida a la del cable de red, y que dentro tiene dos cables de cobre, al que se denomina par telefónico. Ese par telefónico es el que va hasta la central telefónica, a una placa que se la suele denominar placa de abonado. Es la placa que controla nuestra línea. En realidad, puede controlar muchas líneas, no una sola, y tiene una densidad de puertos que depende del fabricante, ronda entre los 8 y 16 abonados (a veces más, a veces menos). El valor exacto depende del equipo en particular. La central telefónica es un conjunto de equipos relacionados. Todo este conjunto forma un equipo muy grande que puede llegar a ocupar varias habitaciones. Como mencionamos, las centrales telefónicas suelen estar diseñadas para tener una muy alta disponibilidad (se suele decir que son carrier class, dado que se dice están disponibles el 99.9% del tiempo, que representa alrededor de 5 minutos al año de interrupción de servicio). Para

lograr este objetivo, cuentan con redundancia en múltiples niveles (procesadores, enlaces, etc.); y en general se conectan a un sistema de energía interrumpida, que tiene un buen número de baterías que se conectan a un grupo electrógeno que se activa cuando se corta la luz.

D1.12.6.2 PROCESAMIENTO DE LLAMADAS

Hasta la central, la voz va en forma analógica. Actualmente ya no existen centrales analógicas, todo lo que hay desde que llega la señal a la central y sale de la otra central hacia el otro abonado, es digital. La placa de abonado es la que se encarga de hacer la conversión de una señal analógica a una digital y viceversa. La señal se convierte a un PCM de 64kbps, que es una señal digital sin pérdida de información y sin compresión, es el formato que se está utilizando desde prácticamente sus comienzos. También es la placa de abonado la que decodifica los tonos de discado (DTMF). Es decir que, se utiliza el concepto de señalización en banda: comandar a la central utilizando la misma banda por la que se habla.

D1.12.6.3 CONEXIÓN ENTRE CENTRALES

La llamada que sale de nuestra central tiene que llegar hasta la central donde está la persona con la que queremos hablar. No hay doscientos millones de cables entre una y otra, sino que hay un enlace, el cual puede ser de diversos tipos. Este enlace se debe multiplexar para que todos los abonados de la central puedan hablar por teléfono. Esta multiplexación es la que hace una diferencia a la hora de la calidad del servicio para el usuario. El sistema de multiplexación que utilizan las centrales telefónicas se llama TDM: Time Division Multiplex. Consiste en dividir el stream de datos en partes iguales de 64k (llamadas time-slots), de manera que los datos correspondientes al primer abonado van en el primer time-slot, los correspondientes al segundo en el segundo, y así sucesivamente. Suponiendo un enlace de 2Mbps de ancho de banda, como se transmiten 64k, podría haber hasta 32 abonados hablando a la vez. Con esta multiplexación en tiempo se separan y luego vuelven a unir los streams de voz que van de una central a otra, de manera transparente para el que lo está utilizando. Lo bueno de esta tecnología es que como se divide por un tiempo fijo, se puede garantizar el time-slot y saber que siempre lo que corresponde al primer abonado va en el primer time-slot y así. Una vez establecida la comunicación, sea de aquí a una cuadra o de aquí a China, está garantizado el ancho de banda necesario para poder hablar sin interrupciones. Esto, en particular, es muy opuesto a lo que es IP, o cualquier enlace de paquetes en los que pueda haber colisiones, se pierdan paquetes, etc. Ya que en esos enlaces es muy difícil garantizar que la calidad inicial se mantenga a lo largo de toda la conversación, puede pasar que haya paquetes que lleguen antes que otros, que se sature la conexión y muchos otros factores que afectan a la calidad final del audio. En definitiva, TDM es una de las diferencias esenciales entre la telefonía común y la de Voz sobre IP, permite tener una red predictiva y garantizar calidad.

D1.12.6.4 RUTEO, SEÑALIZACION Y PROTOCOLOS

Un tema importante es el "ruteo" entre centrales, es decir, como sabe la central del abonado con que central se tiene que conectar. Vamos a denominar señalización a la información relacionada con una llamada que se transmite entre dos equipos (la definición en sí es más amplia, pero esto es en particular lo más relevante para el caso). Podemos dividirla en dos grupos: la que refiere al abonado y las llamadas en sí (levantó, marcó, cortó), y otra parte entre las centrales A través de la señalización, la central puede ubicar a que otra central tiene que llamar, a qué abonado dentro de esa central hay que llamar, saber que se cortó la comunicación, que dio ocupado, etc. Las centrales entre sí se comunican utilizando diversos protocolos, los cuales generalmente son estándares públicos, aunque en muchos casos las especificaciones no son fáciles (o baratas) de conseguir. Los protocolos más comunes son tres: R2, PRI y SS7. R2 es uno de los más viejos y tiene muchas variantes distintas. SS7 es, por otra parte, uno de los más nuevos y complejos. Se necesita que las dos centrales que se están queriendo comunicar puedan hablar un mismo protocolo, de manera que si se quieren intercomunicar dos centrales que no soportan los mismos protocolos, es necesario que utilicen una central intermedia que traduzca la información. Acerca

del enlace por el cual se pasa tanto la señalización como la voz en sí, existen muchísimos tipos. Los más conocidos y comunes son E1 o E3 (europeos), con sus variantes T1 o T3 (utilizadas principalmente en los Estados Unidos). Son cables de cobre, muy parecidos al cable coaxial, que pueden ser de 75 o 120 ohms. El E1 tiene 2Mbps (32 canales de 64kbps), el E3 tiene 32Mbps (512 canales de 64kbps).
En muchos ámbitos cuando se habla de este tipo de enlaces se le da importancia sólo al ancho de banda; sin embargo en nuestro caso también nos interesa el número de times slots en el cual se puede dividir. Sin embargo, no se pueden ocupar todos los canales para pasar todos los abonados. En necesario poder avisar que hay llamadas y ese tipo de información. Por ejemplo, en el caso de una E1 se suelen utilizar 30 canales para el paso de la voz, 1 para framing (el 0) y 1 para señalización (el 15). En el de framing se suele encontrar (entre otras cosas) el CRC de los otros 31 (aunque depende de la configuración), de manera que si un determinado frame esta corrupto, se lo puede notar y actuar en consecuencia. Para telefonía IP hay muchos protocolos. Los vamos a separar en 3 partes: codificación de la voz, transmisión de la voz y señalización.

D1.12.6.4.1 CODIFICACION DE LA VOZ

La transmisión ya no se va a hacer en PCM (protocolo G.711), como en la telefonía tradicional. La voz se puede comprimir: si una persona se queda callada, por ejemplo, no es necesario transmitir el sonido completo del silencio. Hay muchos codecs de compresión. Como todo codec, cuanto más se comprime, más procesador se necesita. Hay codecs con pérdida que comprimen de 64k a 4k, incluso hasta 3.1k. Hay algunos que son sin pérdida, pero la mayoría son con pérdida. Hay muchos estudios al respecto, ya que lo más importante es la percepción que tiene la gente de lo que se escucha, y es muy difícil medir la percepción humana. Para la realización de estos estudios, se comprime el audio y se pide a grupos de personas que lo escuchen y que manifiesten si les parece que es de buena calidad o no, se les asignan puntajes, etc. En general se elige un balance entre compresión y percepción. Hay muchos balances distintos. Hay muchos codecs que están patentados, para los que hay que pagar las licencias de uso (no la implementación, sino el uso en sí). Un ejemplo de un buen codec es el GSM, utilizado en los teléfonos celulares. Es un codec libre, que se escucha bastante bien, comprime bastante bien, y consume muy poco procesador. Que consuma poco procesador es importante cuando se está trabajando a gran escala (200,1000 líneas). En el caso de los celulares, la voz se comprime en el mismo aparato celular y se transmite ya comprimida. Para este protocolo, en GNU/Linux existe la libgsm que es una biblioteca pequeña y útil.

D1.12.6.4.2 SEÑALIZACION

Tal como vimos anteriormente, es necesario tener un protocolo para poder indicar a qué máquina se quiere llamar y demás. Existen actualmente varios protocolos para señalización.
Uno que está cayendo muy en desuso es el H323. No es lindo, no es fácil, y no anda con NAT; pero es muy importante porque fue el primero que se empezó a usar en VoIP de forma masiva. Actualmente se está dejando de usar, y probablemente en el futuro no se use más. Los programas NetMeeting, y su equivalente libre GnomeMeeting utilizan este protocolo.
El protocolo que más se está usando actualmente es SIP: Session Initiation Protocol. Se trata de un protocolo que tiene una característica muy particular: está estandarizado por la IETF (Internet Engineering Task Force) y, en consecuencia, es muy abierto y de fácil acceso.
SIP es un protocolo de texto plano que se utiliza sobre TCP, ya que en el caso de la señalización es importante que no se pierda la información. Tiene una arquitectura que está muy bien pensada, no trata de meter todo el mundo telefónico en IP, ni todo IP en el mundo telefónico. Sin embargo, también tiene problemas para atravesar NAT. Normalmente, cuando se usa SIP, el protocolo que se utiliza para enviar la voz es RTP (Real Time Protocol), que se usa sobre UDP. El programa linphone es un cliente SIP. Existe linphonec para consola (paquete linphone-nox en Debian).

D1.12.6.4.3 EJEMPLO DE CONEXIÓN VoIP USANDO IP

A modo de ejemplo, vamos a considerar dos PC's que están conectadas a través de Internet. Juan, que está conectado desde una PC quiere hablar con María, que está conectada desde otra. A María le llega un invite que le indica que Juan quiere hablar con ella (equivalente a un RING), y si acepta la comunicación (equivalente a levantar el teléfono), puede hablar con Juan.
La conexión se establece usando SIP sobre TCP y luego la transmisión se hace usando RTP sobre UDP. Cuando se termina la conversación, por SIP se transmite la terminación de la conexión. Esto permite que dos usuarios de PC puedan hablar por teléfono, sin tener una central telefónica en el medio, utilizando la estructura IP existente para establecer una comunicación. Durante la inicialización se pasan las IP's y los puertos a utilizar y por eso es que es difícil hacerlo a través de NAT.

D1.12.6.4.4 CONEXIÓN DE MUCHAS COMPUTADORAS

Si en lugar de 2 PC's se quiere conectar un número importante de computadoras, que quieren hablar entre sí sin tener que estar transmitiéndose los números de IP, y el que les está proveyendo el servicio quiere poder tener un registro de las comunicaciones establecidas, se utiliza un Server SIP (que vendría a ser el equivalente a un Gatekeeper en H323). También se lo suele llamar Proxy SIP o Router SIP, que si bien teóricamente cumplen funciones específicas, en general se utilizan los términos de manera indistinta. Teniendo un server, cuando Juan quiere hablar por teléfono, le envía una señal al server indicándole que quiere hablar con María, y este le avisa a María que Juan quiere hablar con ella. A partir de que se acepta la comunicación, se pasan algunos mensajes más a través del server (utilizando SIP) para negociar IP's, puertos, protocolo de compresión a utilizar, etc. Pero una vez que comienza la comunicación, el canal UDP ya no pasa por el server. Una vez terminada la conversación, se utiliza SIP para avisar que se terminó la conversación. Esta es una de las mejores cosas que tiene la telefonía IP, porque por un lado separa la señalización de la transmisión de voz, y por el otro lado la transmisión se hace peer to peer. Pero trae consigo que el server debe confiar en la buena fe de los clientes para saber cuándo una comunicación se terminó realmente. Un cliente que tenga DHCP tiene que avisarle al server en qué IP está, para esto puede autentificarse contra él, utilizando un nombre de usuario y una clave. De manera que el server puede saber que un determinado usuario no está y poner un contestador, dar ocupado, etc. Con este principio se puede hacer que un teléfono VoIP se enchufe en cualquier lugar del mundo donde haya banda ancha y siempre sigue siendo el mismo teléfono. Y de hecho este servicio existe y se vende: Por ejemplo, si a usted le dan una línea en cualquier parte del mundo y quiere llevarse el teléfono VoIP a cualquier lugar, lo puede enchufar a un ADSL y puede hablar o lo pueden llamar como si usted estuviera en el mismo lugar. De la misma manera que con las centrales telefónicas, puede haber varios servers que se comuniquen entre sí, y solamente van a intercambiar la parte correspondiente al protocolo SIP, la parte de RDP/UDP se hace directo entre los dos puntos que se están comunicando. La implementación de referencia del server SIP es Open Source. Por otro lado, se puede hablar desde una computadora a teléfonos comunes, para esto se necesita un gateway que haga la conversión de una tecnología a otra.

D1.12.6.4.5 IMPLEMENTACIONES

A nivel personal, por ejemplo usted o puede hablar con una tía que viva en algún lugar distante a través de VoIP, y otro día, hablar por teléfono de verdad. Es una opción para ahorrar costos. Pero, cuando se habla de una implementación a nivel telefonía real (como la de las tarjetas para hacer llamadas baratas) es diferente, tiene que ir por un enlace controlado. Si se tiene un enlace de fibra es posible pasar muchos más abonados por el mismo enlace E1 por el que se pasaban 30; pero es necesario poner controles en ambas puntas. Hay que tener mucha inteligencia en los equipos de control. Una posibilidad para tener una red de VoIP interna, por ejemplo, es tener unos auriculares y un micrófono en cada estación. Y por otro lado, tener un gateway que se encarga de hacer la conversión a la telefonía tradicional. Para ello, es necesario tener algún contacto con la telefonía tradicional, una E1, 4 líneas telefónicas, etc.

En el caso de la E1, hará falta tener el hardware que se encargue de hacer TDM, para las líneas telefónicas, es necesario tener placas especiales que se conectan a líneas telefónicas.

D1.12.6.4.6 PBX

Las centralitas telefónicas personales o de pequeñas empresas, se llaman PBX. Hay software para VoIP o voz común que permite tener tu propia PBX. Asterix (dual licence GPL y otra comercial) y Bayonne (que es GNU y no es tan completo o estable). Asterix está muy bien pensado. Puede manejar ALSA y usar la placa de sonido. También tiene soporte para placas ISDN, E1, placas telefónicas, y placas que conectan teléfonos (quick jack)

.

D1.13 VENTAJAS Y DESVENTAJAS QUE PRESENTA LA SOLUCION DE VoIP CON RESPECTO A LA TELEFONIA TRADICIONAL

D1.13.1 VENTAJAS

- **Un único número de teléfono** Casi como un celular, si tenemos una conexión a Internet en nuestro departamento y en la casa de fin de semana, el número telefónico será el mismo. Mejor aún, si nos llevamos una notebook al Boliche y la conectamos a la red, tenemos el mismo número de teléfono. Le permite tener un número de teléfono local que transfiera las llamadas de sus familiares y amigos a cualquier parte del mundo que usted elija. Así sus familiares y amigos podrán hablar con usted por sólo el costo de una llamada local mientras usted paga por el consumo de minutos.
- **Ahorro en llamadas de larga distancia** Las mayores ventajas que va a ver un usuario hogareño es la del ahorro en las llamadas de larga distancia ya que las comunicaciones no dependerán del tiempo en el aire. Es decir no dependerá de la duración de la llamada, como estamos acostumbrados hasta ahora, sino más bien por el precio de mercado del proveedor de Internet, ya que estaremos pagando por un servicio más dentro del paquete de datos que nos brinda la red.
- **Llamadas a teléfonos fijos o celulares** Otra gran ventaja de la telefonía IP es que se puede llamar a un teléfono fijo o móvil en cualquier lugar del mundo para transmitir fax, voz, vídeo, correo electrónico por teléfono, mensajería y comercio electrónico. Es decir, la gran variedad de servicios brindados por un sólo operador es una de las grandes ventajas que ven los usuarios hogareños y corporativos.
- **Reducción del abono telefónico** Además, para el usuario común, este sistema reduce los costos de las llamadas (hasta un 74%), cuyo precio depende del mercado pero no del tiempo de conexión, como sucede en la telefonía tradicional; así, donde antes "cabía" una conversación ahora "caben" 10, lo cual reducirá las tarifas para el usuario final.
- **Mensajería unificada y Correo de voz** Cuando está de viaje o fuera de su casa u oficina en vez de marcar su teléfono y clave para escuchar su casilla de mensajes imagínese un sistema telefónico que le proporcione, en su computadora, un listado de esos mensajes y que le permita escucharlos y marcar teléfonos de su libro electrónico de direcciones con un simple click en su ratón. La tecnología VoIP le permite realizar llamadas telefónicas y enviar faxes a través de una red de datos IP como si estuviese utilizando una red tradicional.
- **Ventajas para las empresas** Esta convergencia de servicios de voz, datos y video en una sola red implica para una empresa que lo adopte, un menor costo de capital, procedimientos simplificados de soporte y configuración de la red y una mayor integración de las ubicaciones remotas y oficinas sucursales en las instalaciones de la red corporativa. La Telefonía IP utiliza la red de datos para proporcionar comunicaciones de voz a toda la empresa, a través de una sola red de voz y datos. Es evidente que el hecho de tener una red en vez de dos, es beneficioso para cualquier organización. VoIP proporcionaría a las sucursales de una misma empresa, comunicaciones gratuitas entre ellas, con el ahorro de costos que esto supondría. No sólo entre sus sucursales, sino entre proveedores, intermediarios y vendedores finales, las comunicaciones se podrían realizar de forma completamente gratuita. Además, la red de comunicaciones de la empresa se vería

enormemente simplificada, ya que no habría que cablear por duplicado la red, debido a que se aprovecharía la red de datos para voz. Esta capacidad permite a las compañías reducir los costos de fax y teléfono, agrupar los servicios de datos, voz, fax y vídeo, y construir nuevas infraestructuras de red para aplicaciones avanzadas de comercio electrónico.

- **Centros de llamadas por el Web** Partiendo de una tienda que ofrece sus productos en línea, los visitantes de la Web no sólo tendrán acceso a la información que la Web les proporciona, sino que además podrían establecer comunicación directa con una persona del departamento de ventas sin necesidad de cortar la conexión. Esta cualidad reduciría el enorme temor del usuario a hacer sus compras por Internet por primera vez. Al establecer una conversación directa, le da una confianza que finalmente supondrá una mejora en su relación con el comercio electrónico.
- **Videoconferencia integrada o Multiconferencia** Con los datos de ancho de banda requeridos actualmente (de 8 a 16kbps por llamada), se podrían establecer de 15 a 30 comunicaciones simultáneas con una línea ADSL estándar, que podría satisfacer los requerimientos de una mediana empresa.
- **Posibilidad de usar Push 2 Talk** De esta forma, con el simple gesto de pulsar un botón se establece comunicación directa con la persona que lo ha elaborado.
- **Ventajas para los operadores o proveedores del servicio** Es obvio que este tipo de redes proporciona a los operadores una relación ingreso/recursos mayor, es decir, con la misma cantidad de inversión en infraestructura de red, obtienen mayores ingresos con las redes de conmutación de paquetes, pues puede prestar más servicio a sus clientes. Otra posibilidad sería que prestará más calidad de servicio, velocidad de transmisión, por el mismo precio.

D1.13.2 DESVENTAJAS

- **Calidad de la comunicación** Algunas de sus desventajas son la calidad de la comunicación (ecos, interferencias, interrupciones, sonidos de fondo, distorsiones de sonido, etc.), que puede variar según la conexión a Internet y la velocidad de conexión del Proveedor de servicios de Internet. Garantizar la calidad de servicio sobre una red IP, actualmente no es posible por los retardos que se presentan en el tránsito de los paquetes y los retardos de procesado de la conversación. Por otro lado el ancho de banda el cual no siempre está garantizado, hace desmejorar el servicio. Estos problemas de calidad en el servicio telefónico en el protocolo IP van disminuyendo a medida que las tecnologías involucradas van evolucionando, ya en los Estados Unidos hay servicios que garantizan una excelente calidad en la comunicación.
- **Conexión a Internet** Sólo lo pueden usar aquellas personas que posean una conexión con Internet, tengan computadora con módem y una línea telefónica; algunos servicios no ofrecen la posibilidad de que la PC reciba una llamada, ni tampoco funcionan a través de un servidor proxy.
- **Pérdida de información** Este tipo de redes transportan la información dividida en paquetes, por lo que una conexión suele consistir en la transmisión de más de un paquete. Estos paquetes pueden perderse, y además no hay una garantía sobre el tiempo que tardarán en llegar de un extremo al otro de la comunicación. Imaginemos una conversación de voz en la cual se pierde de vez en cuando información emitida y que sufre retrasos importantes en su cadencia. Si alguna vez han chateado, entenderán la situación. A veces durante estas conversaciones de Chat, recibimos dos o tres preguntas seguidas de nuestro interlocutor, y es que como lo que nosotros escribimos no le llega, pues él sigue con otras preguntas. Estos problemas de calidad de servicio telefónico a través de redes de conmutación de paquetes van disminuyendo con la evolución de las tecnologías involucradas, y poco a poco se va acercando el momento de la integración de las redes de comunicaciones de voz y datos.
- **Incompatibilidad de proveedores del servicio** No todos los sistemas utilizados por los Proveedores de Servicios de Telefonía por Internet son compatibles (Gateway, Gatekeeper) entre sí. Este ha sido uno de los motivos que ha impedido que la telefonía IP

se haya extendido con mayor rapidez. Actualmente esto se está corrigiendo, y casi todos los sistemas están basados en el protocolo H.323. El estándar VoIP o protocolo fue definido en 1996 por la ITU (International Telecommunications Union) y proporciona a los diversos fabricantes una serie de normas con el fin de que puedan evolucionar en conjunto. Por su estructura el estándar proporciona las siguientes ventajas: Permite el control del tráfico de la red, por lo que se disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento de las redes de datos. Proporciona el enlace a la red telefónica tradicional. Al tratarse de una tecnología soportada en IP es independiente del tipo de red física que lo soporta. Permite la integración con las grandes redes de IP actuales. Es independiente del hardware utilizado. Y permite ser implementado tanto en software como en hardware, con la particularidad de que el hardware supondría eliminar el impacto inicial para el usuario común.

D1.14 TELEFONIA SOBRE IP: COMO CAMBIARLE LA CARA A LAS TELECOMUNICACIONES

Frente al constante cambio de las telecomunicaciones, la telefonía sobre IP es excepcionalmente prometedora. Ante un mercado global cada vez más competitivo, las compañías telefónicas ya existentes, los proveedores de servicios de Internet (ISP's), las operadoras locales competitivas emergentes (CLEC's) y las PTT's (autoridades de correo, teléfonos y telégrafos), buscan, en forma constante, maneras de aumentar sus ofertas de servicios. La telefonía sobre IP ha captado la atención de dichos proveedores de servicios en todo el mundo, ofreciendo una amplia gama de servicios nuevos y reduciendo al mismo tiempo sus costos de infraestructura. La VoIP está cambiando el paradigma de acceso a la información, fusionando voz, datos y funciones multimedia en una sola infraestructura de acceso convergente. Mediante la telefonía sobre IP, los proveedores de servicios pueden ofrecer servicios de voz básicos y ampliados a través de Internet, incluyendo la llamada en espera en Internet, el comercio en la web por telefonía ampliada y comunicaciones interactivas de multimedia. Estos servicios se integrarán de manera interrumpida a las redes conmutadas existentes (PSTN) a fin de permitir que se originen o terminen llamadas en teléfonos tradicionales según sea necesario. Dado que IP es una norma abierta, VoIP le brinda a los proveedores de servicios flexibilidad para personalizar sus servicios existentes e implementar nuevos servicios con mayor rapidez y eficiencia en función de los costos, incluso en áreas remotas dentro de su región.

D1.15 COMO FUNCIONA LA VoIP

La voz sobre IP convierte las señales de voz estándar en paquetes de datos comprimidos que son transportados a través de redes de datos en lugar de líneas telefónicas tradicionales. La evolución de la transmisión conmutada por circuitos a la transmisión basada en paquetes toma el tráfico de la red pública telefónica y lo coloca en redes IP bien aprovisionadas. Las señales de voz se encapsulan en paquetes IP que pueden transportarse como IP nativo o como IP por Ethernet, Frame Relay, ATM o SONET. Hoy, las arquitecturas interoperables de VoIP se basan en la especificación H.323 v2. La especificación H.323 define gateways (interfaces de telefonía con la red) y gatekeepers (componentes de conmutación interoficina) y sugiere la manera de establecer, enrutar y terminar llamadas telefónicas a través de Internet. En la actualidad, se están proponiendo otras especificaciones en los consorcios industriales tales como SIP, SGCP e IPDC, las cuales ofrecen ampliaciones en lo que respecta al control de llamadas y señalización dentro de arquitecturas de voz sobre IP.

D1.16 LA PROMESA DE VoIP: MEJORAR LA CALIDAD DE LA VOZ

Existen opiniones encontradas acerca de la calidad de las llamadas de voz que se realizan por Internet. Vale la pena destacar que los carriers utilizarán particiones de backbones de IP bien diseñadas para transportar el tráfico de voz sobre IP, simplemente debido a que Internet tiene patrones de tráfico impredecibles y no fue desarrollado para manejar el tráfico de la telefonía de clase carrier. La demora y la pérdida de paquetes durante los períodos de alto nivel de tráfico en Internet degradan la calidad del tráfico altamente sensible a las demoras como ocurre en el caso

de la voz en tiempo real. La transformación de la voz en Internet puede mejorarse de manera notoria mediante el uso de algoritmos tales como la corrección de errores sin retorno y la protección de paquetes. Las redes analógicas conmutadas por circuitos están limitadas por el legado de la red multiplexión por división de tiempo subyacente, que se basa en 8,000 muestras de voz, o cuatro kilohertz, por segundo. Para ponerlo en perspectiva, la voz humana genera hasta 10khz/segundo y el oído humano puede detectar sonidos de hasta 20,000khz/segundo. Dado que la telefonía sobre IP no está limitada a la multiplexión por división de tiempo, tanto las empresas como los consumidores por igual podrán, en poco tiempo, beneficiarse por una calidad de sonido notablemente superior.

D1.17 LA VOZ SOBRE INTERNET

La voz sobre Internet será, dentro de muy poco tiempo, popular entre los usuarios a causa de su bajo costo (al menos por ahora), necesitar una estructura simple de comunicaciones y por la posibilidad de ofrecer servicios de valor añadido como pueden ser los buzones de voz y la mensajería vocal, aunque difícilmente ofrecerá una calidad tan buena como la que ofrece la red telefónica clásica y una sencillez de uso que hace que cualquier usuario, sin necesidad de formación alguna, sepa utilizarla. La telefonía sobre Internet o Voz sobre IP (VoIP) es más económica que la convencional porque el sistema de encaminamiento y conmutación es más eficiente que al de las grandes centrales telefónicas, que necesitan un circuito por cada conversación, mientras que en IP la información se trocea en paquetes y se pueden enviar varias conversaciones multiplexadas sobre un único circuito físico. La VoIP lleva camino de ser un fenómeno tan importante como lo está siendo el de la telefonía móvil. Para establecer una comunicación de voz utilizando la red Internet, lo primero que se necesita es establecer la conexión entre las dos terminales de los usuarios, equipados con el mismo software o compatible, que desean comunicarse, es decir establecer una sesión IP; a partir de ahí, se digitaliza la voz, se comprime para que ocupe menos ancho de banda, y se transmite a través de la red como si fuese un flujo de datos. La comunicación puede ser multimedia y transferirse ficheros o ver un vídeo mientras se conversa. El atractivo que representa esta solución reside en que en este caso las tarifas que aplican son las propias de Internet, es decir siempre tarifa local en ambos extremos y en muchos casos tarifa plana, en lugar de las telefónicas, que dependen de la distancia y del tiempo de conexión. El usuario admite la peor calidad de la comunicación, que se ve compensada por el ahorro económico que obtiene. Existen otras dos modalidades que se dan en el caso de establecer la comunicación entre un teléfono y una PC o bien entre dos teléfonos, utilizando Internet. En el primer caso es necesario disponer de un gateway con conexión por un lado a Internet y por otro a la RTC, que digitalice la voz si es que ya no lo está, la comprima y empaquete y realice la traslación entre direcciones IP y números de la RTC, realizando el proceso simultáneamente en ambos sentidos. En el caso de llamadas entre teléfonos a través de Internet, el proceso es parecido, utilizando dos gateways, uno en cada extremo, siendo varias las compañías que ofrecen estos servicios aprovechando la ventaja económica que supone encaminar las llamadas normales de voz a través de la red. Los estándares para la comunicación telefónica sobre Internet, utilizando terminales aislados o conectados a una PBX, están ya definidos por el ITU-T, (H-323) y varios fabricantes, entre ellos Intel y Microsoft, están trabajando para desarrollar software con este propósito. Llevar la voz sobre Internet se consigue utilizando técnicas de compresión muy potentes que permiten pasarla sobre un ancho de banda muy pequeño y un software de codificación-decodificación, junto con el protocolo IP. En la PC del usuario se necesita una tarjeta de sonido dúplex, micrófono y altavoces, junto con uno de los paquetes comerciales basados en el estándar mencionado. Por ahora, los proveedores de VoIP no necesitan ninguna licencia para ofrecer el servicio, al menos en Europa, ya que la Comisión Europea no considera este servicio como telefonía básica, al no cumplir los cuatro requisitos básicos siguientes:

- Ser objeto de una oferta comercial independiente.
- Ser accesibles a todo el público.
- Permitir la comunicación con cualquier otro usuario.
- Implicar el transporte de voz en tiempo real, con una mínima calidad de servicio.

El operador de telefonía con el servicio VoIP puede ofrecer tarifas planas y empaquetar los servicios de voz, datos y multimedia según los perfiles de los grupos de clientes, lo que le dota de una ventaja competitiva frente a terceros que no cuenten con este servicio en su cartera de productos.

D1.18 UNA LINEA PARA DOS COMUNICACIONES

Desde el lugar de trabajo y desde casa, el acceso a Internet se hace a través de los dos hilos que nos conecta con la central telefónica local, usando la RTC o la RDSI y un módem o adaptador de terminal; si es por RTC sólo se dispone de una línea y es obvio que cuando estamos conectados con la red no podemos recibir o hacer llamadas telefónicas. Mientras que la duración media admitida para una llamada telefónica es de unos 3 minutos, en el acceso a Internet el usuario suele estar conectado del orden de 20 a 30 minutos, lo que implica que durante este tiempo nadie puede hacer uso de la línea telefónica con los inconvenientes que ello conlleva. Para buscar una solución a este problema algunos fabricantes han desarrollado un sistema que convierte las llamadas de voz en un flujo de datos IP que puede ser remitido directamente a los usuarios a los que van dirigidas. El funcionamiento es como sigue: cuando una llamada entrante se recibe en la central telefónica, la red es capaz de detectar si la línea de destino se encuentra ocupada en una sesión de Internet y en ese caso inmediatamente la reenruta a un servidor especializado que la digitaliza y la convierte en una trama de datos, convierte el número telefónico a la dirección de Internet de destino e inmediatamente envía un mensaje que se representa en un icono en la pantalla indicando que hay una llamada en espera, pidiendo su aceptación. Para las llamadas salientes se realiza el proceso inverso. Si el usuario dispone del ancho de banda mínimo requerido, puede hablar y mantener la sesión de Internet al mismo tiempo, despreocupándose del tiempo que emplea navegando por Internet, teniendo la tranquilidad de que no va perder ninguna llamada. De esta forma, se genera negocio extra para el operador de la red y el proveedor del servicio Internet (ISP).

D2 SEGURIDAD PARA SISTEMAS DE VoIP

La seguridad a menudo es una preocupación cuando se trata de redes IP para comunicaciones. Muchos Especialistas afirman que las nuevas instalaciones son al menos tan seguras como los sistemas de comunicaciones tradicionales que usan PBX's.

D2.1 SEGURIDAD EN LAS COMUNICACIONES IP

Día a día los requerimientos para ser más exitosos en los negocios continúan evolucionando, motivo por el cual las infraestructuras de red deben ir evolucionando también. Las comunicaciones IP permiten a las empresas implementar redes convergentes, donde los servicios de voz, video y datos son provistos sobre la red IP de una manera segura, generando beneficios tales como la reducción de costos (capitales y operativos y aumento de la productividad de los empleados). **La Compañía Cisco define las comunicaciones IP como un sistema de clase empresarial completo, habilitado por la Infraestructura AVVID de Cisco (Arquitectura de voz, video y datos integrados)**, que integra de una manera segura la voz, video y otras aplicaciones de colaboración de datos dentro de una solución de red inteligente. La aplicación de la telefonía IP, comunicaciones unificadas, conferencias de contenido enriquecido, video broadcasting y soluciones de contacto al cliente (customer contact) dan como resultado un ambiente de negocios altamente eficiente y colaborativo que mejora significativamente la manera como las empresas interactúan con sus empleados, socios de negocios y clientes, haciendo posible que las organizaciones puedan diferenciarse de sus competidores a la vez que les permite tener un retorno de Inversión medible. La Compañía Cisco recomienda una política de seguridad integral para proteger la integridad, privacidad y disponibilidad del sistema de comunicaciones IP. Integrando múltiples tecnologías de seguridad aplicadas en diferentes segmentos, aumentamos la seguridad total mediante la prevención de errores aislados que comprometan o impacten el sistema. Más aún, una política de seguridad integral incluye más que tecnología avanzada de seguridad, comprende procesos operacionales que aseguren un rápido despliegue de parches para los

software y aplicaciones, instalación de tecnologías de seguridad en el momento adecuado y finalmente la realización y evaluación de auditorias de seguridad. Desde que se despachó el primer Teléfono a la fecha, la seguridad en la telefonía IP ha avanzado vertiginosamente.

Por el contrario, con los sistemas PBX digitales tradicionales, tenemos que protegernos contra el fraude de llamadas, "masquerading" (personas que se hacen pasar por otras para tomar control del sistema PBX) y "war dialing", asimismo los accesos no autorizados pueden ser frecuentemente ejecutados con técnicas tan simples como usar un par de pinzas, pero probablemente no habrá que preocuparse de los gusanos que vienen de Internet. Sin embargo, algunas personas piensan que no es necesario preocuparse de la seguridad de red si se opta por un sistema de telefonía híbrido que son promovidos por fabricantes tradicionales de telefonía. Típicamente, el primer paso en el proceso de migración a un sistema híbrido es separar el CPU y el procesamiento de llamadas fuera de la "caja" y ponerlo en la red LAN. Es aquí donde tenemos que asegurarnos que la red LAN está completamente segura, dado que un ataque a los componentes que procesan las llamadas afectaría a cada usuario en el sistema, no sólo a los usuarios de los teléfonos IP. En este escenario, no sólo es necesario tener las mismas consideraciones de seguridad como cuando todo el sistema estuviese sobre la red IP, sino también es necesario administrar dos redes separadas, sin notar los beneficios de tener una solución integrada en una única red convergente.

Sería una falacia negar que la seguridad no sea un factor importante cuando una empresa decide implementar un sistema de Telefonía IP, ya sea híbrido o IP puro. La compañía Cisco es el único fabricante que aborda la seguridad en todos los niveles de la infraestructura de Comunicaciones IP: red IP, sistemas de voz y aplicaciones, proveyendo la defensa necesaria para hacer el sistema de Comunicaciones IP tan seguro como estos pueden ser. Cuando nos protegemos contra los tipos de vulnerabilidades comunes de voz y sistemas relacionados a la voz, es importante considerar tres componentes críticos:
Privacidad: Provista vía comunicaciones seguras. Tecnologías como IP Security (IPSec) y SSL nos permiten implementar Virtual Private Networks (VPN's) seguras que nos ayudan a robustecer las comunicaciones tanto en la LAN como en la WAN.
Protección: Provista por sistemas de defensa contra amenazas. Tecnologías como los firewalls, IDS's e IDP's combaten las amenazas originadas interna y externamente.
Control: Provisto vía sistemas de identidad y confiabilidad. Servidores de control de acceso y el Network Admission Control (NAC) de la compañía Cisco por ejemplo hacen posible que las organizaciones puedan controlar el acceso a la información, permitiendo que sólo la gente correcta pueda tener acceso a la información en el momento correcto.

En el caso de Cisco, las comunicaciones seguras empiezan con los teléfonos IP y el Cisco Call Manager (el software de procesamiento de llamadas). Los teléfonos IP de Cisco pueden clasificar automáticamente el tráfico de voz el cual es pasado a una cola de alta prioridad que minimiza la latencia y el jitter. Ellos son el primer punto en el cual la red es dinámicamente particionada en dos redes lógicamente separadas, una para voz y otra para datos. Con la solución apropiada desplegada, cuando un usuario hace una llamada telefónica, el Call Manager es capaz de encriptar y autenticar la señalización. Opcionalmente, la voz puede ser encriptada para lograr un nivel más alto de privacidad. Para una protección adicional, las imágenes del software que corren en los teléfonos IP sólo pueden ser instaladas si éstas tienen la firma apropiada. Todo esto es posible gracias a las capacidades de confiabilidad basadas en certificados digitales y tecnologías relacionadas de autorización y autenticación. La protección contra amenazas es suministrada en todo el sistema también. En el Call Manager, el Cisco Security Agent es usado para la protección contra intrusos y la arquitectura NAC ayuda a que las políticas de seguridad corporativas sean ejecutadas constantemente en toda la red. En la red, los sensores de detección de intrusos del host detectan e identifican actividad inusual y la aísla antes de que ésta pueda afectar a la red. Usando inspección de estado de paquetes, el firewall bloquea puertos de aplicaciones no necesarias y ayuda a asegurar que sólo tráfico autorizado es permitido a acceder a segmentos críticos de la red interna. En unas pruebas de laboratorio realizadas por Miercom (firma independiente especializada en probar y analizar productos de comunicaciones y networking), una solución de Comunicaciones IP de Cisco recibió la más alta calificación posible en seguridad y fue

catalogado como la solución de telefonía IP más segura de entre todas las soluciones que pasaron la prueba. Debido a esta capacidad de las soluciones de Cisco de proveer confiabilidad y seguridad, es posible lograr niveles más altos de seguridad que con sistemas PBX tradicionales basados en TDM. Se ha podido probar que, implementando seguridad siguiendo las guías de diseño de Cisco SAFE, una solución de Comunicaciones IP puede ser la solución de voz (IP) más segura disponible.

D2.2 SEGURIDAD EN EL PROTOCOLO VoIP

Consideremos las limitaciones de seguridad en un sistema de VoIP. En el proceso de ahorrar dinero (factor necesario) e incrementar la eficiencia, dos porciones cruciales de cualquier infraestructura, voz y datos, fueron combinadas. Los servidores de VoIP actúan como puertas de enlace; así, routers especiales, teléfonos, nuevos protocolos y sistemas operativos están ahora entremezclándose con esta nueva tecnología.

D2. 2.1 AMENAZAS

Desafortunadamente existen numerosas amenazas que conciernen a las redes VoIP; muchas de las cuales no resultan obvias para la mayoría de los usuarios. Los dispositivos de redes, los servidores y sus sistemas operativos, los protocolos, los teléfonos y su software, todos son vulnerables. La información sobre una llamada es tan valiosa como el contenido de la voz. Por ejemplo, una señal comprometida en un servidor puede ser usada para configurar y dirigir llamadas, del siguiente modo: una lista de entradas y salidas de llamadas, su duración y sus parámetros. Usando esta información, un atacante puede obtener un mapa detallado de todas las llamadas realizadas en la red, creando grabaciones completas de conversaciones y datos de usuario. La conversación es en sí misma un riesgo y el objetivo más obvio de una red VoIP. Consiguiendo una entrada en una parte clave de la infraestructura, como una puerta de enlace de VoIP, un atacante puede capturar y volver a montar paquetes con el objetivo de escuchar la conversación. O incluso peor aún, grabarlo absolutamente todo, y poder retransmitir todas las conversaciones sucedidas en la red. Las llamadas son también vulnerables al “secuestro”. En este escenario, un atacante puede interceptar una conexión y modificar los parámetros de la llamada. Se trata de un ataque que puede causar bastante pavor, ya que las víctimas no notan ningún tipo de cambio. Las posibilidades incluyen la técnica de spoofing o robo de identidad, y redireccionamiento de llamada, haciendo que la integridad de los datos estén bajo un gran riesgo. La enorme disponibilidad de las redes VoIP es otro punto sensible. En el PSTN (public switched telephone network), la disponibilidad era raramente un problema. Pero es mucho más sencillo hackear una red VoIP. Todos estamos familiarizados con los efectos demoledores de los ataques de denegación de servicio. Si se dirigen a puntos clave de la red, podrían incluso destruir la posibilidad de comunicarse vía voz o datos. Los teléfonos y servidores son blancos por sí mismos. Aunque sean de menor tamaño o nos sigan pareciendo simples teléfonos, son en base, ordenadores con software. Obviamente, este software es vulnerable con los mismos tipos de bugs o agujeros de seguridad que pueden hacer que un sistema operativo pueda estar a plena disposición del intruso. El código puede ser insertado para configurar cualquier tipo de acción maliciosa.

D2.2.2 SPOOFING

Por spoofing se conoce a la creación de tramas TCP/IP utilizando una dirección IP falseada; la idea de este ataque - al menos la idea - es muy sencilla: desde su equipo, un pirata simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado. Y como los anillos de confianza basados en estas características tan fácilmente falsificables son aún demasiado abundantes, el spoofing sigue siendo en la actualidad un ataque no trivial, pero factible contra cualquier tipo de organización. Como hemos visto, en el spoofing entran en juego tres máquinas: un atacante, un atacado, y un sistema suplantado que tiene cierta relación con el atacado; para que el pirata pueda conseguir su objetivo necesita por un lado establecer una

comunicación falseada con su objetivo, y por otro evitar que el equipo suplantado interfiera en el ataque. Probablemente esto último no le sea muy difícil de conseguir: a pesar de que existen múltiples formas de dejar fuera de juego al sistema suplantado - al menos a los ojos del atacado - que no son triviales (modificar rutas de red, ubicar un filtrado de paquetes entre ambos sistemas), lo más fácil en la mayoría de ocasiones es simplemente lanzar una negación de servicio contra el sistema en cuestión. No suele ser difícil "tumbar", o al menos bloquear parcialmente, un sistema medio; si a pesar de todo el atacante no lo consigue, simplemente puede esperar a que desconecten de la red a la máquina a la que desea suplantar (por ejemplo, por cuestiones de puro mantenimiento).

El otro punto importante del ataque, la comunicación falseada entre dos equipos, no es tan inmediato como el anterior y es donde reside la principal dificultad del spoofing. En un escenario típico del ataque, un pirata envía una trama SYN a su objetivo indicando como dirección origen la de esa tercera máquina que está fuera de servicio y que mantiene algún tipo de relación de confianza con la atacada. El host objetivo responde con un SYN+ACK a la tercera máquina, que simplemente lo ignorará por estar fuera de servicio (si no lo hiciera, la conexión se resetearía y el ataque no sería posible), y el atacante enviará ahora una trama ACK a su objetivo, también con la dirección origen de la tercera máquina. Para que la conexión llegue a establecerse, esta última trama deberá enviarse con el número de secuencia adecuado; el pirata ha de predecir correctamente este número: si no lo hace, la trama será descartada, y si lo consigue la conexión se establecerá y podrá comenzar a enviar datos a su objetivo, generalmente para tratar de insertar una puerta trasera que permita una conexión normal entre las dos máquinas. Podemos comprobar que el spoofing no es inmediato; de entrada, el atacante ha de hacerse una idea de cómo son generados e incrementados los números de secuencia TCP, y una vez que lo sepa ha de conseguir "engañar" a su objetivo utilizando estos números para establecer la comunicación; cuanto más robusta sea esta generación por parte del objetivo, más difícil lo tendrá el pirata para realizar el ataque con éxito. Además, es necesario recordar que el spoofing es un ataque ciego: el atacante no ve en ningún momento las respuestas que emite su objetivo, ya que estas van dirigidas a la máquina que previamente ha sido deshabilitada, por lo que debe presuponer que está sucediendo en cada momento y responder de forma adecuada en base a esas suposiciones. Sería imposible tratar con el detenimiento que merecen todos los detalles relativos al spoofing.

Para evitar ataques de spoofing exitosos contra nuestros sistemas podemos tomar diferentes medidas preventivas; en primer lugar, parece evidente que una gran ayuda es reforzar la secuencia de predicción de números de secuencia TCP. Otra medida sencilla es eliminar las relaciones de confianza basadas en la dirección IP o el nombre de las máquinas, sustituyéndolas por relaciones basadas en claves criptográficas; el cifrado y el filtrado de las conexiones que pueden aceptar nuestras máquinas también son unas medidas de seguridad importantes de cara a evitar el spoofing. Hasta ahora hemos hablado del ataque genérico contra un host denominado spoofing o, para ser más exactos, IP Spoofing; existen otros ataques de falseamiento relacionados en mayor o menor medida con este, entre los que destacan el DNS Spoofing, el ARP Spoofing y el Web Spoofing.

- **DNS Spoofing** Este ataque hace referencia al falseamiento de una dirección IP ante una consulta de resolución de nombre (esto es, resolver con una dirección falsa un cierto nombre DNS), o viceversa (resolver con un nombre falso una cierta dirección IP). Esto se puede conseguir de diferentes formas, desde modificando las entradas del servidor encargado de resolver una cierta petición para falsear las relaciones dirección-nombre, hasta comprometiendo un servidor que infecte la caché de otro (lo que se conoce como DNS Poisoning); incluso sin acceso a un servidor DNS real, un atacante puede enviar datos falseados como respuesta a una petición de su víctima sin más que averiguar los números de secuencia correctos.
- **ARP Spoofing** El ataque denominado ARP Spoofing hace referencia a la construcción de tramas de solicitud y respuesta ARP falseadas, de forma que en una red local se puede forzar a una determinada máquina a que envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo. La idea es sencilla, y los efectos del ataque pueden ser muy

negativos: desde negaciones de servicio hasta interceptación de datos, incluyendo algunos Man in the Middle contra ciertos protocolos cifrados.

- **Web Spoofing** Este ataque permite a un pirata visualizar y modificar cualquier página web que su víctima solicite a través de un navegador, incluyendo las conexiones seguras vía SSL. Para ello, mediante código malicioso un atacante crea una ventana del navegador correspondiente, de apariencia inofensiva, en la máquina de su víctima; a partir de ahí, enruta todas las páginas dirigidas al equipo atacado - incluyendo las cargadas en nuevas ventanas del navegador - a través de su propia máquina, donde son modificadas para que cualquier evento generado por el cliente sea registrado (esto implica registrar cualquier dato introducido en un formulario, cualquier click en un enlace, etc.).

D2.2 .3 HERRAMIENTAS DEL HACKER

Es difícil describir el ataque "típico" de un hacker debido a que los intrusos poseen diferentes niveles de técnicos por su experiencia y además son motivados por diversos factores. Algunos hackers son intrigosos por el desafío, otros más gozan de hacer la vida difícil a los demás, y otros tantos substraen datos delicados para algún beneficio propio.

Recolección de información

Generalmente, el primer paso es saber en que forma se recolecta la información y además que tipo de información es. La meta es construir una base de datos que contenga la organización de la red y colectar la información acerca de los servidores residentes. Esta es una lista de herramientas que un hacker puede usar para colectar esta información:

- El protocolo SNMP puede utilizarse para examinar la tabla de ruteo en un dispositivo inseguro, esto sirve para aprender los detalles más íntimos acerca del objetivo de la topología de red perteneciente a una organización.
- El programa Trace Route puede revelar el número de redes intermedias y los ruteadores en torno al servidor específico.
- El protocolo Whois que es un servicio de información que provee datos acerca de todos los dominios DNS y el administrador del sistema responsable para cada dominio. No obstante que esta información es anticuada.
- Servidores DNS pueden accesarce para obtener una lista de las direcciones IP y sus correspondientes Nombres (Programa Nslookup).
- El protocolo Finger puede revelar información detallada acerca de los usuarios (nombres de Login, números telefónicos, tiempo y última sesión, etc.) de un servidor en específico.
- El programa Ping puede ser empleado para localizar un servidor particular y determinar si se puede alcanzar. Esta simple herramienta puede ser usada como un programa de escaneo pequeño que por medio de llamadas a la dirección de un servidor haga posible construir una lista de los servidores que actualmente son residentes en la red.

Sondeo del sistema para debilitar la seguridad

Después que se obtienen la información de red perteneciente a dicha organización, el hacker trata de probar cada uno de los servidores para debilitar la seguridad. Estos son algunos usos de las herramientas que un hacker puede utilizar automáticamente para explorar individualmente los servidores residentes en una red:

- Una vez obtenida una lista no obstantemente pequeña de la vulnerabilidad de servicios en la red, un hacker bien instruido puede escribir un pequeño programa que intente conectarse a un puerto especificando el tipo de servicio que está asignado al servidor en cuestión. La corrida del programa presenta una lista de los servidores que soportan servicio de Internet y están expuestos al ataque.
- Están disponibles varias herramientas del dominio público, tal es el caso como el Rastreador de Seguridad en Internet (ISS) o la Herramienta para Análisis de Seguridad para Auditar Redes (SATAN), el cual puede rastrear una subred o un dominio y ver las posibles fugas de seguridad. Estos programas determinan la debilidad de cada uno de los sistemas con respecto a varios puntos de vulnerabilidad comunes en un sistema. El intruso usa la información colectada por este tipo de rastreadores para intentar el acceso no autorizado al sistema de la organización puesta en la mira.

Un administrador de redes hábil puede usar estas herramientas en su red privada para descubrir los puntos potenciales donde está debilitada su seguridad y así determina que servidores necesitan ser remendados y actualizados en el software.

Acceso a sistemas protegidos

El intruso utiliza los resultados obtenidos a través de las pruebas para poder intentar acceder a los servicios específicos de un sistema. Después de tener el acceso al sistema protegido, el hacker tiene disponibles las siguientes opciones:

- Puede atentar destruyendo toda evidencia del asalto y además podrá crear nuevas fugas en el sistema o en partes subalternas con el compromiso de seguir teniendo acceso sin que el ataque original sea descubierto.
- Pueden instalar paquetes de sondeo que incluyan códigos binarios conocidos como “Caballos de Troya” protegiendo su actividad de forma transparente. Los paquetes de sondeo colectan las cuentas y contraseñas para los servicios de Telnet y FTP permitiendo al hacker expandir su ataque a otras maquinas.
- Pueden encontrar otros servidores que realmente comprometan al sistema. Esto permite al hacker explotar vulnerablemente desde un servidor sencillo todos aquellos que se encuentren a través de la red corporativa.
- Si el hacker puede obtener acceso privilegiado en un sistema compartido, podrá leer el correo, buscar en archivos.

D2.3 DEFENDERSE

Ya hemos hablado de las maravillas de la tecnología de VoIP, y nos hemos encontrado con graves problemas de seguridad. Afortunadamente, la situación no es irremediable. En resumidas cuentas, los riesgos que comporta usar el protocolo VoIP no son muy diferentes de los que nos podemos encontrar en las redes habituales de IP. Desafortunadamente, en los “rollouts” iniciales y en diseños de hardware para voz, software y protocolos, la seguridad no es su punto fuerte. Pero seamos sinceros; esto es lo que siempre suele pasar cada vez que aparece una nueva tecnología. Examinemos ahora algunas pruebas que puedan alivia las amenazas sobre esta tecnología. Lo primero que deberíamos tener en mente a la hora de leer sobre VoIP es la encriptación. Aunque lógicamente no es sencillo capturar y decodificar los paquetes de voz, puede hacerse. Y encriptar es la única forma de prevenirse ante un ataque. Desafortunadamente, toma ancho de banda. Por tanto... ¿Qué podemos hacer? Existen múltiples métodos de encriptación o posibilidades de encriptación: VPN (virtual private network), el protocolo IPSec (IP segura) y otros protocolos como SRTP (secure RTP). La clave, de cualquier forma, es elegir un algoritmo de encriptación rápido, eficiente, y emplear un procesador dedicado de encriptación. Esto debería aliviar cualquier riesgo de amenaza. Otra opción podría ser QoS (Quality of Service); los requerimientos para QoS asegurarán que la voz se maneja siempre de manera oportuna, reduciendo la pérdida de calidad. Lo próximo, como debería esperarse, podría ser el proceso de securizar todos los elementos que componen la red VoIP: servidores de llamadas, routers, switches, centros de trabajo y teléfonos. Se necesita configurar cada uno de esos dispositivos para asegurarse de que están en línea con las demandas en términos de seguridad. Los servidores pueden tener pequeñas funciones trabajando y sólo abiertos los puertos que sean realmente necesarios. Los routers y switches deberían estar configurados adecuadamente, con acceso a las listas de control y a los filtros. Todos los dispositivos deberían estar actualizados en términos de parches y actualizaciones. Se trata del mismo tipo de precauciones que podrías tomar cuando añades nuevos elementos a la red de datos; únicamente habrá que extender este proceso a la porción que le compete a la red VoIP. Tal y como hemos mencionado, la disponibilidad de la red VoIP es otra de nuestras preocupaciones. Una pérdida de potencia puede provocar que la red se caiga y los ataques DdoS son difíciles de contrarrestar. Aparte de configurar con propiedad el router, recordemos que estos ataques no sólo irán dirigidos a los servicios de datos, sino también a los de voz.

Por último, podemos emplear un firewall y un IDS (Intrusion Detection System) para ayudar a proteger la red de voz. Los firewalls de VoIP son complicados de manejar y tienen múltiples requerimientos. Los servidores de llamada están constantemente abriendo y cerrando puertos para las nuevas conexiones. Este elemento dinámico hace que su manejo sea más dificultoso. Pero el

costo está lejos de verse oscurecido por la cantidad de beneficios, así que aconsejamos pasar algo de tiempo perfeccionando los controles de acceso. Un IDS puede monitorear la red para detectar cualquier anomalía en el servicio o un abuso potencial. Las advertencias son una clave para prevenir los ataques posteriores. Y sin duda no hay mejor defensa que estar prevenido para el ataque.

D2.4 IPSEC

La meta de este protocolo es proporcionar varios servicios de seguridad para el tráfico de la capa IP, tanto a través de IPv4 e IPv6. Los componentes fundamentales de la arquitectura de seguridad IPSec son los siguientes:

- Protocolos de Seguridad: Cabecera de autenticación (AH) y los Datos Seguros Encapsulados (ESP).
- Asociaciones de Seguridad.
- Manejo de Clave: manual y automática (Internet Key Exchange, IKE).
- Algoritmos para la autenticación y encriptación.
- IPSec es una extensión al protocolo IP que proporciona seguridad a IP y a los protocolos de capas superiores. Fue desarrollado para el nuevo estándar IPv6 y después fue portado a IPv4. La arquitectura IPSec se describe en el RFC2401.

IPSec emplea dos protocolos diferentes (AH y ESP) para asegurar la autenticación, integridad y confidencialidad de la comunicación. Puede proteger el datagrama IP completo o sólo los protocolos de capas superiores. Estos modos se denominan, respectivamente, modo túnel y modo transporte. En modo túnel el datagrama IP se encapsula completamente dentro de un nuevo datagrama IP que emplea el protocolo IPSec. En modo transporte IPSec sólo maneja la carga del datagrama IP, insertándose la cabecera IPSec entre la cabecera IP y la cabecera del protocolo de capas superiores.

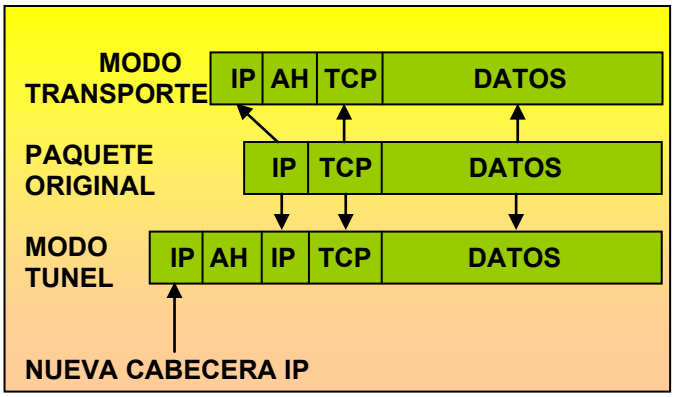


Figura 329 IPSec: modos túnel y transporte

Para proteger la integridad de los datagramas IP, los protocolos IPSec emplean códigos de autenticación de mensaje basados en resúmenes (HMAC - Hash Message Authentication Codes). Para el cálculo de estos HMAC los protocolos HMAC emplean algoritmos de resumen como MD5 y SHA para calcular un resumen basado en una clave secreta y en los contenidos del datagrama IP. El HMAC se incluye en la cabecera del protocolo IPSec y el receptor del paquete puede comprobar el HMAC si tiene acceso a la clave secreta. Para proteger la confidencialidad de lo datagramas IP, los protocolos IPSec emplean algoritmos estándar de cifrado simétrico. El estándar IPSec exige la implementación de NULL y DES. En la actualidad se suelen emplear algoritmos más fuertes: 3DES, AES y Blowfish. Para protegerse contra ataques por denegación de servicio, los protocolos IPSec emplean ventanas deslizantes. Cada paquete recibe un número de secuencia y sólo se acepta su recepción si el número de paquete se encuentra dentro de la ventana o es posterior. Los paquetes anteriores son descartados inmediatamente. Esta es una medida de protección eficaz contra ataques por repetición de mensajes en los que el atacante almacena los paquetes originales y los reproduce posteriormente.

Para que los participantes de una comunicación puedan encapsular y desencapsular los paquetes IPSec, se necesitan mecanismos para almacenar las claves secretas, algoritmos y direcciones IP involucradas en la comunicación. Todos estos parámetros se almacenan en asociaciones de seguridad (SA - Security Associations). Las asociaciones de seguridad, a su vez,

se almacenan en bases de datos de asociaciones de seguridad (SAD - Security Asocciation Databases). Cada asociación de seguridad define los siguientes parámetros:

- Dirección IP origen y destino de la cabecera IPSec resultante. Estas son las direcciones IP de los participantes de la comunicación IPSec que protegen los paquetes.
- Protocolo IPSec (AH o ESP). A veces, se permite compresión (IPCOMP).
- El algoritmo y clave secreta empleados por el protocolo IPSec.
- Índice de parámetro de seguridad (SPI - Security Parameter Index). Es un número de 32 bits que identifica la asociación de seguridad.
- Algunas implementaciones de la base de datos de asociaciones de seguridad permiten almacenar más parámetros:
- Modo IPSec (túnel o transporte)
- Tamaño de la ventana deslizante para protegerse de ataques por repetición.
- Tiempo de vida de una asociación de seguridad.

En una asociación de seguridad se definen las direcciones IP de origen y destino de la comunicación. Por ello, mediante una única **SA** sólo se puede proteger un sentido del tráfico en una comunicación IPSec full duplex. Para proteger ambos sentidos de la comunicación, IPSec necesita de dos asociaciones de seguridad unidireccionales. Las asociaciones de seguridad sólo especifican como se supone que IPSec protegerá el tráfico. Para definir qué tráfico proteger, y cuando hacerlo, se necesita información adicional. Esta información se almacena en la política de seguridad (SP - Security Policy), que a su vez se almacena en la base de datos de políticas de seguridad (SPD - Security Policy Database). Una política de seguridad suele especificar los siguientes parámetros:

- Direcciones de origen y destino de los paquetes por proteger. En modo transportes estas serán las mismas direcciones que en la SA. En modo túnel pueden ser distintas.
- Protocolos y puertos a proteger. Algunas implementaciones no permiten la definición de protocolos específicos a proteger. En este caso, se protege todo el tráfico entre las direcciones IP indicadas.
- La asociación de seguridad a emplear para proteger los paquetes.
- La configuración manual de la asociación de seguridad es proclive a errores, y no es muy segura. Las claves secretas y algoritmos de cifrado deben compartirse entre todos los participantes de la VPN. Uno de los problemas críticos a los que se enfrenta el administrador de sistemas es el intercambio de claves: ¿cómo intercambiar claves simétricas cuando aún no se ha establecido ningún tipo de cifrado? Para resolver este problema se desarrolló el protocolo de intercambio de claves por Internet (IKE - Internet Key Exchange Protocol). Este protocolo autentica a los participantes en una primera fase. En una segunda fase se negocian las asociaciones de seguridad y se escogen las claves secretas simétricas a través de un intercambio de claves Diffie Hellmann. El protocolo IKE se ocupa incluso de renovar periódicamente las claves para asegurar su confidencialidad.

D2.4.1 LOS PROTOCOLOS IPSEC

La familia de protocolos IPSec está formada por dos protocolos: el AH (Authentication Header - Cabecera de autenticación) y el ESP (Encapsulated Security Payload - Carga de seguridad encapsulada). Ambos son protocolos IP independientes. AH es el protocolo IP 51 y ESP el protocolo IP 50.

D2.4.1.1 CABECERA DE AUTENTIFICACIO (AH)

El protocolo AH protege la integridad del datagrama IP. Para conseguirlo, el protocolo AH calcula una HMAC basada en la clave secreta, el contenido del paquete y las partes inmutables de la cabecera IP (como son las direcciones IP). Tras esto, añade la cabecera AH al paquete.

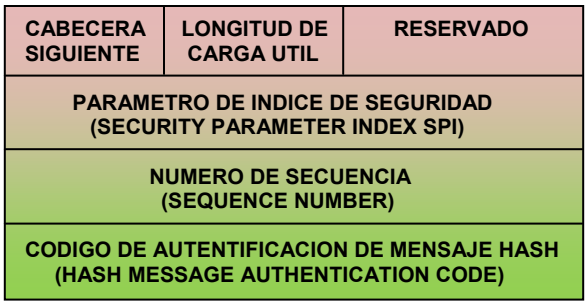


Figura 330 La cabecera AH protege la integridad del paquete

La cabecera AH mide 24 bytes. El primer byte es el campo Siguiente cabecera. Este campo especifica el protocolo de la siguiente cabecera. En modo túnel se encapsula un datagrama IP completo, por lo que el valor de este campo es 4. Al encapsular un datagrama TCP en modo transporte, el valor correspondiente es 6. El siguiente byte especifica la longitud del contenido del paquete. Este campo está seguido de dos bytes reservados. Los siguientes 4 bytes especifican en Índice de Parámetro de Seguridad (SPI). El SPI especifica la asociación de seguridad (SA) a emplear para el desencapsulado del paquete. El Número de Secuencia de 32 bits protege frente a ataques por repetición. Finalmente, los últimos 96 bits almacenan el código de resumen para la autenticación de mensaje (HMAC). Este HMAC protege la integridad de los paquetes ya que sólo los miembros de la comunicación que conozcan la clave secreta pueden crear y comprobar HMAC's. Como el protocolo AH protege la cabecera IP incluyendo las partes inmutables de la cabecera IP como las direcciones IP, el protocolo AH no permite NAT. NAT (Network Address Translation - Traducción de direcciones de red) también conocido como Enmascaramiento de direcciones reemplaza una dirección IP de la cabecera IP (normalmente la IP de origen) por una dirección IP diferente. Tras el intercambio, la HMAC ya no es válida. La extensión a IPSec NAT-transversal implementa métodos que evitan esta restricción.

D2.4.1.2 CARGA DE SEGURIDAD ENCAPSULDA (ESP)

El protocolo ESP puede asegurar la integridad del paquete empleando una HMAC y la confidencialidad empleando cifrado. La cabecera ESP se genera y añade al paquete tras cifrarlo y calcular su HMAC. La cabecera ESP consta de dos partes. La cabecera ESP

Figura 331

Los primeros 32 bits de la cabecera ESP especifican el Índice de Parámetros de Seguridad (SPI). Este SPI específica que SA emplear para desencapsular el paquete ESP. Los siguientes 32 bits almacenan el Número de Secuencia. Este número de secuencia se emplea para protegerse de ataques por repetición de mensajes. Los siguientes 32 bits especifican el Vector de Inicialización (IV - Initialization Vector) que se emplea para el proceso de cifrado. Los algoritmos de cifrado

simétrico pueden ser vulnerables a ataques por análisis de frecuencias si no se emplean IV's. El IV asegura que dos cargas idénticas generan dos cargas cifradas diferentes.

IPSec emplea cifradores de bloque para el proceso de cifrado. Por ello, puede ser necesario rellenar la carga del paquete si la longitud de la carga no es un múltiplo de la longitud del paquete. En ese caso se añade la longitud del relleno (pad length). Tras la longitud del relleno se coloca el campo de 2 bytes Siguiente cabecera que especifica la siguiente cabecera. Por último, se añaden los 96 bits de HMAC para asegurar la integridad del paquete. Esta HMAC sólo tiene en cuenta la carga del paquete: la cabecera IP no se incluye dentro de su proceso de cálculo. El uso de NAT, por lo tanto, no rompe el protocolo ESP. Sin embargo, en la mayoría de los casos, NAT aún no es compatible en combinación con IPSec. NAT- Transversal ofrece una solución para este problema encapsulando los paquetes ESP dentro de paquetes UDP.

D2.4.1.3 EL PROTOCOLO IKE

El protocolo IKE resuelve el problema más importante del establecimiento de comunicaciones seguras: la autenticación de los participantes y el intercambio de claves simétricas. Tras ello, crea las asociaciones de seguridad y rellena la SAD. El protocolo IKE suele implementarse a través de servidores de espacio de usuario, y no suele implementarse en el sistema operativo. El protocolo IKE emplea el puerto 500 UDP para su comunicación. El protocolo IKE funciona en dos fases. La primera fase establece un ISAKMP SA (Internet Security Association Key Management Security Association - Asociación de seguridad del protocolo de gestión de claves de asociaciones de seguridad en Internet). En la segunda fase, el ISAKMP SA se emplea para negociar y establecer las SA's de IPSec. La autenticación de los participantes en la primera fase suele basarse en claves compartidas con anterioridad (PSK - Pre-shared keys), claves RSA y certificados X.509. La primera fase suele soportar dos modos distintos: modo principal y modo agresivo. Ambos modos autentican al participante en la comunicación y establecen un ISAKMP SA, pero el modo agresivo sólo usa la mitad de mensajes para alcanzar su objetivo. Esto, sin embargo, tiene sus desventajas, ya que el modo agresivo no soporta la protección de identidades y, por lo tanto, es susceptible a un ataque man-in-the-middle (por escucha y repetición de mensajes en un nodo intermedio) si se emplea junto a claves compartidas con anterioridad (PSK). Pero sin embargo este es el único objetivo del modo agresivo, ya que los mecanismos internos del modo principal no permiten el uso de distintas claves compartidas con anterioridad con participantes desconocidos. El modo agresivo no permite la protección de identidades y transmite la identidad del cliente en claro. Por lo tanto, los participantes de la comunicación se conocen antes de que la autenticación se lleve a cabo, y se pueden emplear distintas claves pre-compartidas con distintos comunicantes. En la segunda fase, el protocolo IKE intercambia propuestas de asociaciones de seguridad y negocia asociaciones de seguridad basándose en la ISAKMP SA. La ISAKMP SA proporciona autenticación para protegerse de ataques man-in-the-middle. Esta segunda fase emplea el modo rápido. Normalmente, dos participantes de la comunicación sólo negocian una ISAKMP SA, que se emplea para negociar varias (al menos dos) IPSec SA's unidireccionales.

D2.4.2 FIREWALLS

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

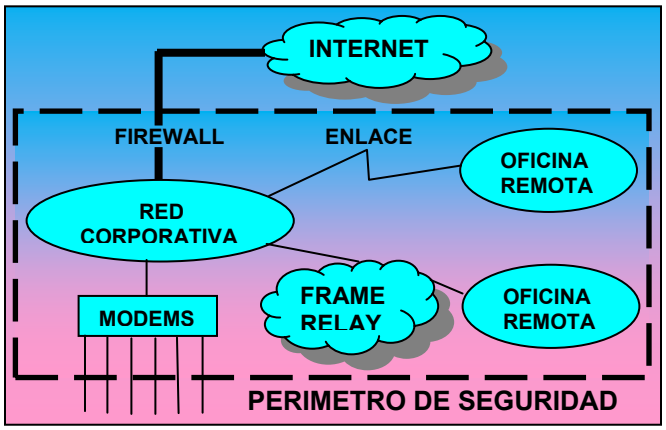


Figura La Política De Seguridad Crea Un Perímetro De Defensa.

Esto es importante, ya que debemos de notar que un firewall de Internet no es justamente un ruteador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial-in y dial-out, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad. Un firewall de Internet sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda.

D2.4.3 REDES PRIVADAS VIRTUALES

Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte. Los paquetes de datos de la red privada viajan por medio de un “túnel” definido en la red pública.

D2.5 SEGURIDAD EN LOS SISTEMAS VoIP

Haciendo alusión a un reciente debate en línea sobre temas de seguridad, los expertos coinciden en que falta muy poco para que los sistemas de VoIP, sean inundados de spam, se abran a los piratas informáticos, y sean derribados por los gusanos. Es importante que la industria se adelante a estas expectativas. VoIP, es una tecnología que permite la transmisión de la voz a través de redes IP, en forma de paquetes de datos. La aplicación más notoria de esta tecnología, es la realización de llamadas telefónicas ordinarias a través de la red. Las empresas se han enfocado casi exclusivamente en el precio, las características y el desempeño, a menudo liberando nuevos sistemas que están abiertos a insospechadas amenazas.

Los riesgos incluyen las infracciones comunes de la seguridad que las empresas tratan hoy, incluyendo DDoS (ataques distribuidos de denegación de servicio), código malicioso, spoofing (práctica de hacer que una transmisión aparezca como venida de un usuario diferente al usuario que realizó la acción) y phishing (atraer mediante engaños a un usuario hacia un sitio Web falso). Pero las empresas necesitan también tener cuidado respecto a las amenazas propias de VoIP, tales como escuchas furtivas y "VBombing", donde centenares o miles de mensajes de voz pueden ser rápidamente enviados a una sola consola VoIP.

La mayoría de estos ataques, pueden alcanzarse al nivel de las aplicaciones, que para la mayoría de los grandes vendedores se basa en el SIP (Session Initiation Protocol). SIP es un protocolo de señalización para conferencia, telefonía, presencia, notificación de eventos y

mensajería instantánea a través de Internet. Los cortafuegos y las redes privadas virtuales (VPN), pueden manejar de forma adecuada la seguridad en la capa de transporte para VoIP, pero SIP puede compararse con el SMTP y el HTTP para las aplicaciones de la Web y el correo electrónico, que fueron ignorados hasta que surgieron los problemas de seguridad.

D3 PRESENTE Y FUTURO DE LAS COMUNICACIONES DE VOZ

D3.1 EMPRESA RELACIONADAS CON EL ESTANDAR VoIP

D3.1.1 3COM CORPORATION Y SIEMENS COMMUNICATIONS NETWORKS

La plataforma Total Control de 3Com y el switch digital EWSD de Siemens permiten una nueva generación de funciones de llamadas personalizadas, incluyendo VoIP. 3Com Corporation y Siemens Public Communications Networks, poseen un acuerdo conjunto de desarrollo que combina un sistema de red de voz y datos para producir el primer y único switch multiservicio de la oficina central. Las compañías han integrado la plataforma multiservicio Total Control de 3Com con el sistema digital de switches Class 5 EWSD (Elektronisches Wahlsystem Digital) de Siemens para simplificar el acceso remoto a Internet y permitir la entrega de una nueva generación total en servicios de llamadas personalizadas, incluyendo VoIP. Este acuerdo conjunto de desarrollo entre dos compañías los ubica en la vanguardia de la convergencia de redes. La implementación de la vía de acceso a Internet de Total Control en el sistema EWSD permite los servicios de llamadas personalizadas que pueden facilitar en gran manera el uso de Internet y el teléfono. Al mismo tiempo, los operadores de redes telefónicas pueden ofrecer un acceso eficaz a Internet a través de las redes existentes, reduciendo de este modo la inversión en nueva infraestructura. Algunos de los nuevos servicios potenciales son:
Acceso mejorado a VoIP: este servicio le ofrece al usuario la opción de completar una llamada telefónica a través de la red convencional telefónica, o de manera opcional, para completar la llamada a través de una red IP. La vía de acceso integrada IP para comunicaciones telefónicas le suministra al usuario un acceso amigable a este servicio. El acceso mediante el discado y los cargos de medición se administran dentro del switch EWSD multiservicio.

- **Llamada en espera de Internet**: mientras un usuario está "navegando por" Internet, el servicio de llamada en espera de Internet alerta al usuario de que hay llamadas entrantes por medio de una ventana en la pantalla. Hasta ahora, la persona que recibe la llamada no tiene manera de reconocer y aceptar las llamadas entrantes. La línea de teléfono estaría constantemente ocupada mientras el usuario está conectado a una sesión de Internet. Este nuevo servicio le permite al receptor decidir si acepta o no la llamada o si continúa con la sesión de Internet y tal vez, llama más tarde.
- **Realización de la llamada**: este servicio es como el servicio de llamada en espera de Internet, excepto que la sesión de Internet no necesita interrumpirse para aceptar la llamada. Utilizando la capacidad de VoIP del switch integrado EWSD multiservicio, el receptor puede hablar desde la PC y continuar, de este modo, con la sesión de Internet interrumpida mientras acepta llamadas telefónicas entrantes.
- **Señal de espera de e-mail**: el servicio de señal de espera de e-mail le informa al usuario que ha recibido un mensaje de e-mail utilizando el mismo método que usa el sistema de mensajes de voz basados en la red. Esta información se recibe en el teléfono del usuario, sin la necesidad de encender la PC. La información de espera de un mensaje se señala a través del panel de visualización del teléfono – un LED - o un tono de discado especial "entrecortado" similar a un correo de voz.
- **Entrada controlada por el usuario**: utilizando la tecnología basada en la Web, los usuarios pueden por sí mismos configurar estos servicios de llamadas personalizadas para sus líneas telefónicas con la ayuda de una interfaz gráfica fácil para el usuario en sus PC's. También pueden obtener una visualización online (en línea) de los gastos actuales de servicios.

En enero de 1999, 3Com lanzó con éxito las capacidades de VoIP, construido en parte sobre la base del servidor de Microsoft Windows NT, en la plataforma Total Control multiservicio, un sistema avanzado basado en DSP considerado por las firmas de investigación de industrias como el sistema de acceso remoto líder en el mundo de los mercados. Cambiando la definición de acceso remoto, la plataforma Total Control multiservicio de 3Com es un sistema de última generación, totalmente modular, con acceso tipo portador basado en la tecnología HiPero DSP de 3Com que puede entregar servicios de valor tales como voz, fax, video, sistema de red privada virtual y sus contenidos todo en un sistema simple con un software que se puede actualizar. Más de tres millones de puertos Total Control se han desarrollado hasta la fecha.
Además, 300 proveedores, que ofrecen servicios a más de 150 millones de suscriptores en 100 países, utilizan el sistema EWSD de Siemens, convirtiéndolo en el switch digital líder en el mundo y confirmando la larga tradición de Siemens como el primer proveedor de soluciones para los sistemas con infraestructuras de telecomunicaciones.

D3.1.2 CISCO

La Compañía Cisco Systems anuncia la introducción de mejoras en software y hardware para su línea de productos de acceso de múltiples servicios. Esta línea permite ahora a los proveedores de servicio y a los clientes corporativos desarrollar infraestructuras de red a gran escala y de voz basadas en paquetes, a una fracción del precio de tecnologías tradicionales. Con las nuevas funciones incorporadas, los clientes pueden aprovechar la integración de voz, video y datos sobre sus redes. En software, las nuevas características ofrecen voz sobre Frame Relay -VoFR- en los routers de acceso de múltiples servicios Cisco 2600, Cisco 3600, Cisco 7200 y en los concentradores de acceso de múltiples servicios Cisco MC permiten al usuario ofrecer voz y evitar los PBX's a través de múltiples circuitos permanentes virtuales, con base en el número telefónico marcado. Adicionalmente, aportan a los clientes una red de VoIP confiable y escalable con posibilidad de integrar con facilidad locaciones internacionales. Las interfaces soportan VoFR o VoIP, haciendo posible las conexiones a los PBX's (private branch exchanges) con interfaces Base Rate (BRI), así como con las tradicionales interfaces de telefonía.

D3.1.2.1 ARQUITECTURA DE VOZ COMUN

El marco de voz con el software integrador Cisco IOS ofrece la integración completa y sin fisura de voz, video y datos. Permite a los clientes corporativos y a los proveedores de servicio manejar grandes redes y servicios basados en VoIP o VoFR. Por ejemplo, el marco de voz común de Cisco basado sobre la arquitectura Open Packet Telephony de Cisco, ofrece escalabilidad e interoperabilidad de voz sobre servicios de paquetes desde routers de múltiples servicios de baja densidad VoIP/VoFR, hasta gateways VoIP de tipo carrier. Adicionalmente, los routers de acceso de múltiples servicios de Cisco, en combinación con su H.323 Gatekeeper, permite a los clientes construir redes muy grandes de VoIP. A los proveedores de servicio, las nuevas características incluye el Integrated Voice Response (IVR), características de seguridad AAA para autenticación de usuarios e historiales detallados sobre las llamadas realizadas. Los routers de acceso de múltiples servicios como los de las series Cisco 2600 y 3600, trabajan con el Gateway Cisco 5300 VoIP, haciendo que sea una solución ideal para el proveedor de servicios que esté lanzando servicios administrados de VoIP.

D3.1.3 MOTOROLA

El objetivo de Motorola ING es minimizar los costos de comunicaciones, un aspecto cada vez más crítico. Esta reducción de costos se puede conseguir por dos caminos: por un lado, con equipos flexibles, capaces de adaptarse a distintos entornos LAN (Ethernet, Token Ring, SDLC) y WAN (X.25, FR, PPP); y por otro, con equipos con capacidad de tráfico multimedia (voz y vídeo), a fin de sacar el máximo rendimiento de las líneas de comunicaciones. Los equipos de Motorola ING son a la vez router y conmutador y pueden comunicarse utilizando redes WAN, públicas o privadas, de líneas punto a punto, RDSI, X.25, Frame Relay o IP. Además, dependiendo del modelo, los routers de Motorola tienen interfaces Ethernet, Token Ring, Serie y RDSI. Este amplio abanico de

interfaces, junto con las funcionalidades de routing disponibles (RIP, OSPF, NAT), permiten procesar distintos tipos de tráfico con un único equipo.
Por otro lado, Motorola ING es pionera en la implementación de tráfico multimedia sobre redes de datos; ello nos permite poder ofrecer la posibilidad de aumentar el rendimiento de los enlaces de datos mediante la multiplexación de datos, voz y vídeo vigilancia, con el consiguiente ahorro de costos que ello implica. En este campo Motorola ING es el único fabricante del mundo capaz de ofrecer soluciones para voz sobre Frame Relay y VoIP con el mismo equipo. Motorola ING presenta VoFR (Voz sobre Frame Relay) y VoIP utilizando la misma plataforma hardware. Motorola ING fue pionera en 1995 al integrar la transmisión de voz en redes WAN Frame Relay. Aprovechando esa experiencia, única en el mercado, Motorola ING lanza VoIP, utilizando los mismos equipos, empleando tanto protocolos propietarios (SoTCP) como protocolos estándar (H.323). Los equipos de Motorola ING ofrecen una calidad excelente en transmisión de voz, tanto analógica (FXS, FXO, E&M) como digital (T0, E1), sobre líneas Frame Relay y/o IP. Hoy en día Motorola ING es el único fabricante del mundo que ofrece soluciones de voz sobre redes Frame Relay y voz sobre redes IP con el mismo equipo, incluso de manera simultánea. Este hecho permite a los equipos de Motorola ING funcionar de forma simultánea como VoIP Gateway y router voz/datos sobre Frame Relay.

D3.2 LA SOLUCION DE VoIP DE 3COM

El sistema de telefonía sobre IP de clase carrier de 3Com se basa en una arquitectura abierta de tres niveles de gateways, gatekeepers y servidores de backend interconectados mediante protocolos abiertos basados en normas. La arquitectura modular de 3Com presenta API's estándar en cada nivel a fin de brindarle a los carriers flexibilidad para personalizar el sistema, facilitando la diferenciación de servicios y la integración de las "mejores" aplicaciones de oficina back-to-back "de su clase". Este sistema modular llave en mano basado en normas soporta la telefonía sobre IP de teléfono a teléfono y de PC a teléfono en redes conmutadas por paquetes. Sobre la base de la plataforma de acceso Total Control Multiservice Access Platform de 3Com, el sistema de VoIP de clase carrier está basado en normas y acepta protocolos internacionales entre los que se incluyen las especificaciones ITU T.120 y H.323v2. Además, el sistema utiliza la codificación de voz G.711, G.723.1 y G.729a para garantizar la compatibilidad con los sistemas de telefonía mundiales. Este desarrollo representa el próximo paso lógico para una plataforma diseñada para servicios múltiples. Además de la voz, la plataforma también brindará un soporte extensivo a los servicios de fax y video.

D3.2.1 GATEWEAY DE VoIP

Los gateways de VoIP proveen un acceso interrumpido a la red IP. Las llamadas de voz se digitalizan, codifican, comprimen y paquetizan en un gateway de origen y luego, se descomprimen, decodifican y rearman en el gateway de destino. Los gateways se interconectan con la PSTN según corresponda a fin de asegurar que la solución sea ubicua. El procesamiento que realiza el gateway de la cadena de audio que atraviesa una red IP es transparente para los usuarios. Desde el punto de vista de la persona que llama, la experiencia es muy parecida a utilizar una tarjeta de llamada telefónica. La persona que realiza la llamada ingresa a un gateway por medio de un teléfono convencional discando un número de acceso. Una vez que fue autenticada, la persona disca el número deseado y oye los tonos de llamada habituales hasta que alguien responde del otro lado. Tanto quien llama como quien responde se sienten como en una llamada telefónica "típica".

D3.2.2 GATEKEEPER DE VoIP

Los gateways se conectan con los gatekeepers de VoIP mediante enlaces estándar H.323v2, utilizando el protocolo RAS H.225. Los gatekeepers actúan como controladores del sistema y cumplen con el segundo nivel de funciones esenciales en el sistema de VoIP de clase carrier, es decir, autentificación, enrutamiento del servidor de directorios, contabilidad de llamadas y determinación de tarifas. Los gatekeepers utilizan la interfaz estándar de la industria ODBC-32

(Open Data Base Connectivity – Conectividad abierta de bases de datos) para acceder a los servidores de backend en el centro de cómputos del carrier y así autenticar a las personas que llaman como abonados válidos al servicio, optimizar la selección del gateway de destino y sus alternativas, hacer un seguimiento y una actualización de los registros de llamadas y la información de facturación, y guardar detalles del plan de facturación de la persona que efectúa la llamada.

D3.2.3 SERVIDORES DE BACKEND

El tercer nivel de la arquitectura de VoIP de clase carrier de 3Com corresponde a la serie de aplicaciones de backoffice que constituyen el corazón del sistema operativo de un proveedor de servicios. Las bases de datos inteligentes y redundantes almacenan información crítica que intercambian con los gatekeepers durante las fases de inicio y terminación de las llamadas. En el entorno de una oficina central, resulta vital preservar la integridad de los datos de las bases de datos de backend. La solución de 3Com ofrece un enfoque único que garantiza la resistencia de los servidores de backend y la seguridad de sus bases de datos. Los servidores SQL de Microsoft están integrados dentro de la arquitectura del sistema de Backend y administran las bases de datos SQL para las funciones de autentificación, mapeo de directorios, contabilidad y determinación de tarifas. Este nivel de la arquitectura fue optimizado a fin de responder a las necesidades exclusivas de seguridad y disponibilidad de los proveedores de servicios. Para implementaciones a menor escala, el sistema ofrece flexibilidad para consolidar las bases de datos en un sólo servidor robusto o en la plataforma de un gatekeeper.

D3.2.4 OTRAS SOLUCIONES DE VoIP DE 3COM

Este nuevo sistema se expande sobre la estrategia de convergencia de 3Com para segmentos de mercado clave. 3Com también ofrece soluciones de VoIP para empresas que permiten que los usuarios actuales de routers agreguen voz a su infraestructura empresarial de área amplia ya existente. Los sistemas para empresas también se basan en normas y forman parte de las soluciones end-to-end de la compañía.

D3.3 FUTURO DE LA TECNOLOGIA DE VoIP

En la actualidad, son cada vez más numerosas las compañías que ven esta tecnología como una herramienta de comunicaciones comercialmente viable.

D3.3.1 LAS PREDICCIONES DEL MERCADO

El servicio de voz en protocolos de Internet está atravesando poco a poco el umbral que separa lo novedoso de lo que está generalmente aceptado. Muchas de las portadoras que ofrecen servicios de voz a través de IP fueron creadas principalmente con ese fin, y la industria se encuentra en crecimiento constante. Sin lugar a dudas, los primeros que van a aprovechar las ventajas de la voz sobre IP serán las grandes compañías que, en general, se encuentran geográficamente distribuidas. Según diversas consultoras de nivel internacional, como Frost & Sullivan, IDC y Probe Research, los pronósticos indican un crecimiento significativo en el mercado de voz sobre IP.

VIII.-CONCLUSIONES

Este trabajo trata de dar una visión del amplio campo que abarcan las comunicaciones y redes de computadoras. Destaca principios básicos y temas de fundamental importancia que conciernen ala tecnología.

Los estándares para sistemas de cableado de red sí tratan el tema de los transitorios, especialmente al brindar requisitos de aislamiento. Los diferentes sistemas de cableado de redes varían con respecto a la susceptibilidad a los transitorios, y los usuarios pueden estar interesados en conocer estas diferencias cuando escojan un sistema de cableado, especialmente si la instalación estará en un entorno que se sabe que está sujeto a transitorios. Tales ambientes podrían ser:

- Edificios viejos con un mal sistema de tierra o un cableado viejo.
- Ambientes sometidos a frecuentes caídas de rayos en la cercanía.
- Locaciones donde hay actividades de construcción cercanas.
- Áreas rurales distantes de las subestaciones locales de distribución de potencia.
- Edificios que contienen equipo industrial pesado.

Además, los instaladores de cableado de red deben estar familiarizados con los requisitos de seguridad para LAN de modo que no creen accidentalmente situaciones de peligro potencial.

ATM, es igualmente adecuada para entornos LAN y WAN, para aplicaciones de voz, datos, imagen y video, para redes públicas y privadas. A diferencia de otras tecnologías utilizadas hoy, ATM puede manejar tráfico isócrono y tráfico en ráfagas y proporcionar la Calidad del Servicio (QoS) solicitada. Combina los beneficios de la conmutación de paquetes y la conmutación de circuitos, reservando ancho de banda bajo demanda de una manera eficaz y de costo efectivo, a la vez que garantiza ancho de banda y calidad de servicio para aquellas aplicaciones sensibles a retardos.

La tecnología xDSL permitirá en un futuro la transmisión de datos a altas velocidades utilizando una combinación de cables de fibra óptica y la red telefónica de cobre existente. Esta tecnología proporcionará un acceso a Internet más rápido, así como la transmisión de video interactivo y mayor velocidad para los servicios de comunicación de datos. Sin embargo, aún es necesario definir ciertos aspectos como lo son, el modelo adecuado del ruido, la interferencia con señales de radio y cables aéreos y los códigos de línea que serán utilizados.

MPLS es el último paso en la evolución de las tecnologías de conmutación multinivel (o conmutación IP). La idea básica de separar lo que es el envío de los datos (mediante el algoritmo de intercambio de etiquetas) de los procedimientos de encaminamiento estándar IP, ha llevado a un acercamiento de los niveles de transporte y de red, con el consiguiente beneficio en cuanto a rendimiento y flexibilidad de esta arquitectura. Por otro lado, el hecho de que MPLS pueda funcionar sobre cualquier tecnología de transporte (no sólo sobre infraestructuras ATM) va a facilitar de modo significativo la migración para la próxima generación de Internet óptico, en la que se acortará la distancia entre el nivel de red IP y la fibra. En principio se está suponiendo que se trata de un paquete IP, pero nada impide etiquetar paquetes de otros protocolos (IPX, AppleTalk, etc.). De ahí el calificativo "multiprotocolo" de MPLS.

Las redes inalámbricas pueden tener mucho auge en nuestro país debido a la necesidad de movimiento que se requiere en la industria.

IX.-BIBLIOGRAFIA

David Kruglinski. Guía de las Comunicaciones del IBM/PC. Aosborse/McGraw-Hill. 1984

A. Alaban y J. Riera. Teleinformática y Redes de Computadores. Serie: Mundo electrónico. Teleinformática.

César Macchi y Jean Francois Guilbert. Transporte y tratamiento de la información en las redes y sistemas teleinformáticos. Omega. Serie Informática de Gestión.

Rafael Ale, Fernando Cuellar. Teleinformática. McGraw-Hill. Guía de Conectividad y Redes locales. Libros PC Magazine

http://pclt.cis.yale.edu/pclt/comm/sna.htm

Uyless Black. Redes de Ordenadores. Protocolos, Normas e Interfaces. Ra-ma. Edición: 1989.

Andrew S. Tanenbaum. Redes de Ordenadores. Prentice-Hall. Segunda Edición: 1988.

Dan Kegel's ISDN Page: <www.idiscover.co.uk/isdn/>

Conceptos generales de RDSI: <www.cis.ohio-state.edu/%7Ejain/cis788/isdn/index.htm>

Broadcast ISDN User & Directory: <www.sms.oc.uk/isdn/home.htm>

RDSI en español: <www.geocities.com/SiliconValley/Heights/5770/>

María Jesús Recio. Redes de Ordenadores. Prensa Técnica. Edición de 1997.

José Félix Rabago. Redes de Computadores. Anaya Multimedia. Edición de 1994.

Greg Nunemacher. Introducción a las redes de área local.

Gilbert Held. Internetworking LAN's and WAN's: concepts, techiques and methods.

Roger L. Freeman. Practical data communications.

Andrew S. Tanenbaum. Computer Networks.

FDDI Fundamentals. Artículo de Internet.

Andrew S. Tanenbaum "Computer Networks, second edition" Prentice Hall International Editions, 1989.

Martin de Prycker "Asyncronous Transfer Mode", páginas 260-269. Ellis Horwood series in Computer Comunications & Networking. Ed. Ellis Hoorwod, U.K, 1993.

D. Black "Data Networks", páginas 797-801. Prentice Hall International Editions

Dave Katz "A proposed Standard for the tranmission of IP Datagrams over FDDI Networks". RFC 1188, Octubre 1990.

Michael Tangemann, Klaus Sauer. "Performance Analysis of the Timed Token Protocol of FDDI and FDDI-II". IEEE Journal on Selected Areas in Communications Febrero 1991

Richard O. LaMaire, Ethan M. Spiegel "FDDI Performance Analysis: Delay Approximations". Octubre 1990.

Dionysios Karvelas, Alberto Leon-Garcia "Delay Analysis of Varios Service Disciplines in Symmetric Token Passing Networks". IEEE Transactions on Communications Septiembre 1993.

D. Karvelas, A. Leon-Garcia "Delay Analysis of Timed-Token Protocol And Its Applications to a Hybrid Switching System". Globecomm 1990, páginas 897-901.

D. Karvelas, A. Leon-Garcia "Transmission of Time Critical Information Over FDDI and FDDI-II Networks. Globecomm 1992, páginas 1045-1049

RFC 1619, PPP encima de SONET/SDH, Simpson, W., Mayo 1994.

Emulación de LAN encima de ATM, versión 1.0, Foro de ATM, Febrero 1995.

Multiprotocol encima de ATM (MPOA), versión 1.0, Foro de ATM, Junio 1997.

RFC 1577, IP Clásico y ARP encima de ATM, Laubach, M., Enero 1994.

RFC 1483, Multiprotocol Encapsulation encima de la Adaptación de ATM Capa 5, Heinanen, J., Julio 1993.

RFC 1626, IP MTU Predefinido para el uso encima de ATM AAL5, Atkinson, R., Mayo 1994.

RFC 1755, ATM Señalización Apoyo para IP encima de ATM, Pérez, M., al del et, Febrero 1995.

Draft-ietf-ion-ipatm-classic2-03.txt, IP clásicos y ARP encima de ATM, Laubach, M., Halpern, J, Octubre 1997.

Draft-ietf-rolc-nhrp-12.txt, el próximo Protocolo de Resolución de Brinco (NHRP), Luciani, J., al del et., Octubre 1997.

Draft-ietf-ion-scsp-02.txt, servidor Escondite Sincronización Protocolo (SCSP), Luciani, J., al del et., Octubre 1997.

Draft-ietf-mpls-framework-01.txt, un Armazón para Multiprotocol Label que Cambia, Callon, R., al del et., Julio 1997.

Steve Spanier, Tim Stevenson Tecnologías de Interconectividad de Redes. Editorial Prentice Hall. Cisco Press

Philip Smith. Frame Relay Principles and Applications. Editorial Addison-Wensley Publishers 1993. Data Communications and Networks Series

W. Stallings. ISDN and Broadband ISDN with Frame Relay and ATM. 3Th Ed. Prentice Hall. international editions.

http://webdesk.com/pages/networking/ccitt.html

http://www.dsi.com.mx/

http://www.cisco.com

Cereceda Javier, Houldsworks: Wireless ATM: Technology and Applications, EE 4984: Telecommunication Networks, Abril 15, 1997.

Honcharenko Walter, Kruys Jan: Broadband Wireless Access, IEEE Communications Magazine, Enero 1997.

Sobirk Daniel, Karlsson Johan: An Overview of Proposed MAC Algorithms for Wireless ATM, Computer Netwoks and ATM Networks, 1997.

“Native ATM Service: Semantic Description Version 1" ATM Forum Technical Committee, ATM Forum Document af-saa-0048.000, (Febrero 1996).

T. Zahariadis, J. Sanchez-P, C. Georgopoulos, V. Nellas, T. Arvanitis, D. Economou, G. Stassinopoulos, "Native ATM Protocol Stack for Internet Applications in Residential Broadband Networks," Multimedia Applications Services and Techniques ECMAST’98, Springer, (Mayo 1998).

E. Gauthier, J. Le Boudec and P. Oechslin, "SMART: A many-to-many Multicast protocol for ATM," IEEE Journal on Selected Areas in Communications. Vol. Nº 3 (Abril 1997).

W. D. Zhong, K. Yukimatsu, "Design requeriments and architectures for multicast ATM switching," IEICE Trans. Com., Vol. E77-B, pp. 1420-1428, (Noviembre 1994).

"ATM user-network interface version 3.1 specification", ATM Forum, (1994).

"Traffic Management Specification Version 4.0," ATM Forum Technical Committee, ATM Forum Document af-tm-0056.000, (Abril 1996).

D. Kandlur, D. Saha and W. Willebeck, "Protocol Architecture for multimedia Application over ATM Networks," IEEE Journal Selected and Communications Vol. 14, Nº 7, pp. 1.349-1.359, (Septiembre 1996).

R. Ahuja, S. Keshav and H. Saran, "Design, Implementation, and Performance Measurement of a Native-Mode ATM Transport Layer (Estended Version)," IEEE/ACM Transactions on Networking, Vol. 4, Nº 4, (Agosto 1996).

R. Karabek, "A Native ATM Protocol Architecture Design and Performance Evaluation," IEEE Proceedings 22nd Annual Conference on Local Computer Networks, pp. 204-210, (1997).

D. C. Feldmeier "A framework of architectural concepts for high-speed communications systems," IEEE J. Select. Areas Commun, Vol.11, Nº 4, (Mayo 1993).

T. Anker, D. Breitgand, D. Dolev, Z. Levy, "Congress: Connection-oriented Group-address Resolution Service," Proceeding of SPIE'97 Vol. 3233 on Broadband Networking Technologies, (Noviembre 1997).

T. La Porta and M. Schwartz, "Architectures, Features, and Implementation of High-Speed Transport Protocols," IEEE Network Magazine, pp. 14-22, (Mayo 1991).

"B-ISDN, ATM Adaptation Layer Service. Specific Connection Oriented Protocol (SSCOP) Q.2110," ITU-T, (10 Marzo 1994).

J. Solé-Pareta, J. Vila-Sallent, "Network-based paralell computing over ATM using improved SSCOP protocol," Computer Communications 19 pp. 915-926, (1996).

K. Obraczka, "Multicast Transport Protocols: A survey and Taxonomy," IEEE Communi. Magazine, (1998).

R. Venkateswaran, C.S. Raghavendra, X. Chen and V.P. Kumar, "A Scalable, Dynamic Multicast Routing Algorithm in ATM Networks" IEEE, pp. 1361-1365 (1997).

Matthias Grossglauser and K.K. Ramakrishnan, "SEAM: Scalable and Efficient ATM Multicast," IEEE 1.997, pp. 867-875, (1.997).

M. Nguyen, and M. Schwartz, "MCMP: A Transport/session level Distributed Protocol for Desktop Conference Setup," IEEE Journal Selected and communications, Vol. 14 Nº 7, pp. 1404-1421, (Septiembre 1996)

D. Tennenhouse et al., "A Survey of Active Network Research," IEEE Communications Magazine, (1997).

David C. Feldmeier, Anthony J. McAuley. Jonathan M. Smith, Deborah S. Bakin, William S. Marcus and Thomas M. Releigh, "Protocol Boosters," IEEE JSAC Vol. 16, Nº 3, pp. 437-443, (Abril 1.998).

R. Kishimoto, "Agent communication system for multimedia communication services," INFOCOM'96. Fifteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Networking the Next Generation, Proceedings IEEE Vol. 1, pp. 10-17, (1996).

David A. Halls and Sean G. Rooney, "Controlling the Tempest: Adaptive Management in Advanced ATM Control Architecture," IEEE JSAC Vol. 16, Nº 3, pp. 414-423, (April 1.998).

http://fiddle.ee.vt.edu/courses/ee4984

http://www.tts.lth.se/personal

http://www-comm.itsi.disa.mil/atmf/watm.html

http://fiddle.ee.vt.edu/courses/ee4984

http://www.tts.lth.se/personal

http://www-comm.itsi.disa.mil/atmf/watm.html

GigabitEthernet. Características y prestaciones. Comunicaciones World, Diciembre 1996.

GigabitEthernet. Perspectivas de mercado. Comunicaciones World, Diciembre 1996.

GigabitEthernet. Moviliza la industria. Comunicaciones World, Diciembre 1996.

Andersson L. et al., "LDP Specification", Internet Draft, <draft-ietf-mpls-ldp-05.txt>, Junio 1999

Awduche D.O. et al., "Requirements for Traffic Engineering over MPLS", Internet Draft, <draft-ietf-mpls-traffic-eng-01.txt>, Junio 1999

Callon R. et al., "A Framework for Multiprotocol Label Switching", Internet Draft, <draft-ietf-mpls-framework-04.txt>, Julio 1999

Rosen E.C., Viswanathan A., Callon R., "Multiprotocol Label Switching Architecture", Internet Draft, <draft-ietf-mpls-arch-06.txt>, Agosto 1999

Semeria C., "Multiprotocol Label Switching: Enhancing Routing in the New Public Network", Juniper Networks Inc., White Paper, http://www.juniper.net/techcenter/techpapers/mpls/mpls.html, Marzo 1999

Semeria C., "Traffic Engineering for the New Public Network", Juniper Networks Inc., White Paper, Enero 1999, http://www.juniper.net/techcenter/techpapers// TE_NPN.html

Semeria C., Stewart III J.W., "Optimizing Routing Software for Reliable Internet Growth", Juniper Networks Inc., White Paper, Julio 1999, http://www.juniper.net/techcenter/techpapers/optimizing-routing-sw.fm.html

Charter IETF sobre MPLS http://www.ietf.org/html.charters/mpls-charter.html

Blake S. et al., "An Architecture for Differentiated Services", RFC 2475, Diciembre 1998

Li T., Rekhter Y., "A Provider Architecture for Differentiated Services and Traffic Engineering (Paste)", RFC 2430, Octubre 1998

Nichols K. et al., "Differentiated Services Operational Model and Definitions", Internet Draft, <draft-nicholsdsopdef-00.txt>, Febrero 1998

Shenker S., Partridge C., Guerin R., "Specification of Guaranteed Quality of Service", RFC 2212, Septiembre 1997

Stephenson, "DiffServ and MPLS: A Quality Choice", Tech Tutorial, Noviembre 1998, http://www.data.com/issue/981121/quality.html

Xiao X., NI L., "Internet QoS: A Big Picture", IEEE Network Magazine, Marzo-Abril 1999

Redford R., "Enabling Business IP Services with Multiprotocol Label Switching", Cisco Systems, Inc., White Paper, 1999 http://www.cisco.com/warp/public/cc/cisco/mkt/wan/ipatm/tech/mpls_wp.htm

"Intranet and Extranet Virtual Private Networking", Cisco Systems, Inc., Technical Service Description, http://www.cisco.com/warp/public/cc/cisco/mkt/servprod/dial/tech/ievpn_rg.htm

"Delivering New World Virtual Private Networks with MPLS", Cisco Systems, Inc., White Paper, http://www.cisco.com/warp/public/cc/cisco/mkt/servprod/dial/tech/mpls_wi.htm

Trillium. Multiprotocol Label Switching (MPLS). The International Engineering Consortium, http://www.iec.org/tutorials/ .

Netplane. A comparison of Multiprotocol Label Switching (MPLS) traffic-engineering initiatives. The International Engineering Consortium, http://www.iec.org/tutorials/.

Riverstone Networks. MPLS: Making the Most of Ethernet in the Metro. http://www.mplsrc.com/articles.shtml .

Paul Brittain y Adrian Farrel. Data Connection. MPLS traffic engineering: a choice of signaling protocols. http://www.mplsrc.com/articles.shtml .

André Danthine MPLS – The New IP Architecture. MPLS World Congress, Paris, Febrero de 2001.

Zhensheng Zhang, James Fu, Dan Guo, and Leah Zhang “Lightpath Routing for Intelligent Optical Networks” Network Interactive Julio 2001.

Gurusamy Mohan “Ligthpath Restoration in WDM Optical Networks” Network Interactive November 2000.

Bala Rajagopalan, Dimitrios Pendakaris, Debajan Saha and Krishna Bala “IP over Optical Networks: Architectural Aspects” Communications Interactive Septiembre 2000.

Jaafar M. H. Elmirghani and Hussein T. Mouftah “All-Optical Wavelength Conversion: Technologies and Applications In DWDM Networks” Communications Interactive March 2000.

Jonh M. Señor, Michael R. “Developments in wavelength Division Múltiple Access Networking” Communications Interactive December 1998.

IEEE Communications Magazine www.comsoc.org/pubs/commag/commag.html

Optical Network Magazine optical-networks.com/editor.htm

The Optical Internetworking Forum www.oiforum.com

G. Corral, J. Abella. ADSL y MPLS. Editorial Ingeniería La Salle. Madrid, España, 1997.

Barberá, José. MPLS: Una arquitectura de backbone para la Internet del siglo XXI. Revista: Actas del V Congreso de Usuarios de Internet. Mundo Internet 2000. Madrid, febrero 2000. Madrid, España, 1997.

Rui T. Valadas, Adriano C. Moreira, A.M. de Oliveira Duarte. Documento IEEE "Redes Híbridas" páginas 21-26. 1992 universidad de Aveiro, Portugal.

T.J. Watson Reserach Center Charles E. Perkins. Documento IEEE "Ruteando con TCP/IP" páginas 7-12. 1992 IBM

Chandos A. Rypinski. Documento IEEE "Características de una Radio LAN" páginas 14-19. 1992 LACE Inc.

Nicolás Baran.Revista PC/Tips Byte páginas 94-98. Articulo: "Redes Inalámbricas". Abril 1992

Padriac Boyle. Revista PC/Magazine páginas 86-97. Artículo: "Sin Conexión". Marzo1995.

Sheldon Tom. LAN Times Encyclopedia of Tetworking

R. Arick Martin. The TCP/IP Companion, a Guide for the Common User.

Hopper, Temple, Williamson. Diseño de Redes Locales.

Freedman Alan. Diccionario de Computación.