Capítulo 7: Interconexión de Redes:La evolución de LANs a WANs y de estas a Redes de Banda Ancha. Tecnologías tradicionales.

Objetivos: Describir la evolución natural de las redes de comunicación digitales. Explicar las tecnologías tradicionales de interconexión de redes: conexiones punto a punto de baja capacidad, sistemas de transporte,(T1 a T4,y E1 a E4 y su necesidad de sincronización, PDH y SDH),y los protocolos de interconexión más importantes: X.25,TCP/IP, y Netware IPX.

7.1.-Desarrollo natural de las Redes de Comunicación Digitales.

En el **Capítulo 1** se ha hecho referencia extensamente a las **Redes de Comunicaciones**, y se mostró que su evolución, debido a razones históricas, ha sido **progresiva** y en **diversas direcciones**, se comenzó con la red telegráfica, luego la telefónica, siguieron las redes privadas y públicas de datos, las redes de CATV, Internet, etc.

Estas Redes de Comunicaciones, al tratar de satisfacer **necesidades** siempre crecientes producidas por la evolución del ser humano y de la sociedad que este conforma, son dinámicas. Y lo son no “per se”(aún no hemos llegado a ese punto de desarrollo tecnológico, no descartable en un futuro cercano),sino por la acción de los administradores de las redes, que responden a los requerimientos de los usuarios.

Las **Redes de Computadoras** fueron descriptas en la **Sección 1.4,**en la **Sección 4.1** se mencionó que las **Redes de Computadoras** son un subconjunto de las **Redes de Comunicación Digitales**(datos, voz y video),que a su vez lo son de las **Redes de Comunicación**(que abarcan tanto las analógicas como las digitales).

Sin embargo la digitalización creciente de voz y video, así como la utilización de computadoras(ó más bien procesadores en el lenguaje del Capítulo 4)para su almacenamiento, proceso y transferencia hacen que las técnicas utilizadas por ellas sean comunes.

Por lo tanto las fronteras entre esos tipos de Redes son cada vez más borrosas y los nombres, por costumbre, se usan indistintamente. En consecuencia, salvo raras excepciones, nos estaremos refiriendo siempre a **Redes de Comunicación Digitales.**

Como se dijo en la **Sección 4.1** las “redes de computadores” ó más bien las **Redes de Comunicación Digitales** enlazan computadores(procesadores), cercanos ó distantes(LAN.MAN ó WAN), con diversos propósitos. Los más importantes son: **compartir recursos tales como programas, datos y equipos; aumentar la fiabilidad disponiendo de recursos alternos; ahorrar distribuyendo las funciones entre computadores de bajo costo; establecer: sistemas de correo electrónico, distribución de noticias, transferencia de archivos ASCII y binarios; comunicación de voz, audioconferencia, videoconferencia, sistemas de información tipo multimedia (WWW); etc.**

La importancia de interconectar computadores surgió al mismo tiempo que estos e históricamente puede decirse que hubo dos concepciones distintas de hacerlo, una que pudiera denominarse WAN y la otra LAN.

En los 60 y 70 IBM concibió la computación como una gran **computador central**(mainframe) con funciones masivas de procesamiento y almacenamiento de datos que presta servicios interactivos ó por proceso, a cientos(tal vez miles) de **terminales** e **impresoras** remotos, utilizándose **controladores**(que atendían localmente a grupos de terminales)y se conectaban vía modems con un **FEP(F**ront **E**nd **P**rocessor)que liberaba al computador central de las tareas de comunicaciones,tal como se mostró en la **Figura 2.27.** Esta estructura jerárquica fue adoptada por muchos fabricantes e IBM la formalizó en una arquitectura que denominó **SNA**(**S**ystems **N**etwork **A**rchitecture).Obviamente el hecho de tener grupos de terminales a enormes distancias del computador central y la necesidad de interconectar "mainframes" distantes hizo que se prestase gran atención a lograrlo con eficiencia, dando lugar a redes amplias, mejor conocidas como **WAN.**

La invención del modem impulsó las WAN y estas usufructuaron de tecnologías como líneas discadas, lineas dedicadas, multiplexión, lineas digitales(DDS, Digital Data Service a 56 kbps)) y enlaces con muchos canales a 64 Kbps(T1 a 1,544 Mbps ó T3 a 45 Mbps),a las que nos referiremos más adelante.

La otra concepción, LAN, puede decirse que comenzó con la red ALOHA de la Universidad de Hawai(ver **Capítulo 6**)descripta en 1970 en un "paper" de Abramson**[1]**,y fué creada para permitir la interconexión vía radio entre un computador central y terminales dispersos en las islas, además utilizaba conmutación de paquetes. Por otra parte las bases de "token ring" fueron establecidas en 1969 pero aplicadas a telefonía no a datos, asimismo la tecnología Ethernet fue utilizada por Xerox en 1972 en un bus interno de las fotocopiadoras.

En 1977 la empresa Datapoint Corporation lanzó al mercado la primera red LAN comercial:**ARCnet**, ésta utilizaba tecnología "token passing" con topología lineal ó estrella, operaba a 2.5 Mbps e interconectaba computadoras Datapoint de modo que pudiesen compartir archivos, impresoras, etc. Inmediatamente comenzaron a venderse gran cantidad de ARCnet pues eran baratas y fáciles de instalar.

Sin embargo este éxito tuvo corta vida pues otras importantes empresas, como ya se dijo, tenían la tecnología y la capacidad de acceder a tan promisor mercado.

Así Digital Equipment Corporation(DEC) en 1959 creó un computador llamado PDP-1(Programed Data Processor),este evolucionó hasta el PDP-11 y luego una familia de computadores de 32 bits con VAX(Virtual Address Extension) que dio lugar a las minicomputadoras, para las que también implementó un sistema de red que llamó DNA(**D**istributed **N**etwork **A**rchitecture)pero conocido como DECnet, que no copiaba el esquema monolítico de IBM sino que combinada los recursos de procesamiento y almacenamiento de esos minicomputadores. Como DEC,y más aún sus clientes deseaban una velocidad que no daban los enlaces tipo WAN, debió cambiar distancia por velocidad y emplear la tecnología LAN.

A fines de los 70 Xerox, Intel y DEC unieron esfuerzos y produjeron Ethernet version 1.

Por su parte IBM,que en 1982 lanzó su PC(Personal Computer),reaccionó a mediados de los 80 con su red "token ring"(red en anillo con testigo)que comenzó a 4Mbps y luego fue llevada a 16 Mbps, esta es también una LAN.

Ante tal proliferación de tecnologías propietarias intervino IEEE y aparecieron los estándares de la serie 802 ya descriptos en el **Capítulo 6.**

Ha ocurrido que la tecnología SNA desapareció, debido a que las PC han experimentado una drástica disminución en el costo y un enorme aumento de la capacidad de procesamiento dando paso a las LAN.

Pero las LANs aisladas son de poca utilidad, existe pues la **necesidad** de interconectarlas a fin de extender en distancia las características que las hicieron existir y perdurar, dando paso a las Redes Digitales de Comunicaciones.

La UIT(Unión Internacional de Telecomunicaciones)emplea los términos "Modo de Transferencia" ó "Técnica de Transferencia" para referirse a las técnicas empleadas en la interconexión, que cubren los aspectos de: transmisión, multiplexión y conmutación.

Las **necesidades** de interconexión, son producidas y a la vez posibles de satisfacer, por la existencia de estaciones de trabajo cada vez más poderosas en : número de instrucciones por segundo, facilidades de comunicación, manejo de imágenes y sonido, etc. La enumeración de estas necesidades no es fácil, pero daremos una lista sin pretender agotar el tema:

- Transferencia de grandes volumenes de datos a gran velocidad, para aplicaciones como CAD/CAM (Computer Aided Design/Computer Aided Manufacturing), elaboración de imágenes médicas(telemedicina),etc.

- Transferencia de sonido y video para aplicaciones como:

  Enseñanza y entrenamiento a distancia.
  Videoconferencia y videotelefonía.
  Trabajo a distancia (telecommuting, empresas virtuales).
  Simulaciones, juegos, realidad virtual, que requieren de sonido y video interactivo.
  Multimedia distribuido para educación, entretenimiento, comercio, turismo, etc.
  Video por demanda con evolución hacia HDTV(High Definition Television),video interactivo y realidad virtual.

Los diversos servicios tienen requerimientos de velocidad de transmisión muy diferentes, la Tabla 7.1 dá algunos valores representativos.

Aplicación	Velocidad requerida(ancho de anda)
Datos,ráfaga	1 Mbps
Audio Digital	1.411 Mbps
Video Comprimido(MPEG-2)	4-6 Mbps
Gráficos de documentos	20-100 Mbps
Video comprimido calidad broadcasting	20-100 Mbps
HDTV,full motion	1-2 Gbps

Tabla 7.1

Estos resultados son fáciles de obtener: un cuarto de pantalla de una PC puede utilizar 200 x 200 pixeles, con 24 colores por pixel y 15 pantallas por segundo, lo que da 200 x 200 x 24 x15 = 14.4 Mbps,a lo que hay que agregar unos 32 Kbps para voz ó 384 Kbps para un estereo razonable. Si el cálculo se hace para una pantalla completa SVGA de 1024 x 768,24 colores y 30 pantallas por segundo tendremos 566 Mbps, es evidente la necesidad de compresión, de ello se han ocupado el CCIR(recomendación 601), Digital Video Interactive (DVI),el CCITT (recomendación H.261), Joint Motion Photographic Experts Group(JPEG) y Motion Picture Experts Group(MPEG)con sus estandares MPEG-1,2,3 y 4(200:1)mencionados en **Sección 3.6.** .

Las compresiones de 100:1,dan los resultados mencionados en la Tabla 7.1,a ello agregaremos que con uno de esos esquemas(MPEG-2) se logran aplicaciones de video que para videoconferencia van de 128 a 768 Kbps, a 1.3Mbps para calidad VCR ó CD-ROM y 6 Mbps para video de entretenimiento, otros esquemas:fractales(.fif)y wavelets(.wa)ofrecen mejoras.

La **realidad** de las redes tiende a satisfacer esas necesidades, las LANs deben ser interconectadas, utilizando repetidores, puentes, ruteadores y puertos (gateways),con los que rápidamente se configuraron MAN's y WAN's tanto privadas como públicas que pueden hacer uso de la red telefónica, redes digitales, u otras(CATV).

La aparición de redes locales(LAN's) de **muy alta velocidad** como FDDI, 100BaseT,etc requiere de interconexiones cónsonas.

La tecnología a su vez mediante la **fibra óptica**, el **perfeccionamiento del par de cobre** y los usos de la **radiopropagación**(enlaces de microondas, satélites y packet radio) van dando lugar a "**backbones**" ó **troncales de gran capacidad**.

Las interconexiones, ya sea entre computadores ó entre redes locales, comenzaron utilizando **líneas dedicadas**, esto tiene dos inconvenientes importantes:

- la arquitectura, por ser punto a punto **es poco flexible,** y el acceso a diversos puntos da lugar a redes de conectividad total(tipo mesh)cuyo costo es prohibitivo.
- el tráfico, cuando se trata de LANs, correo eléctrónico, consulta de base de datos, etc, es **tipo ráfaga,** durante un tiempo muy corto se requiere de gran ancho de banda y luego hay un período de inactividad, obsérvese que la multiplexión(TDM)no resuelve el problema.

De modo que fue necesario utilizar otros esquemas de interconexión, así aparecieron las **redes de difusión** y las **conmutadas** en sus diversas versiones.

Tenemos entonces:

- **Conexion fija**, líneas dedicadas, tipo T1/E1 a T4/E4,etc.
- **Redes de Difusión.**(ver Secs 6.4,5 y 6)
- **Redes Conmutadas**, dado que las anteriores no siempre satisfacen el servicio a prestar
  La conmutación tuvo sus orígenes en telefonía analógica(POTS, Plain Old Telephone System)y en digitales podemos distinguir varios tipos de conmutacion:
  - **Conmutación de circuitos(CSDN**).
    con dos versiones: una con conmutadores rápidos apropiada para sesiones cortas, y otra con conmutadores más lentos que se usa en sesiones largas, llamada "conmutación de canal".
  - **Conmutación de mensajes**(ver Sec.5.2 y 5.3)
  - **Conmutación de paquetes(PSDN)**.(ver Sec.5.2 y 5.3)

Tener una red para cada tipo de servicio(datos, voz, video)es ilógico ,más aún cuando la digitalización unifica, por ello la tendencia hacia **ISDN**(**I**ntegrated **S**ervices **D**igital **N**etwork) y **BISDN**(**B**roadband **ISDN**)es muy grande.

Las **redes de banda ancha,ó broadband networks**, son fundamentalmente redes de **servicios integrados,** que al unir voz, video y datos, todos ellos bajo la forma digital, no solo requieren de altas velocidades(high speed networks ó gigabits networks),sino de una adecuación al tipo de servicio pues en voz y video estamos trabajando en tiempo real.

En lo que sigue describiremos las tecnologías de interconexión y/o protocolos, existen tres grupos:

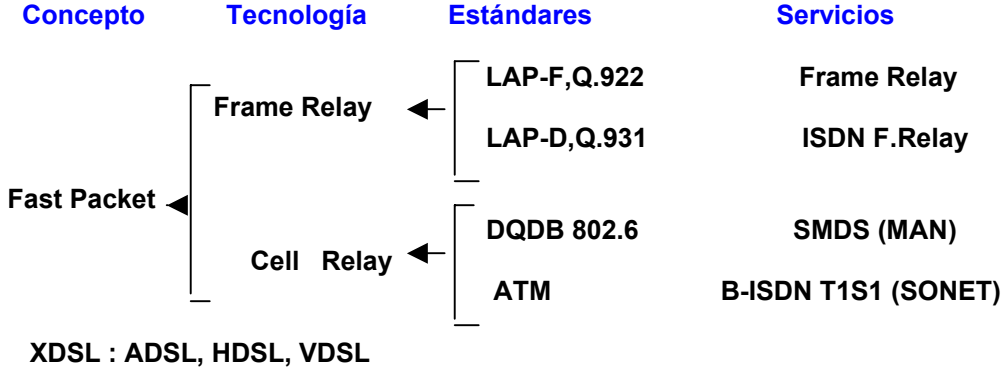
- **Tradicionales**(que no son de banda ancha),tales como:
  - **Conexiones punto a punto** y que a veces se llaman **conexiones de circuitos:**
    - **Sistemas de baja capacidad : líneas analógicas y digitales desde 56 Kbps** (ya sean **fijas** ó **conmutadas**).
    - **Sistemas de transporte ó sistemas portadores,** comenzaron con **T1 a T4** y pasaron a DS1 a DS4,son **plesíncronas**(término que se explicará dentro de poco).
  - **Conmutación de paquetes: tipo X.25,TCP/IP y Netware(IPX).**
- **Nuevas tecnologías**

  Nos van acercando al objetivo de redes de banda ancha, ellas son:

  SDH/SONET

  WDM/DWDM

  Fast Packet es un **concepto de interconexión de redes** generado por la existencia de **emisores y receptores más inteligentes** y por **enlaces digitales de alta velocidad** y **pocos errores**, de manera que puede enviar datos(pero no direcciones)con errores, de cuya detección y corrección se ocuparan capas superiores.



- **Banda Ancha: ISDN , BISDN**

  Que son soportadas por algunas de las nuevas tecnologías.

Tecnologías de interconexión tradicionales

7.2.-Conexiones punto a punto.

7.2.1.-Sistemas de baja capacidad.

Las **conexiones punto a punto** establecen una conexión física entre la estación local y la remota suministrando un **ancho de banda dedicado** durante todo el tiempo que dura la conexión.

Existen **conexiones punto a punto dedicadas** y **conexiones punto a punto conmutadas** y normalmente son servicios suministrados por las LEC(Local Exchange Carriers) ó Compañías de Teléfono Locales en conjunto con Compañias de Larga Distancia.

El miembro más simple de esta familia de conexiones punto a punto es la "vieja" **línea telefónica conmutada** que corresponde a la POT(Plain Old Telephony),le sigue la **línea telefónica analógica dedicada.**Ambas hacen uso de **modems** y al calcular su costo debe tenerse en cuenta además del costo de la línea(normalmente la conmutada se paga por tiempo y distancia mientras que la dedicada sólo por distancia)el valor de un modem en cada extremo.La velocidad máxima que se logra en estas líneas es de 56 Kbps(sin compresión),ver **Sección 2.7**,aunque este valor no es garantizado, pues depende grandemente de la calidad de las líneas, que normalmente dejan mucho que desear.

Le sigue **DDS**(**D**igital **D**ata **S**ervice),donde el usuario se conecta a una línea digital que le une a la Oficina Central(CO,Central Office)de la empresa telefónica mediante un dispositivo denominado **DSU/CSU**(**D**ata **S**ervice **U**nit/**C**hannel **S**ervice **U**nit) que remplaza al modem y cuyas funciones son: **DSU**: se conecta serialmente con el usuario(vía RS-232,V.35,RS-442),formatea los datos para transmitirlos sobre la línea digital y controla el flujo de datos,**CSU**:termina la conexión de larga distancia en el extremo del usuario, procesa las señales digitales para la línea digital, puede hacer loopback y sirve como defensa del servicio digital contra equipos de usuario dañados. Como no hay conversión analógica-digital y viceversa estas líneas se usan hasta 56 Kbps,pero tienen limitaciones de distancia entre el usuario y la CO. La señal una vez en la CO puede ser multiplexada para su transporte a grandes distancias.Aquí también al costo de la línea debe agregarse el de las DSU/CSU.El valor de 56 Kbps en lugar de los 64 Kbps que uno esperaría(tal como se verá al considerar DS0)surge del hecho de que esta línea debe llevar, además de los datos información los de control,eso se hace utilizando para datos solo 7 de cada 8 bits transmitidos.Este método de señalización se denomina *in band signaling.*

Además de los DDS existen el **Switched-56**(SW56) que permite efectuar llamadas a otro suscriptor del SW56 en el país, y a veces inclusive internacionalmente. El equipo DSU/CSU incluye un teclado para introducir el número del abonado lejano en forma similar a lo que ocurre con los teléfonos.

Si los 56 Kbps son insuficientes el usuario tiene la posibilidad de combinar varios canales de 56 Kbps llevando su capacidad hasta 384 Kbps ó contratar sistemas de transporte de alta capacidad(hasta 45 Mbps).

En las líneas conmutadas,un problema importante es precisamente el del **sistema de conmutación** que se compone de: la red de conmutación,interfaces en el lazo del abonado, interfaces troncales,control de conmutación,operación y mantenimiento(OAM) e interfaces de control **[7],[8]**,otro importante aspecto es la **señalización**,tanto a nivel de suscriptor como a nivel de troncales,y hablamos de señalización en el propio canal ó de señalización en canal separado,este último esquema se denomina también **señalización en canal común**(**CCS C**ommun-**C**hannel **S**ignaling)estandarizado en el CCS7,**[7],[8].**

7.2.2.-Sistemas de Transporte ó Portadores.

Los **sistemas de transporte ó sistemas portadores**,se diseñaron inicialmente para optimizar el uso del medio físico, que en esa época era el par de cobre,pues resultaba antieconómico utilizar ese medio para un solo canal de voz ,la solución fué el **multiplexaje**.

Se comenzó con el multiplexaje **analógico**,llamado **FDM(Frequency Division Multiplexing),**que fué extensamente usado en enlaces de pares de cobre,coaxiales y de microondas,pero que hoy ha perdido importancia frente a los similares digitales.

A continuación se resumen los niveles de multiplexión analógica más comunes.

Niveles de multiplexaje FDM

12 canales telefónicos analógicos son multiplexados en un **grupo básico**

5 grupos básicos son multiplexados en un **super grupo básico**

10 supergrupos básicos son multiplexados en un **grupo maestro básico**

6 grupos maestros básicos son multiplexados en un **grupo jumbo básico**

2 grupos jumbo básicos son multiplexados en un nivel **AR6A**[1]

3 grupos jumbo básicos son multiplexados en un nivel **L5**

3 niveles intermedio de 4200 canales son multiplexados en un nivel **L5E**

Tenemos entonces:

Grupo básico = 12 canales
Super grupo básico = 60 canales
Grupo maestro básico = 600 canales
Grupo jumbo básico = 3600 canales
Nivel AR6A = 6000 canales
Nivel L5 = 10800 canales
Nivel L5E = 13200 canales.

A los sistemas analógicos siguieron los **digitales** y describiremos en forma básica los **sistemas de transmisión digitales**,comunmente conocidos como **sistemas digitales de transporte**(digital carrier systems),estos sistemas de alta capacidad son de importancia tanto para las empresas de telecomunicaciones de transporte(telecommunication carriers), como para los usuarios finales,son punto a punto y por lo tanto **conexiones fijas**.

La tecnologia de transporte digital fué instalada inicialmente (1962) entre Oficinas Centrales(OC) metropolitanas,desde comienzos la década del 80 la tecnología de multiplexaje digital estuvo disponible para el usuario final bajo la forma de líneas privadas **T1**(nomenclatura que se explicará más adelante),y poco más tarde como líneas privadas **T1 fraccionales**(parte de T1).

[1] AR6A es un sistema de transmisión single sideband (SSB).

A sus comienzos el transporte digital estuvo intimamente ligado a la transmisión digital de voz y a PCM,luego aparecieron esquemas de digitalización de voz no-PCM, y aplicaciones de transmisión de datos de alta velocidad que hacen importante describir este sistema indudablemente influído por su origen telefónico.

La multiplexión en transmisión digital es **TDM(Time Division Multiplexing)**,la jerarquía tradicional era los **portadores T(T-carriers)**donde la T viene de telefonía y se refiere a medios de cobre que llevan 24(**T1**),96(**T2**),672(**T3),**4032(**T4**) y 8064(**T5**) canales de voz a 64 Kbps,velocidad que corresponde al canal de voz 0-4Khz muestrado,cuantificado y codificado.

Hoy muchos sistemas de transporte ó portadores ya no utilizan medios de cobre por lo que la denominación adecuada para esos niveles de multiplexaje es :**DS1, DS2,DS3, DS4 y DS5**,donde **DS** va por **D**igital **S**ystem.

A continuación se resumen los niveles de multiplexión digital más comunes:

Niveles de multiplexaje TDM

24 canales telefónicos(64 Kbps c/u)son multiplexados en nivel **DS1**

48 canales telefónicos(64 Kbps c/u)son multiplexados en nivel **DS1C**

96 canales telefónicos(64 Kbps c/u)son multiplexados en nivel **DS2**

2 niveles DS1 son multiplexados en un nivel **DS1C**

4 niveles DS1 son multiplexados en un nivel **DS2**

28 niveles DS1 son multiplexados en un nivel **DS3**

14 niveles DS1C son multiplexados en un nivel **DS3**

7 niveles DS2 son multiplexados en un nivel **DS3**

6 niveles DS3 son multiplexados en un nivel **DS4**

Tenemos entonces:

DS1 = 24 canales
. **DS1C** = 48 canales
DS2 = 96 canales
DS3 = 672canales
DS4 = 4032 canales

Esta es la jerarquía digital utilizada en los Estados Unidos que tiene 1.544 Mbps para 24 canales,3.152 Mbps para 48 canales,6.312 Mbps para 96 canales,44.736 Mbps para 672 canales,274.176 Mbps para 4032 canales y 560.160 Mbps para 8064 canales(**DS5**).La diferencia entre el resultado de multiplicar 64 Kbps por el número de canales corresponde a un pequeño numero de bits que se denomina encabezamiento(overhead),Según que se utilicen en sistemas de fibra ó en radioenlaces,se dan otras denominaciones.

Nivel Digital	Mbps	Facilidades de Transmisión		
		Cobre	Radio	Fibra Optica
DS4	274,176	T4M	DR18	
DS3	44,736		3ARDS	FT3
DS2	6,132	T2		
DS1C	3,152	T1C,T1D		
DS1	1,544	T1,T1/OS	1ARDS	
DS0	0,064			

Un esquema similar de TDM se ha adoptado en Japón.

En Europa la jerarquía digital está basada en 30 canales de voz(64 Kbps),en realidad son 32 canales de los que 2 son de señalización,por lo que comenzando con ese nivel básico,llamado **E1** que está a 2.048 Mbps,sigue **E2** con 120 canales a 8.448 Mbps,**E3** con 480 canales a 34.368 Mbps y **E4** con 1920 canales a 139.264 Mbps,tal como se muestra en la **Figura 7.1,**la formación del multiplexado es muy interesante pero escapa al objetivo de esta parte,ver **[5]**páginas 23 a 35.

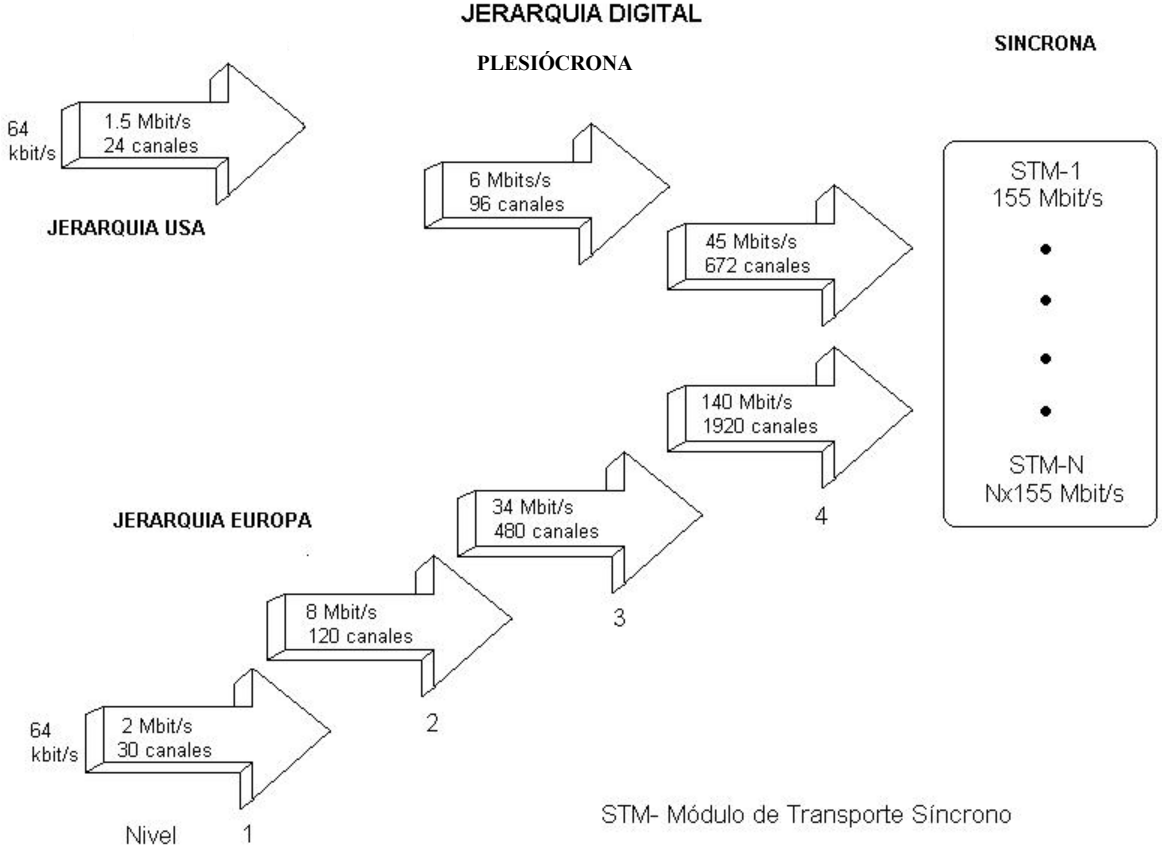


Figura 7.1
Jerarquía Digital Plesiócrona con sus niveles y evolución hacia Jerarquía Digital Síncrona(JDS),base de BISDN(RDSI-BA)

Es ilustrativo analizar como es el formato de las señales digitales pues debe establecerse un sistema que permita determinar cúal bit ó grupo de bits corresponde a determinado canal,para ello hay dos esquemas:

- bits de alineación de trama,norma americana,jerarquía DS.
- alineación por palabra,norma europea,jerarquía E.

Comenzaremos con la norma americana explicando el sistema DS1**[2]** y luego veremos el europeo.

Inicialmente el sistema D1 de AT&T,ahora llamado **D1A**,utilizaba un PCM de 24 canales cada uno cuantificado a 7 niveles,o sea 7 bits a los que se agrega uno de señalización,dando 8 bits,un **byte ú octeto**,por canal.Resulta así que como tenemos en PCM 8000 muestras por segundo cada canal opera a 56 Kbps..

Tenemos entonces 24 canales ó subgrupos de 8 bits cada uno,a los que se agrega un bit adicional para ubicar el comienzo de este grupo llamado **"frame"ó trama** lograndose así la "sincronización",ese bit adicional naturalmente se llama **"framing bit"** ó **F-bit** ó **bit de alineación** y se transmite al final(last bit) de los 192 bits de información.Por lo tanto como cada canal ocupa 5.2μseg,tendremos una duración de la trama de 125.45μseg(24x5.2+0.65).

Como el muestreo dá 8000 muestras por segundo tendremos 8000 tramas por segundo cada una de 193 bits(24x8+1),lo que dá 1.544 Mbps.

Este esquema fué modificado tomando el nuevo sistema el nombre de **D1D**,y lo que se hizo fué utilizar los 8 bits de cada octeto para enviar información(256 niveles),cambiar el μ del PCM de 100 a 255,con lo que se mejoró sensiblemente la relación señal a ruido.El número de bits por trama sigue siendo 193,y hay dos incognitas por despejar: una como el "framing bit"permite determinar el comienzo de la trama y la otra como se señaliza si el bit respectivo se usa ahora(D1D)para información.

Las soluciones son ingeniosas,hay por lo menos cinco,dos de ellas son utilizadas comunmente y corresponden a la Recomendación G.704 del CCITT.

La primera llamada **SF Superframe Format**,consiste en agrupar 12 tramas en una **supertrama(superframe)**que el CCITT llama **multitrama**,cuya duración será de 1.505mseg.Los 12 F-bits se dividen en dos grupos alternados:pares $\mathbf{F_s}$ é impares $\mathbf{F_t}$

Los pares llevan la secuencia 001110 y se usan para identificar las tramas 6 y 12 que son tramas de señalización,las impares conforman unos y ceros alternados (101010) , se utilizan para sincronización.

La secuencia total de F-bits es 100011011100,y su identificación es clave para determinar el comienzo de cada octeto,para ello el equipo receptor debe comenzar postulando que un bit de valor 1 cualquiera es el primer F-bit,luego observa el bit que está 192 bits más alla para ver si es un 0,si no lo es busca el siguiente 1 para reiniciar el proceso,si sí es mira 192 bits más allá en busca de otro 0,y así sucesivamente hasta localizar la secuencia ó **bandera(flag)** completa,obviamente el receptor debe almacenar las 12 tramas(2316 bits)para hacer este proceso.

Como se dijo las tramas 6 y 12 se usan para señalización,en cada una de ellas el bit 8 de cada octeto es "robado" y se usa para señalización reduciendose así el número de bits para información(solo en esas tramas)a 7 bits,cada bit de la trama 6 conforma el canal de señalización A del canal respectivo,lo mismo ocurre con la trama 12,que dá lugar al canal de señalización B,cada canal de señalización opera a 667 bps(1 bit cada 1.5 ms)combinados lo hacen a 1333 bps.La **Tabla 7.2** sumariza estas reglas.

Frame Number	Frame Alignment Signal (Mirar Nota1)	Multiframe Alignment Signal (S bit)	Bit Number(s) in Each Channel Time Slot		Signaling Channel Designation (Mirar Nota 2)
			For Character Signal	For Signaling	
1	1	-	1-8	-	
2	-	0	1-8	-	
3	0	-	1-8	-	
4	-	0	1-8	-	
5	1	-	1-8	-	
6	-	1	1-7	8	A
7	0	-	1-8	-	
8	-	1	1-8	-	
9	1	-	1-8	-	
10	-	1	1-8	-	
11	0	-	1-8	-	
12	-	0	1-7	8	B

Nota 1: When The S-bit is modified to signal the alarm indications to the remote end, the S-bit in frame 12 is changed from 0 to 1.
Nota 2: Channel associated signaling provides two independent 667-bit/s signaling channels designated A and B or one 1333 bit/s signaling channel.

Tabla 7.2

La segunda solución llamada **Extended Superframe Format(ESF)**es consecuencia del desarrollo tecnológico,recuerdese que en el SF se usa 1 bit de alineación de trama en cada trama y como hay 12 tramas en 1.5 mseg significa que 8Kbps de “ancho de banda” son destinados a alineación,el mismo resultado se puede lograr ahora con solo 2Kbps quedando 6Kbps para otro uso.

El ESF forma una **supertrama ó multitrama**(terminología CCITT)de 24 tramas, sigue teniendo un F-bit cada trama,pero se comparten en tres usos:

- **FAS** la tradicional trama de alineación,que en este caso es 001011,con un bit cada 579 bits,lo que dá una velocidad de 2Kbps.
- **DL**,Data Link,comenzando con la trama 1, cada trama impar provee de un bit ,lo que dá lugar a un canal de 4Kbps usado para datos y secuencias de canales inactivos ó secuencia de pérdida de alineación de trama(16 bits,8 ceros y 8 unos).
- **CRC**, transmite a 2Kbps el bloque de mensaje de CRC-6 llamado CMB,que es una secuencia de 4632 bits(coincide en longitud con la multitrama).

La **Tabla 7.3** siguiente ilustra este formato ESF,y también muestra los canales de señalización,similares a los A y B mencionados,que aqui se dividen en 4:A,B,C y D.

Multiframe Number	F Bits				Bits Number(s) in each Channel Time Slot		Signaling Channel Designation
	Multiframe Bit Number	Assignments			For Character Signal	For Signaling	
		FAS[a]	DL[b]	CRC[c]			
1	0	-	n	-	1-8	-	
2	193	-	-	e1	1-8	-	
3	386	-	n	-	1-8	-	
4	579	0	-	-	1-8	-	
5	772	-	m	-	1-8	-	
6	965	-	-	e2	1-7	8	A
7	1158	-	m	-	1-8	-	
8	1351	0	-	-	1-8	-	
9	1544	-	m	-	1-8	-	
10	1737	-	-	e3	1-8	-	
11	1930	-	m	-	1-8	-	
12	2123	1	-	-	1-7	8	B
13	2316	-	m	-	1-8	-	
14	2509	-	-	e4	1-8	-	
15	2702	-	m	-	1-8	-	
16	2895	0	-	-	1-8	-	
17	3088	-	m	-	1-8	-	
18	3231	-	-	e5	1-7	8	C
19	3474	-	m	-	1-8	-	
20	3667	1	-	-	1-8	-	
21	3860	-	m	-	1-8	-	
22	4053	-	-	e6	1-8	-	
23	4246	-	m	-	1-8	-	
24	4439	1	-	-	1-7	8	D

[a]FAS: Frame alinment Signal (...001011...).
[b]DL: 4 kbits/s data link (message bits m).
[c]CRC: CRC-6 block check field (check bits e_1 to e_6).

Tabla 7.3

El formato ESF funciona muy bien para voz pues la pérdida de un bit cada 6 tramas no afecta la calidad de ese servicio,pero para datos ese bit perdido es una falla inaceptable por ello deben utilizarse otros esquemas que,suministrando en las 24 tramas 8 bits para datos,aseguren determinar el comienzo de la trama,la sincronización,y suficientes bits de control,existen varios,uno de ellos multiplexa las señales de llamada y de supervisión en el bit 193 de cada trama,recuerdese que ese bit se ofrece 8000 veces por segundo dandonos un canal de 8Kbps que es suficiente para los fines mencionados**[3],[4].**

Además de T1 existe T1 fraccional(**FT1**) que permite a los usuarios alquilar cualquier número de canales de 64 Kbps entre DS0 y DS1.Sin embargo FT1 tiene características propias pues como no se esta alquilando un T1 completo no se puede fijar la ubicación del otro extremo del circuito.El extremo lejano de una FT1 es un equipo llamado **DACS**(**D**igital **A**ccess **C**ross-Connect **S**witch).

En el sistema europeo(CEPT)el equivalente es **E1** que tiene 32 canales ú octetos, de los que 30 son de información y dos de servicio,el canal 1 se usa para la palabra de alineación de trama ó para alarma,el canal 16 para señalización,cada trama tendrá entonces 256 bits y ocupará 125μseg lo que implica 8000 tramas por segundo,para un total de 2,048 Mbps,este primer nivel trabaja bajo la forma de octetos mientras que el segundo,tercero y cuarto niveles(8.32 y 140 Mbps) se tratan bajo la forma bits**[5],[6].**

7.2.3.-.-Necesidad de sincronización.Deslizamientos.PDH.

Se ha visto que en las jerarquías digitales descriptas(también en la red digital integrada),el bloque constructivo básico es el canal de 64 Kbps.

La estructura de trama del primer nivel jerárquico europeo de 2.048 Mbps se logra mediante la multiplexión **síncrona** de los afluentes ó tributarios de 64 Kbps,esto significa que cada octeto proveniente del respectivo tributario,debe ir exactamente en el espacio de tiempo que se le ha asignado(time slot),que se denomina"**espacio de carga**".Esto a su vez requiere que los 30 relojes de los tributarios de este nivel jerárquico **oscilen exactamente a la misma frecuencia** y ese es el significado de la palabra **sincronismo** aquí.

Sin embargo en este primer nivel jerárquico,y también en los de 8,32,140 y 565 Mbps,como no se ha implementado un mecanismo de sincronización de los relojes, ocurre que a pesar de que nominalmente estos tienen la misma frecuencia,esta y la fase de los diversos relojes es ligeramente diferente,por lo que realidad los tributarios son **asíncronos.**

Debido a ello cuando se construye un nivel jerárquico a partir de los tributarios(**multiplexaje)**las señales de cada uno de estos se almacenan en una memoria llamada:**elástica, tampón** ó **buffer** del tributario respectivo y capaz de almacenar una trama completa. El tributario **escribe** en la memoria **a su velocidad** y la memoria es **leída a la velocidad del reloj del multiplex**,con lo que se logra absorber las variaciones instantáneas de los relojes.

Sin embargo de no desaparecer la diferencia de velocidades de **escritura** (determinada por el reloj del equipo distante),y de **lectura**(determinada por el reloj local)se producirá un **desbordamiento** ó un **vaciado** de la memoria elástica,en el primer caso habrá que descartar octetos y en el segundo se repiten octetos,lo que resulta en **pérdidas** ó **duplicaciones** de fragmentos de información.Cuando esto ocurre decimos que hay **deslizamientos**(**slips**).Estas pérdidas ó repeticiones(slips),ocurren con un período que es calculable,cuya inversa es la "**tasa de deslizamiento**" .

Los deslizamientos son uno de los factores que contribuyen a la degradación de una red digital y ellos afectan en forma diferente los distintos servicios(voz,datos, facsimil,etc),los más perjudicados son aquellos con menor nivel de redundancia (datos,facsimil,etc)donde la pérdida de un octeto es grave,en cambio en voz produce pulsos parásitos("cliks") que molestan poco a menos que sean muy frecuentes.

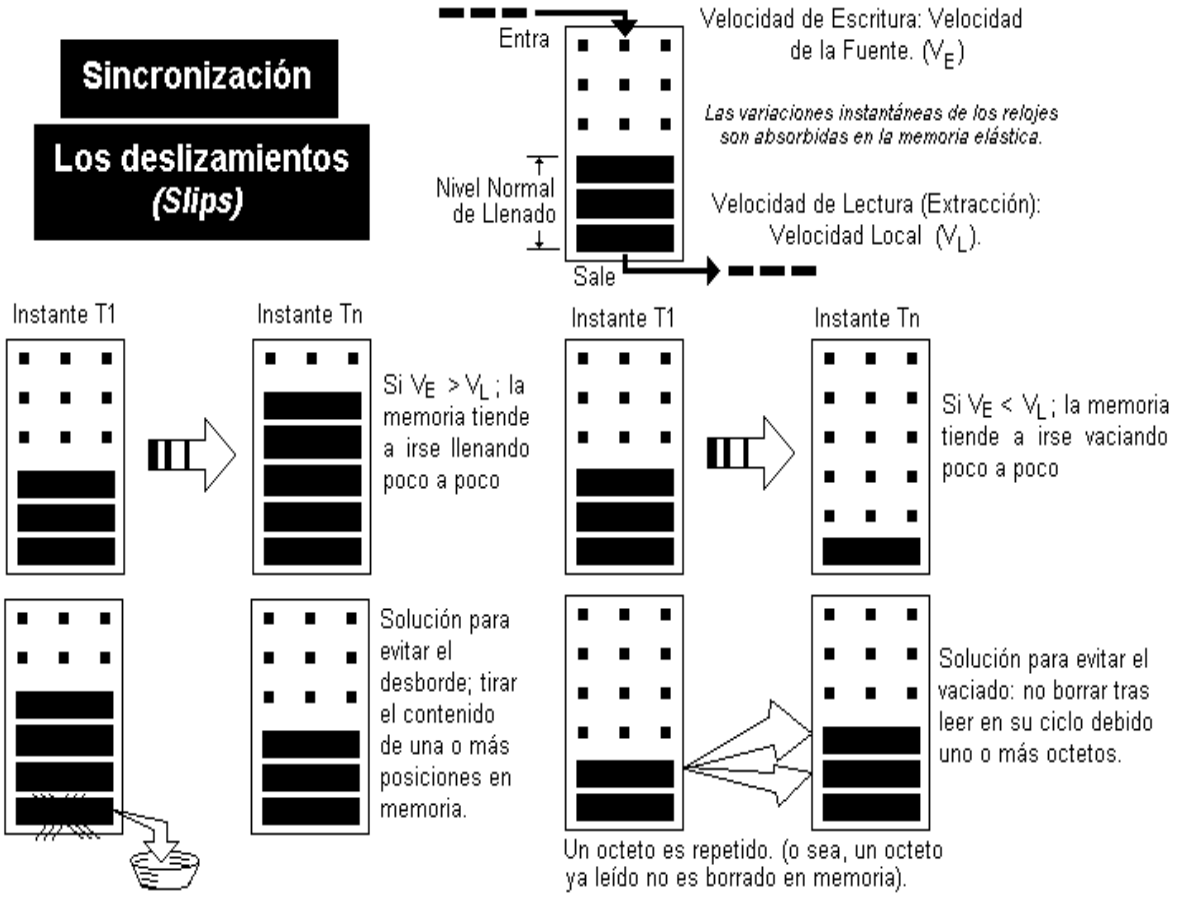


Figura 7.2

Para evitar el deslizamiento se emplea una técnica llamada **justificación**,que consiste en insertar periodicamente un bit que no transporta información en la más rápida de las dos velocidades mencionadas..

Las causas del deslizamiento(slip rate)son varias:

- Diferencia de frecuencia y variación en el tiempo de los propios relojes.
- Variaciones de fase:
  - **Fluctuación de fase(jitter)**
    Se produce a lo largo de todos los elementos constitutivos del sistema de transmisión, especialmente en los regeneradores y multiplex digitales que emplean procesos de justificación.
  - **Fluctuación lenta de fase(wander)**
    Debida principalmente a la variación del tiempo de propagación de la señal digital a través del medio de transmisión,producida generalmente por cambios climáticos(en los medios inalámbricos).
  - **Saltos de fase**
    Son debidos a perturbaciones transitorias,tales como reencaminamientos, cambios automáticos de referencia de sincronización,interferencias,etc.

Para controlar los deslizamientos y no exceder la tasa de deslizamientos que se fija en la red se requiere:

- **limitar las desviaciones de frecuencia entre los relojes de la red**,esto se consigue sincronizando los relojes,lo que se hace por diversos métodos.

- **limitar la fluctuación de fase**,para lo que los equipos de sincronización deben admitir una fluctuación de fase a su entrada que este dentro de los límites máximos especificados por el CCITT(ITU-T). Este fenómeno puede compensarse con la memoria elástica,cuya lectura, para extraer la señal recibida, se retrasa sistemáticamente un tiempo superior al valor máximo esperable de la fluctuación de fase.

Métodos de sincronización

Existen dos soluciones diferentes de red:

Plesíncrona

En la que los relojes de control de las distintas centrales son independientes entre sí.No obstante su exactitud de frecuencia se mantiene dentro de límites estrechos especificados.

Síncrona

En la que los relojes están controlados manteniéndose una frecuencia idéntica,ó la misma frecuencia media,con un desplazamiento de fase relativamente limitado.

Los métodos de sincronización son:

Despóticos:

Maestro-esclavo(director-subordinado).
Maestro-esclavo jerárquico.
Referencia externa

Mutuos:

Sincronización mutua simple.
Sincronización mutua doble.

Se definen entonces como **plesíncronos** todos los nodos de la red que tienen relojes independientes operando nominalmente igual.La precisión y estabilidad de cada reloj es tal que hay una cercana coincidencia en tiempo y fluctuaciones de fase,eliminando en teoría los deslizamientos,ó al menos manteniéndolos dentro de lo tolerable.

Las jerarquías digitales descriptas en la sección 7.2.2 son plesíncronas,o sea PDH, estrictamente estas estructuras jerárquicas son **asíncronas**,sin embargo dado que la variación de cada tributario jerárquico está dentro de una especificación de error determinada,se denominan **plesíncronas**,por lo que entenderemos ambos términos como sinónimos.

Existe una jerarquía digital síncrona ó SDH,diferente de la anterior,y que analizaremos más adelante.

Este SDH está reemplazando a los PDH,como muestra la Figura 7.3

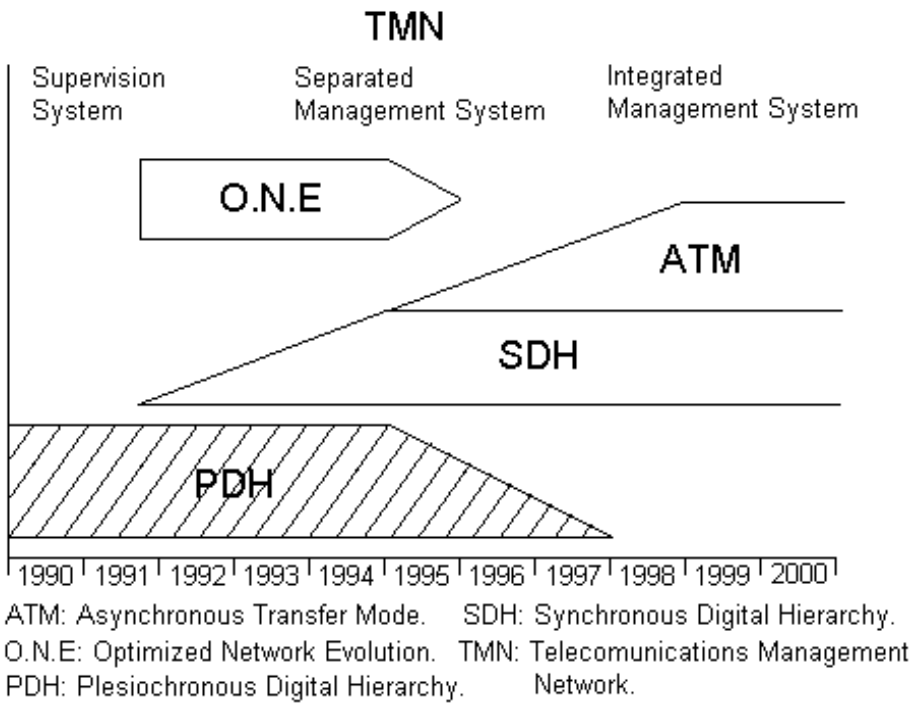


Fig.7.3 Evolución de PDH

7.3.- Conmutación de paquetes.

La conmutación de paquetes, tal como se dijo en el **Capítulo 5**, surge intentando optimizar la utilización de la capacidad de las líneas de transmisión de existentes. Para ello seria necesario disponer de un método de conmutación que proporcionara la capacidad de retransmisión en tiempo real de la conmutación de circuitos y la capacidad de direccionamiento de la conmutación de mensajes.

La conmutación de paquetes se basa en la división de la información que entrega a la red el usuario emisor en **paquetes** del mismo tamaño, que generalmente oscila entre 1000 y 2000 bits.

La técnica de conmutación de paquetes permite dos formas características de funcionamiento: **Circuito Virtual y Datagrama**, en la primera se establece un circuito virtual, esto es un camino entre nodos que siguen todos los paquetes de esa comunicación, y lo hacen por lo tanto en forma secuencial, en cambio en la segunda cada paquete puede seguir un camino distinto(dependiendo de el estado de la red cada nodo toma la decisión de por donde enviar ese paquete específico),por lo que no se asegura el arribo secuencial de los paquetes..

7.3.1.-X.25

X.25 es un estándar del CCIT(ahora ITU-T)de conmutación de paquetes,orientado a conexión mediante circuitos virtuales(ver la norma respectiva o la Referencia **[8]**)y constituye el predecesor de todos los protocolos de transporte WAN.Fue creado con la idea de garantizar un transporte seguro,para ello cada paquete durante su tránsito es almacenado en cada nodo hasta que se recibe una confirmación de correcta recepción del nodo siguiente(acknowledgment),si ocurre un error entre dos nodos el paquete almacenado es retransmitido.

El primer borrador de X.25 apareció en 1974,época en que las líneas eran mucho menos confiables que hoy día,por ello se estableció ese criterio de almacenamiento y envío(store and

forward),que incluye control de flujo,detección y corrección de errores, etc, esto indudablemente hace lenta la comunicación y que los paquetes tengan un enorme over-head.

El estándar de 1974 tenía una velocidad máxima de 64 Kbps, fue revisado en 1976,1978,1980,1984 y en 1985 se emitió el texto "definitivo" de X.25,sin embargo en 1992 IUT lo revisó nuevamente incrementando la velocidad a 2,048 Mbps y la última revisión corresponde 1996 y abarca 157 páginas en la versión castellana, por lo tanto aquí daremos un breve descripción de sus características fundamentales.

X.25 fue promovido por Datapac,Telenet y Tymmet con la idea de crear una red pública de datos con tecnología de conmutación de paquetes, llamada en inglés **PSN**(**P**acket **S**witched **N**etwork),estas redes han sido instaladas en casi todos los países del mundo pero están siendo substituídas por otras tecnologías.

La arquitectura de este protocolo define el **DTE** (**D**ata **T**erminal **E**quipment) siendo este el equipo en el extremo del usuario(terminal ó computador con su tarjeta de X.25),el **DCE**(**D**ata **C**ircuit-terminating **E**quipment)que es el equipo del prestatario del servicio(modems, switches de paquetes y puertos para la PSN,llamado a veces **nodo local ó periférico** y los **PSE** (**P**acket **S**witching **E**xchanges)que son **nodos intermedios**, tal como muestra la **Figura 7.4**

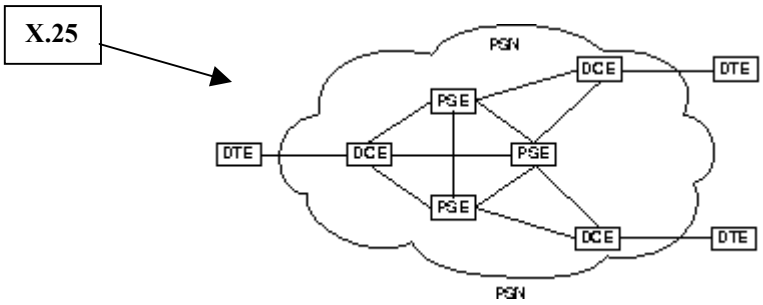


Figura 7.4 Arquitectura de X.25

X.25 especifica dos niveles y una interfaz entre el DTE y el DCE, apareció mucho antes de que ISO finalizara su modelo OSI(ver **Capítulo 4),**de modo que no fue definido según el modelo de 7 capas y el término interfaz aquí tiene un significado diferente, sin embargo puede decirse que hay una correspondencia con las tres capas inferiores de OSI: capas física, de enlace y de red que en X.25 son llamadas, capas **física**, **de acceso al enlace** y **de paquete** tal como muestra la **Figura 7.5.**

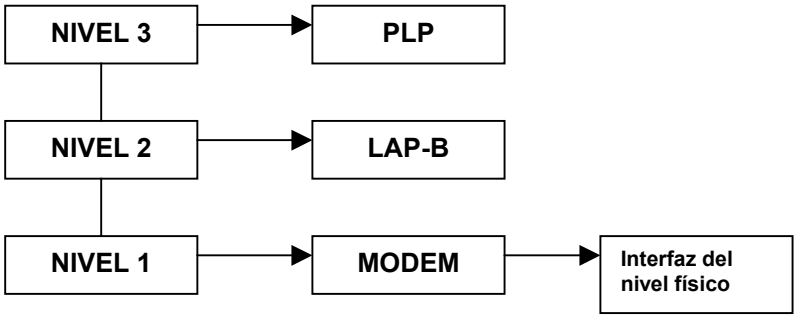


Figura 7.5 Niveles de X.25

El **nivel 1** es la **interfaz física** ó **capa física** y tiene que ver con las señales eléctricas, incluye dos estandares:

- X.21: Se utiliza para el acceso a redes de conmutación digital sincrónicas y es básicamente un conector de 15 pines de las que solo ocho se usan para conectar conductores que interconectan los DTE con los DCE.
- X.21bis:es una norma provisional para ser utilizada en redes analógicas con modems sincronos de la serie V hasta que se tenga acceso fácil a las redes digitales,incluye a RS-232C(conocida en el CCITT como V.24) y al V.35.

El **nivel 2** es el de **acceso al enlace,**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**alanced) que es un protocolo orientado al bit compatible con HDLC,por ejemplo 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,utilizado para establecer conexiones virtuales,manejar control de flujo en una sesión asíncrona balanceada y liberar los circuitos cuando la transmisión se ha completado..

El **nivel 3** es el de **paquete**, **orientado a conexión** y especificado por el **PLP (Packet Layer Protocol**),este es un protocolo de acceso a nivel de red que trata de las conexiones entre un par de DTE, habiendo para ello dos formas de hacerlo, a través de una **llamada virtual(ó circuito virtual)** y de **circuitos virtuales permanentes**. La primera se parece a una llamada telefónica, finalizada esta el circuito se libera, la segunda se asemeja a una línea dedicada que permite la comunicación entre los DTE en cualquier momento que ellos lo deseen. Luego de 1976 las administraciones norteamericana y japonesa a fin de eliminar la sobrecarga de los paquetes de establecimiento y liberación de conexión presionaron para incluir un servicio de **datagramas**, en 1980 el CCITT lo incluyó pero casi nadie lo utilizó y fue eliminado en 1984,sin embargo en otras redes se usa bajo el estándar IEEE 802.

A pesar de ello la demanda de un servicio sin conexión continuó y por ello desde 1984,el nivel 3 de la norma ofrece una facilidad denominada **selección rápida** a fin de satisfacer algunas aplicaciones especializadas como verificación de tarjetas de crédito y transferencia electrónica de fondos,en ellas lo usual es que quien inicia la llamada lo hace por medio de una solicitud,y la parte llamada le dá una respuesta.Cuando se utiliza selección rápida el paquete de **solicitud de llamada** se expande hasta incluir 128 octetos de datos del usuario y el DTE destinatario puede(hay otras opciones) responder con un paquete de **liberación de conexión** con un campo para datos del usuario de hasta 128 octetos.

En la **conmutación de paquetes**,de la que X.25 es un protocolo muy difundido,la información es dividida en muchos **paquetes** pequeños direccionados individualmente,la estación transmisora envía estos paquetes a través de la red de comunicaciones al equipo destinatario,y este rearma el mensaje original.El equipo que divide el mensaje asincrónico, lo direcciona y luego lo rearma se denomina **PAD**(**P**acket **A**ssembler/**D**isassembler),puede ser un equipo contiguo a un terminal (ó incorporado a una PC según el caso) ó un tipo de multiplexor que permite que varias computadoras de una red local unidas a un enrutador,se comuniquen con otras en diferentes redes locales conectadas a la misma PSN,así lo ilustra la **Figura 7.6.**

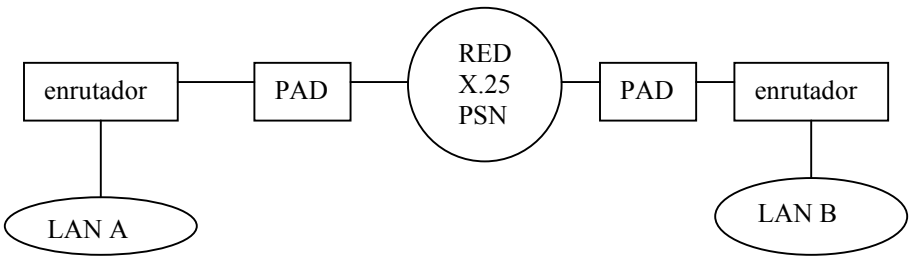


Figura 7.6 Funciones de un PAD

El trabajo de un PAD esta gobernado por tres protocolos adicionales,ellos son:

- X.3,que especifica como un PAD arma y desarma los paquetes.
- X.28,define la interfase entre el DTE y el PAD ó entre dos PAD.
- X.29,define la interfase entre el DCE y el PAD.

Como en todo protocolo orientado al bit la estructura de los paquetes ó tramas es del tipo de la mostrada en la **Figura 7.7**,la única diferencia es la adición de datos de identificación en el encabezamiento del campo de información a fin de permitir convertir este campo en un paquete de datos.

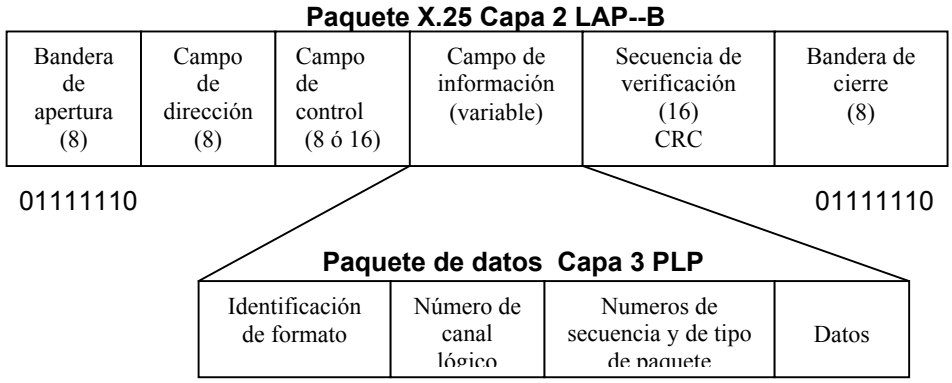


Figura 7.7 Paquete ó trama X.25

El corazón de X.25 es el manejo de los **paquetes de datos**(cuya longitud por defecto es de 128 bytes ó menos,pueden convenirse otras longitudes),la norma define procedimientos para:

- **Control de llamada**(conexión y desconexión de circuitos virtuales).
- **Transferencia de datos.**
- **Control de flujo.**
- **Recuperación desde condiciones anormales.**

7.3.1.1.-Nivel de Enlace(LAP-B).

Cada función que se necesita en la red esta asociada con un **tipo de paquete** y este se identifica con una secuencia única de bits en el **campo de control**,existen tres tipos de tramas:

- **Tramas de información.**

  El campo de control tiene la siguiente forma:

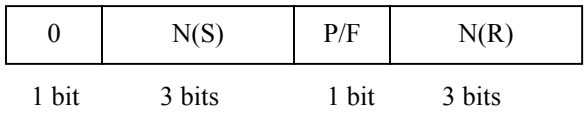


Figura 7.8 Campo de control en una trama de información

- El primer bit es un 0
- Los tres bits siguientes son el número de secuencia de la trama de información respectiva.
- P/F es el bit Poll/Final de los protocolos HDLC.
- Los últimos tres bits son una secuencia de asentimiento.Se utiliza **piggybacking**, esto significa que se aprovechan las tramas de información para mandar asentimientos. Si un 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 en otras ocasiones se representa con I2 y ACK3, es decir, envía la trama 2 y advierte de que recibió correctamente 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 asentimiento, tiempo que transcurre desde que se envía el último bit de una trama hasta que se recibe su asentimiento, es muy alto, puede interesar aumentar la numeración para poder mandar más tramas en dicho tiempo de asentimiento. Este es el motivo por el que se permite utilizar numeración extendida a módulo 127 (7 bits).

♦ **Tramas de supervisión.**

El campo de control tiene la siguiente forma:

1	0	Tipo	P/F	N(R)
1 bit	1 bit	2 bits	1 bit	3 bits

Figura 7.9 Campo de control en una trama de supervisión

Si se utiliza numeración extendida el campo de control de 16 bits será así:

1	0	Tipo	X	X	X	X	P/F	N(R)
		2 bits						7 bits

Figura 7.10 Campo de control con numeración extendida.

Los tipos son:

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 al 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.

- **Tramas no numeradas.**

El campo de control es:

1	1	Tipo	P/F	Tipo
1 bit	1 bit	2 bits	1 bit	3 bits

Figura 7.11.Campo de control en tramas no numeradas

Algunos tipos utilizados son:

- **SABM** (*S*et *A*syncronous *B*alance *M*ode): Sirve para configurar el receptor y el emisor.
- **UA** (*U*nnumbered *A*CK): Confirma tramas no numeradas que funcionan en modo parada y espera.
- **DISC**: Se utiliza para desconectar.
- **SABME**: Se configuran emisor y receptor acordando utilizar numeración extendida.
- **RESET**: Ante situaciones irrecuperables se pone todo a cero y se informa al nivel superior de que ha habido un fallo grave.

Veamos como es que se maneja la comunicación en este **nivel de enlace ó de acceso al enlace**,que denominamos **nivel 2**,y que se ocupa de lo que ocurre entre un DTE y su DCE vecino(recordemos que el nivel de enlace es solo para equipos contiguos).Para ello consideremos lo que muestra la **Figura 7.12**.

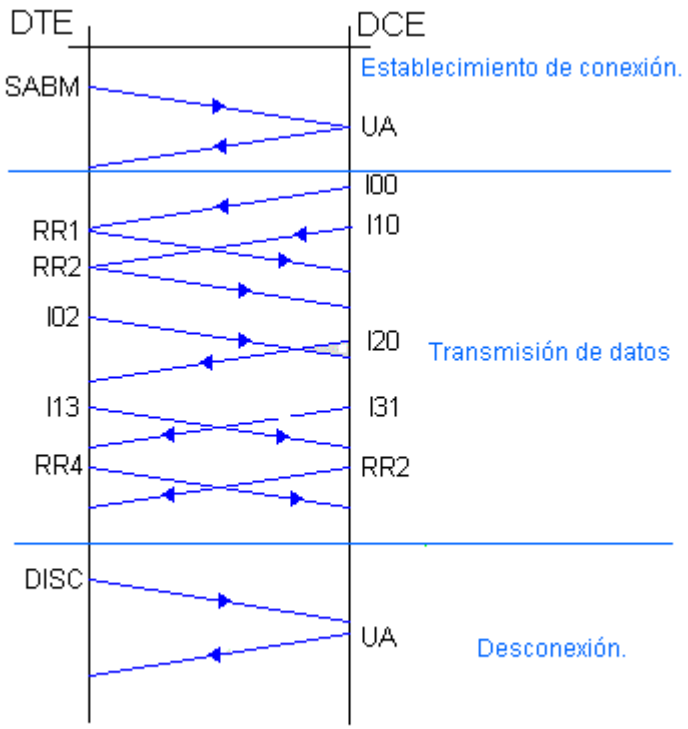


Figura 7.12.Secuencia en el nivel de enlace con LAP-B

Establecimiento de conexión:

En esta fase, DTE pide que se abra una comunicación con la trama SABM,como ya sabemos el receptor será siempre un DCE puesto que estamos en el nivel de enlace.Con la trama citada, el DTE consigue informar al DCE de qué 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 7.12**, se trabaja en modo pare y espere.

Fase de transmisión de datos:

Establecida la conexión,y alguno de sus parámetros,ya se puede mandar información.En el caso de la **Figura 7.12**,es el DCE quien envía una trama,esta es I00 lo que significa:se está enviando la trama 0 y se espera 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,y aclaremos que no se asiente una trama con su número sino con el número de la trama siguiente a la que se confirma,por ello 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,en este caso el DTE,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. Son:

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 del que hemos venido hablando hasta ahora.

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 comprobar el enlace para comprobar una posible falla 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 ó se desconecta informando al nivel superior.

K o Tamaño de Ventana.

7.3.1.2.-Nivel de paquete(X.25) ó Nivel de red(OSI).

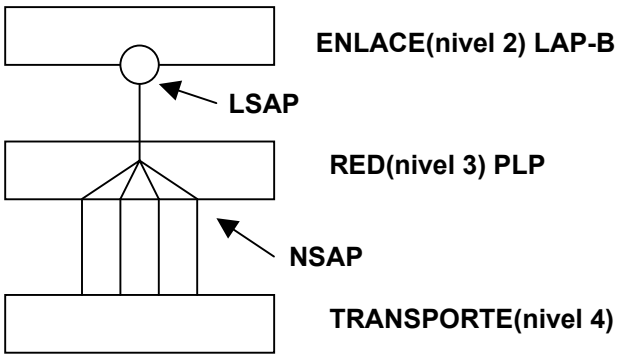
Ya se mencionó que nivel está especificado por el **PLP (Packet Layer Protocol)** que es un protocolo de acceso a nivel de red y proporciona un servicio de la siguientes caraterísticas al nivel superior:

- 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 DTEs multiplexados.

Recordemos los **circuitos virtuales(CV)**,en X.25 son de dos tipos:

- **Conmutados(CVC)**,que requieren de un diálogo previo con el nodo local para establecerlos.
- **Permanentes(PVC)**,están contratados previamente,de modo que no es necesaria la fase de establecimiento.Se utilizan cuando se transmite frecuentemente y en grandes volúmenes de información a un mismo destino.

Dentro de cada DTE los CVCs son identificados por un **número de canal lógico(NCL)** que se negocia en la fase de establecimiento,es posible tener varios CV(hasta 4095) establecidos en la misma máquina,obviamente cada uno con su NCL,veamos con un poco más de detalle esto de varios canales ó multiplexión.



.**Figura 7.13.Los CVs y la multiplexión con términos OSI.**

En la **Figura 7.13** se muestra como la multiplexión que se ofrece es al **nivel de transporte**, no es tal a nivel de enlace: en LAPB sólo hay una conexión.

La multiplexión se resuelve a nivel de red, aunando las diferentes conexiones (asimilables a CVs) que aparecen en el *NSAP* (Punto de Acceso al Servicio a Nivel de Red), en una sola desde el nivel de enlace en el *LSAP*.

Veamos como funcionan las cosas en el **nivel 3 ó de red**,con relación a la **Figura 7.14** tenemos:

- **Fase de Establecimiento:** Hemos supuesto que la llamada es aceptada, pero como veremos más adelante, podría ser rechazada. Esta fase sólo tiene lugar para CVCs.

  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').

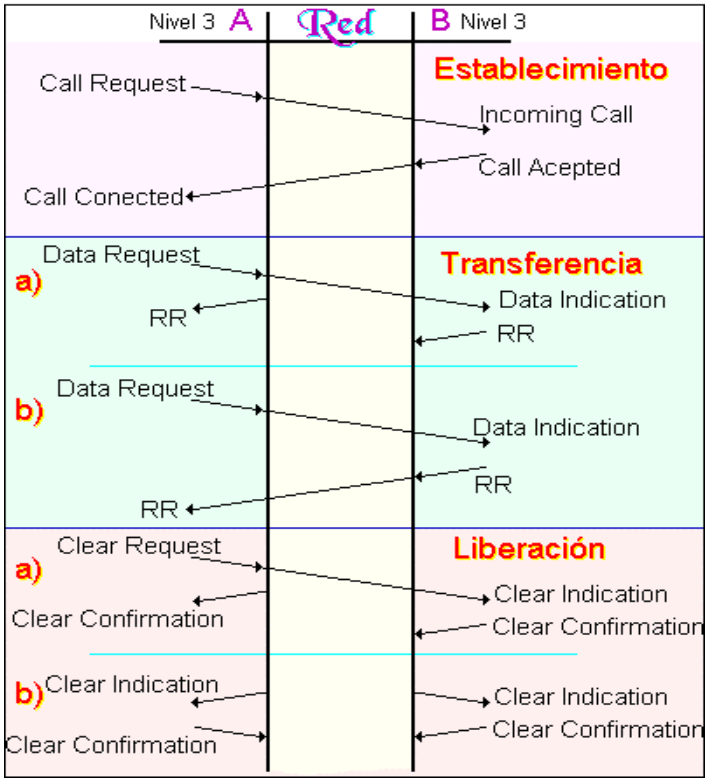


Figura 7.14.Fases de la transmisión a nivel 3

Observese que los dialogos son entre dos PLP,el nivel de enlace solo sirve de transporte.

Las direcciones a nivel de enlace son distintas de las de nivel de red. Con la dirección de enlace (que ya vimos que no se necesitaba realmente) llego al primer nodo. Allí se desencapsula y se usa la de red para llegar a los demás.

A nivel de paquete no tenemos retransmisiones. Sí hay control (detección) de errores, pero no corrección.

Adicionalmente existen otros protocolos que completan el X.25:

7.3.1.3.-Direcciones en X.25.

Las direcciones en X.25 vienen dadas por la norma X.121 que reserva 14 bits para ello,la **Figura 7.15** muestra este campo.

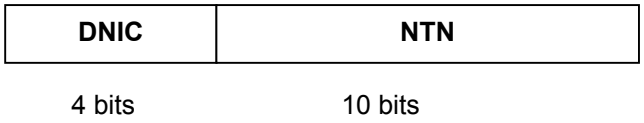


Figura 7.15.Campo de direcciones de 14 bits

- **DNIC** (*Data Network Identifier Code*): Identifica a cada red X.25 y distingue al operador público (Iberpac tiene uno, Transpac (Francia) otro, etc.). Es único a nivel mundial.
- **NTN** (*Network Terminal Number*): Número de abonado. En España está limitado a 9 dígitos.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 (España p.ej.) lo cual da lugar a medio octeto sobrante y que probablemente habrá que usar un relleno (*pading*).
- **Utilización:**
  - Usar siempre el DNIC, incluso si llamo a mi propia red. (es como si telefoneo Valencia-Valencia y siempre pongo el prefijo 041 delante).
  - No usar el DNIC internamente y usar para llamadas externas **0+DNIC+NTN** (esto es lo que se utiliza en redes como Iberpac).

7.3.1.4 Número de canal lógico (NCL).

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 (Telefónica, etc.). Cuanto mayor es el NCL, tendremos mayor número de CVs establecibles. Un NCL se especifica con 12bits, lo cual da lugar a que puedan usarse como máximo 4095 NCLs (el 0 tiene un significado especial).

Utilización:

Los NCLs se escogen por el DTE o por el DCE (la escogencia es entonces de la red) cuando se necesitan, liberándolos cuando los acaban de usar. Ambos tienen una lista donde se estan los NCLs libres y ocupados (lo que se registra en una lista se refleja inmediatamente en la otra).

- El DTE empieza a escoger por los NCLs de mayor numeración.
- El DCE (la red) empieza por los de menor numeración.
- Podría ocurrir que se juntasen *en el centro* (los DTE vienen de arriba y los DCE de abajo) y esto desemboca en varias posibilidades:

  1. 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.

2. Que sólo quede un NCL por elegir y los dos lo cojan 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.

7.3.1.5.-Interconexión de redes X.25.

Para tener WANs verdaderas tiene que ser posible interconectar redes X.25,el CCITT desarrollo un protocolo interredes conocido como X.75,esta es la norma para especificar terminales,procedimientos de control de llamadas y transferencia de datos en circuitos internacionales de PSN.

X.75 tiene los mismos tres niveles de X.25:físico,enlace y paquete.Los puertos de salida ó gateways se denominan **STE**(**S**ignal **T**erminal **E**xchanges).A nivel físico X.75 es casi igual a X.25,la mayor diferencia es que soporta el establecimiento de **multienlaces.**significa que se crea la impresión de mayor ancho de banda utilizando operaciones simultáneas con enlaces de datos en paralelo a lo largo de la misma ruta,obviamente tendremos mayor velocidad que en los de enlace único.La **Figura 7.16** ilustra estas características.

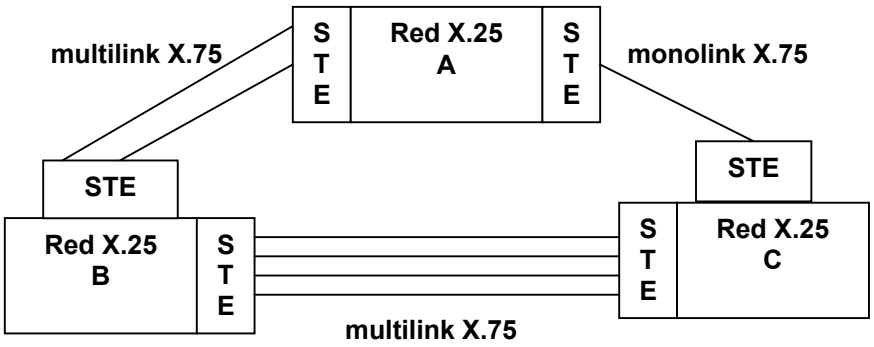


Figura 7.16. Multilinks X.75

X.75 además define ciertas condiciones adicionales bajo las cuales un paquete es rechazado como si fuese erróneo.

7.3.2.-TCP/IP y Netware(IPX).

7.3.2.1.-TCP/IP.

7.3.2.1.1.-Conceptos generales de TCP/IP.

TCP/IP se originó en 1969**[10][11]**con un proyecto de investigación financiado por la agencia **ARPA**(**A**dvanced **R**esearch **P**rojects **A**gency) de los Estados Unidos que tenía el propósito de establecer un red de conmutación de paquetes entre diversas Instituciones de Investigación mediante satélites y radio. Esto se hizo con el fin investigar cómo construir redes que pudieran soportar fallas parciales (como las producidas por bombardeos, recuérdese que era el apogeo de la Guerra Fría)y aún así seguir funcionando.

En el modelo DARPA(ARPA se transformó en DARPA donde la **D** es por **D**efense) desarrollado por los investigadores de Stanford University,Bolt, Beranek y Newman(BBN) se crearon una serie de protocolos de comunicaciones que utilizaban UNIX 4.2 de la Universidad de California, Berkeley, sistema operativo de gran popularidad en la Universidades y de dominio público(como es **LINUX** hoy día),el trabajo completado a fines de los 70 dio lugar al Grupo de Protocolos de Internet(Internet Protocols Suite).

En DARPA la comunicación ocurre siempre entre una computadora fuente y una de destino, la red asume por sí misma que pueden, y ocurrirán, fallas por las que cualquier parte de la red puede desaparecer. Para solventar este problema la red fue diseñada de modo que una computadora que desea enviar un mensaje, solo tiene que ponerlo en un sobre, llamado paquete de protocolo Internet(IP, Internet Protocol)y le asigna el domicilio de destino, el paquete viaja por el mejor camino que se encuentra hasta ser entregado,

La red se llamó **ARPANET** y los académicos e investigadores que tenían acceso a ella se volvieron adictos, por eso la demanda por la red creció enormemente, además dado el éxito de ARPANET comenzaron a instalarse otras redes: CSNET, BITNET,etc.

En 1983 ARPANET fue dividida en **MILNET**(para uso militar) y **ARPANET**(para uso civil), esto dio lugar a **Internet,** cuyo desarrollo fue impulsado también porque la U.S. Defense Communications Agency(DCA) hizo obligatorio el uso de TCP/IP en todas las máquinas de ARPANET y lo hizo modificando el software de conmutación de paquetes. Nuevos troncales fueron instalados para satisfacer la demanda de MILNET y ARPANET, en 1986 la **NSF**(**N**ational **S**cience **F**oundation) comenzó a dar servicio de Internet conectado centros de supercomputación de varias Universidades, otros troncales de Estados Unidos, y de otros países, comenzaron a conectarse y el desarrollo de Internet ha sido asombroso.

Los motivos de la popularidad de TCP/IP pueden resumirse así:

- Independencia del fabricante
- Soporta múltiples tecnologías
- Puede funcionar en máquinas de todo tamaño (multiplataforma)
- Estándar en EE.UU. desde 1983
- Su destino está ligado a la INTERNET

Para explicar los aspectos fundamentales(hay textos enteros dedicados a este grupo de protocolos **[10],[11],[12]**) de TCP/IP comenzaremos por hacer notar que TCP/IP es básicamente un **grupo de protocolos**(reglas y estándares) **de interconexión de redes**, y los dos fundamentales, en realidad hay muchos más, le dan nombre:

- **TCP**(**T**ransport **C**ontrol **P**rotocol),es un protocolo orientado a conexión responsable de proveer una comunicación confiable y recuperable entre dos puntos extremos.
- **IP**(**I**nternet **P**rotocol),que maneja la parte de enrutamiento y envío de los mensajes TCP.

En la arquitectura de Internet dos ó más redes se interconectan con **routers** ó **ruteadores** ó **enrutadores**(ver **Sección 2.10.8**).Cada red está compuesta de una ó más **máquinas ó computadoras de extremo(end systems)** donde está el usuario que desea conectarse con otro de otra red(ó de la misma, este caso es el más simple),esto es esquematizado en la **Figura 7.17**,en la que se muestra en la parte inferior el detalle interno de solo una red, las demás pueden ser de del mismo ó de cualquier otro tipo: token-ring, ethernet, X.25,etc y donde **me** significa **máquina de extremo**.

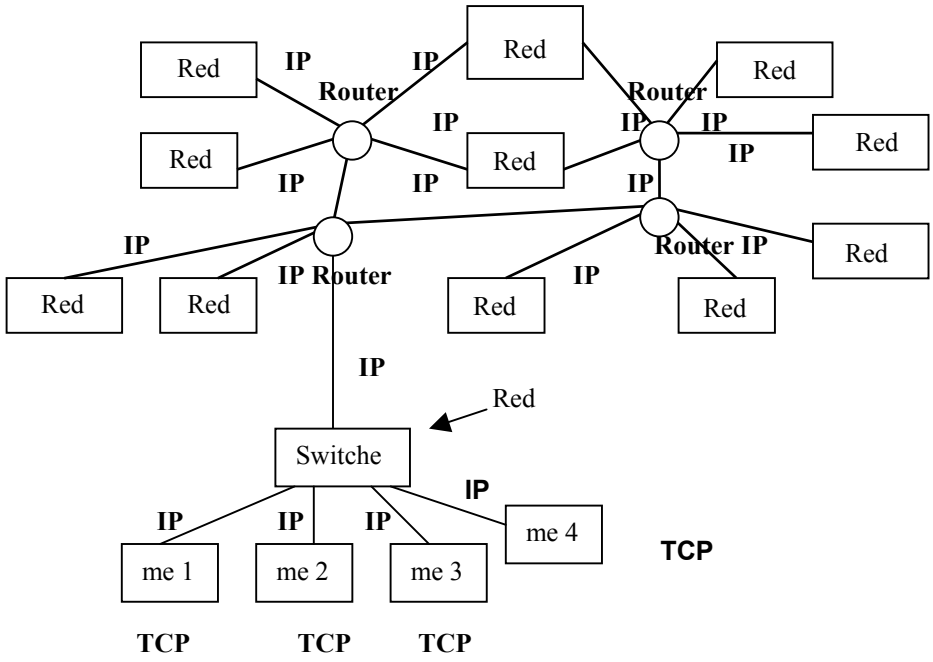


Figura 7.17.Interconexión de redes

TCP reside en las máquinas extremo pues es un **protocolo extremo a extremo,** que define las reglas y procedimientos para el intercambio **seguro** de información entre interlocutores en máquinas de destino, lo de seguro significa se encarga que todos los datos **sean recibidos** y **ordenados adecuadamente**.

IP establece las reglas y procedimientos que aseguran que los datos puedan ser enviados entre redes, y por lo tanto es responsable del enrutamiento, llevando a los routers la información que necesitan para tomar decisiones de enrutamiento.

IP provee envío de datos extremo a extremo **sin conexión** y en base al criterio de **mejor esfuerzo**, esto quiere decir que IP no establece una conexión lógica entre dos máquinas de extremo que se conectan, en cambio esta capa simplemente conduce los paquetes individuales, llamados **datagramas IP**, a través de la internet, y son los **enrutadores IP** los responsables de enrutar estos datagramas.

Cada enrutador mantiene **tablas de enrutamiento** que describen como pueden ser alcanzadas otras redes, estas tablas contienen información que describe **el próximo salto**, que llevará el datagrama IP a su destino, ningún enrutador conoce la ruta completa.

Se dijo también que IP hace el **mejor esfuerzo**, y ello significa que IP **no asegura** la entrega, pues prácticamente no tiene detección y corrección de errores. Si por alguna razón (congestión o falta de ruta a la red destino)el datagrama es descartado, IP **no notifica** al usuario lo ocurrido. Además cada datagrama IP tiene el número total de enrutadores que tocará antes de ser descartado, esto evita datagramas errantes.

Si el usuario requiere una entrega **segura** usa **TCP**, este protocolo asegura secuencia correcta, que no falten trozos del mensaje, y que no haya duplicaciones. Para ello cuando una máquina de extremo desea enviar un paquete le pone un **encabezado** compuesto por una serie de bits adicionales(que serán descriptos más adelante) que incluyen un número de secuencia, creando algo llamado **segmento TCP,** estos datos son colocados en un **sobre IP**, que también consiste en agregar una serie de bits (entre ellos la dirección de origen y la de destino) y que da lugar al ya mencionado **datagrama IP.**

A **IP** no le interesa lo que va dentro del sobre, solo le se ocupa de la dirección en su encabezamiento ya que en una red de redes TCP/IP, las computadoras llamadas **enrutadores** ó **ruteadores** ó **routers**(algunos autores aún las denominan gateways) proporcionan las interconexiones entre las redes físicas y para ello **utilizan la dirección de la red de destino** y no la de la **máquina de extremo** destinataria, en consecuencia la cantidad de información que debe guardar un enrutador es proporcional al número de redes dentro de la Internet y no al número de computadores. De esto se deduce que como operan y enrutan esos enrutadores, así como un sistema eficiente de direcciones, son temas de gran importancia.

Los protocolos de enrutamiento de IP son **dinámicos**, lo que significa que las rutas son calculadas a intervalos regulares por el software de los enrutadores, esto contrasta con el enrutamiento estático cuyas rutas son establecidas por el administrador y sólo él puede cambiarlas. Una tabla IP de enrutamiento consiste de pares **dirección de destino/próximo salto**, así por ejemplo 34.1.0.0/54.34.23.12 significa para llegar a la red 34 subred 1 el salto debe ir al nodo 54.34.23.12(lo de las subredes se aclara dentro de poco).

El protocolo **TCP** de la máquina de extremo destinataria abre el sobre IP, organiza los datos según el número de secuencia detectando faltantes y duplicaciones, si todo llegó correctamente notifica la máquina de extremo que lo envió que todo está bien, si ésta al cabo de cierto tiempo no tiene ese OK retransmite los datos.

Como se señaló en la **Sección 4.10**,TCP/IP es un **protocolo de red**, y se ocupa desde capa 3 hasta la de Aplicación, recordemos que el modelo de capas de TCP/IP es diferente de el de OSI, aunque pueden establecerse paralelos, tal como ilustra la **Figura 7.18**.

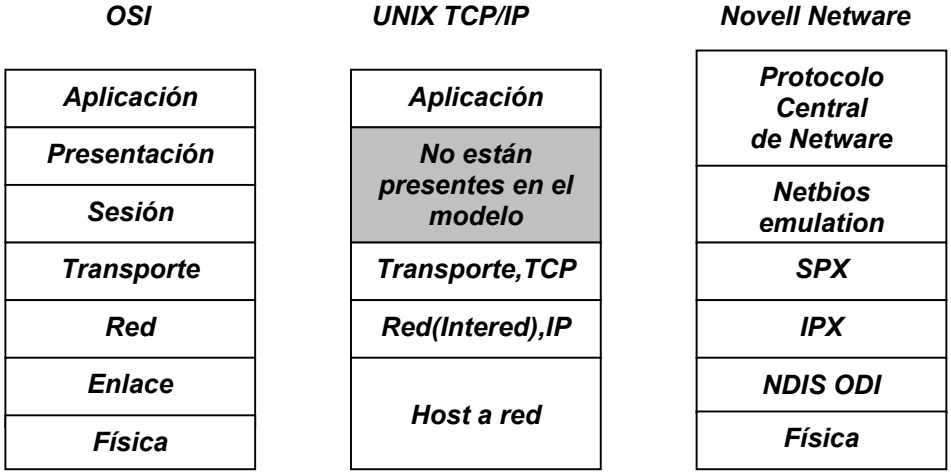


Figura 7.18. Correspondencia entre capas del modelo OSI, TCP/IP y Netware

Muchas redes usan sus propios protocolos, que denominamos en el Capítulo 4 **protocolos de acceso**, tales como Ethernet, Token-Ring, etc.,que corresponden a las capas 1 y 2,TCP/IP provee mecanismos para que esas máquinas de destino de redes diversas se comuniquen **sin que tengan que cambiar** sus propios protocolos.

Para ello la máquina de extremo **encapsula** el **datagrama IP** en una **trama**, por ejemplo **Ethernet**, el enrutador al recibirla y determinar que está destinada a él, elimina el encapsulado y envía el **datagrama IP** al próximo salto.

Cuando el datagrama llega a la red de destino, el enrutador determina la dirección local de la máquina de extremo destinataria y utilizará el protocolo de esa red, **encapsulándolo,** para entregar el **datagrama IP**.

Como cada red tiene diferentes limitaciones y dimensiones de paquetes(Ethernet 1500 bytes, X.25 128 bytes, etc)los enrutadores **fragmentan** y **rearman** los datagramas según sea necesario.

TCP/IP también puede usarse para redes locales(LANs) solo que en ellas no es necesario IP, a menos que tenga un enrutador, sin embargo por previsión es prudente usar también IP pues deja todo preparado para la interconexión con otras redes.

Los **protocolos de este grupo TCP/IP** son varios que pueden agruparse en:

- **Servicios ó Protocolos Interred:**

  IP(**I**nternet **P**rotocol)
  ARP(**A**ddress **R**esolution **P**rotocol)
  RARP (**R**everse **A**ddress **R**esolution **P**rotocol)
  ICMP(**I**nternet **C**ontrol **M**essage **Pr**otocol)

- **Servicios ó Protocolos de Transporte:**

  TCP(**T**ransport **C**ontrol **P**rotocol)
  UDP(**U**ser **D**atagram **P**rotocol)

- **Servicios ó Protocolos de Aplicación:**

  TELNET
  FTP(**F**ile **T**ransfer **P**rotocol)
  SMTP(**S**imple **M**ail **T**ransfer **P**rotocol)
  NNTP(**N**etwork **N**ews **T**ransfer **P**rotocol)
  CMOT(CMip/cmis **O**ver **T**cp (Common Management Information Services/ Common Management Information Protocol)
  DNS(Domain **N**ame **S**ystem)
  SNMP(**S**imple **N**etwork **M**anagement **P**rotocol)
  TFTP(**T**rivial **F**ile **T**ransfer **P**rotocol)
  BOOTP(**BOOT**strap **P**rotocol)
  NFS(**N**etwork **F**ile **S**ystem)
  XDR(e**X**ternal **D**ata **R**epresentation)
  RPC(**R**emote **P**rocedure **C**all)

Este estándar es mantenido por el **IAB**(**I**nternational **A**ctivities **B**oard) a través de la **IETF**(**I**nternet **E**ngineering **T**ask **F**orce).Pueden obtenerse estos estándares en línea mediante los **RFC**(**R**equest **F**or **C**omments Documents),así por ejemplo **IP** es definido por RFC 791 y **TCP** por RFC 793,ver también la Referencia **[10]** Apéndice 1,puede hacerse ftp://ds.internic.net usuario anonymous y clave de acceso guest.

7.3.2.1.2.-Servicios ó Protocolos Interred:

IP(Internet Protocol)

7.3.2.1.2.1.-Direcciones IP

En este esquema la **dirección** de cada computador, es **única** y está compuesta de 4 bytes(32 bits) llamados **dirección IP**. Normalmente se representa como ***w.x.y.z*** donde ***w,x,y,*** y ***z*** son reemplazados por un número decimal entre 0(Hex 00) y 255 (hex FF),por ejemplo 150.186.32.90 es una dirección válida, esos cuatro decimales se dividen en dos partes(no necesariamente de la misma longitud),una identifica la red y la otra el nodo, ó equipo terminal(end system)dentro de la red.

Hay varias formas de dividir estos 32 bits, cada una da lugar a una **clase**, y existen cinco clases, de las que las tres primeras son las más importantes:

- **Clase A**, utilizadas para las pocas redes muy grandes que tienen más de 2^{16} (65.536) equipos terminales, se asignan 7 bits para identificar la red y 24 bits para identificar a los equipos terminales, el bit restante es un 0 que encabeza la dirección, ver **Figura 7.19**.

- **Clase B**, utilizadas para las redes medianas que tienen entre 2^8 (256) y 2^{16} (65.536) equipos terminales, se asignan 14 bits para identificar la red y 16 bits para identificar a los equipos terminales, los dos bits faltantes son un 1 y un 0 (10) que encabezan la dirección, ver **Figura 7.19**.

- **Clase C**, utilizadas para redes pequeñas que tienen hasta 2^8 (256) equipos terminales, se asignan 21 bits para identificar la red y 8 bits para identificar a los equipos terminales, los tres bits faltantes son 110 que encabezan la dirección, ver **Figura 7.19**.

- **Clase D**, reservada para multidifusión está encabezada por cuatro bits 1110.

- **Clase E**, reservada para uso posterior, es encabezada por cinco bits 11110

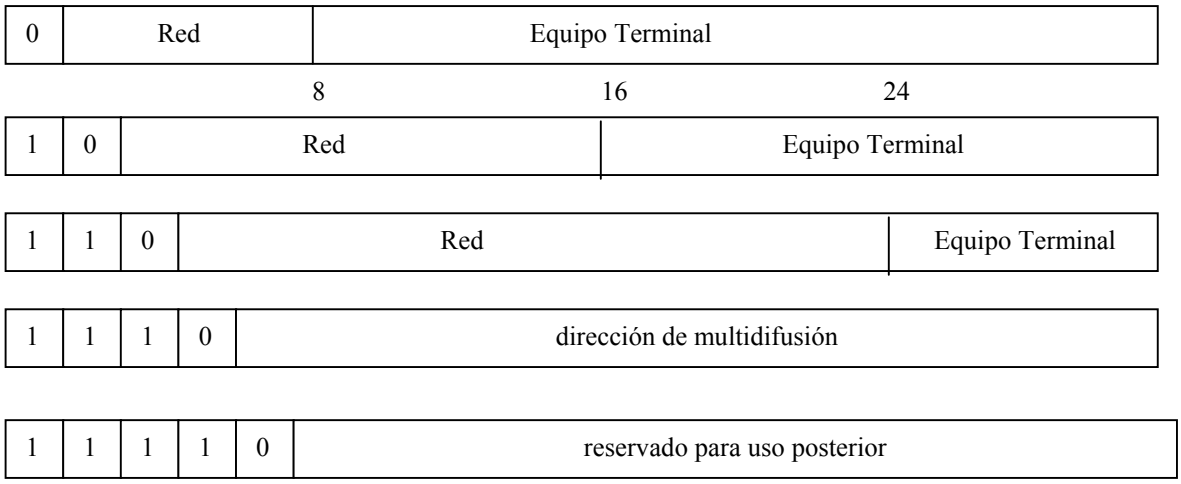


Figura 7.19.Clases de direcciones en IP.

Obsérvese que aún cuando cada equipo de extremo tiene un número(en realidad cuatro números de 8 bits cada uno **w,x,y,**y **z**) esto no es totalmente cierto, el número corresponde a **la conexión a la red**, del mismo modo que un número telefónico no corresponde al aparato sino al punto de conexión(SAP en la nomenclatura OSI),de manera que si el equipo terminal se mueve de una red a otra su número cambia.

Cuando se comunican a los usuarios, las direcciones IP no se dan como secuencia de bits sino como **cuatro enteros decimales separados por puntos**, donde cada entero corresponde al valor del octeto respectivo, así:

10010110 10111010 00100010 01011010

corresponde a una dirección **Clase B**, que en decimal se leerá como:

150.186.34.90

La siguiente lista identifica los rangos en valores decimales:

	Dirección más baja	Dirección más alta	Número Máximo de redes	Máximo de terminales
Clase A	0 . 1 . 0 . 0	126. 0 . 0 . 0	126	16.777.124
Clase B	128 . 0 . 0 . 0	191. 255 . 0 . 0	16.384	65.534
Clase C	192 . 0 . 1 . 0	223 . 255 . 255 . 0	2.097.152	254
Clase D	224 . 0 . 0 . 0	239 . 255 . 255 . 255		
Clase E	240 . 0 . 0 . 0	247 . 255 . 255 . 255		

7.3.2.1.2.2.-Direcciones especiales.

Dentro de los lineamientos señalados hay varias condiciones especiales que requieren de reglas y/o direcciones especiales, veamos:

- ✓ Las direcciones IP pueden referirse **tanto** a redes(muchas máquinas) como a máquinas de extremo(individuales),por ello **nunca se asigna al campo de una maquina de extremo el valor 0**,en cambio cuando una dirección IP tiene 0 en el campo de máquina extremo se refiere a **la red en sí misma,** por ejemplo la red clase B de la UC se identifica con 150.186.0.0 y la subred de Ingeniería Eléctrica será 150.186.34.0
- ✓ Las direcciones IP de cualquier campo de máquina extremo consistente en todos 1s es una **dirección de difusión**. Esta difusión se llama **dirigida** debido a que tiene una dirección válida de red y un campo de máquina extremo de difusión, así la dirección de difusión de la red 150.186 será 150.186.255.255
- ✓ Existe la **difusión limitada ó difusión de red local** que consiste en 32 bits iguales a 1 que corresponden a 255.255.255.255,obsérvese que esta dirección fue excluida más arriba y no es válida, se usa para dirigirse a todas las máquinas extremo de la red en que se esta produciendo el paquete. Esta dirección puede ser utilizada como parte de un protocolo de arranque antes de conocer su dirección IP, ó la dirección IP de la red local.
- ✓ La dirección 127.0.0.0 se reserva para **loopback** y es utilizada para pruebas de TCP/IP y comunicación entre procesos en la **máquina local**. O sea que si un programa utiliza esa dirección, el software de la red entiende que ese paquete está dirigido a un proceso que se está ejecutando, ó se va a ejecutar, en la misma máquina, y por lo tanto lo pasa internamente a ese proceso. En realidad cualquier dirección encabezada por 127 se considera de **loopback**.

Las direcciones IP oficiales son otorgadas por InterNIC cuyo teléfono es 1-800-444-4345, el texto *TPCP/IP Network Administration de O´Reilly & Associates* dá más detalles al respecto.

7.3.2.1.2.3.- Subredes y máscaras.

El esquema original de direccionamiento IP descripto no tuvo en cuenta el explosivo crecimiento de Internet y los inconvenientes(trabajo administrativo excesivo, tablas de ruteo muy grandes y agotamiento de direcciones)que ello producía. Esto será radicalmente resuelto por Ipv6(IP versión 6), pero mientras tanto se han adoptado soluciones para hacer manejable el problema. Hay tres esquemas:

- Uso de enrutadores transparentes.
- Uso del protocolo Proxy ARP.
- Direccionamiento de subredes.

Aquí nos ocuparemos sólo de este último dado que es el más utilizado, al punto que puede ser considerado estándar en Internet, para los demás ver las Referencias **[10] y [11].**

El **direccionamiento de subredes, enrutamiento de subred ó utilización de subredes** tiene como propósito evitar que el número de redes físicas manejadas por los enrutadores crezca desmesuradamente, además permite organizar las direcciones IP en concordancia con las subredes físicas y/o lógicas. El esquema puede ser implementado totalmente con software en los enrutadores y representa un cambio de detalle en el esquema original de direcciones y es parte obligatoria del direccionamiento IP vigente y descripto con relación a la **Figura 7.19.**

Lo que se hace es cambiar la forma de interpretar los 32 bits que corresponden a la dirección IP, recuérdese que ésta está dividida en dos partes una que corresponde a la red y la otra a la máquina de extremo. En el **direccionamiento de subredes** la parte de la dirección correspondiente a la red no se toca y ello hace a este esquema compatible con el original, sin embargo la parte correspondiente a la máquina de extremo será **reinterpretada localmente** de manera que, una parte identifique una subred física, y la otra a las máquinas de extremo dentro de esas diferentes subredes físicas.

Imaginemos que una localidad tiene asignada una grupo de dirección tipo B, pero que tiene **muchas** subredes físicas(la **Figura 7.20a** muestra dos). **Solo el enrutador local sabe** que existen varias redes físicas **y**, a diferencia de los enrutadores de sistemas autónomos ó sin subredes, **sabe** como enrutar el tráfico entre ellas.

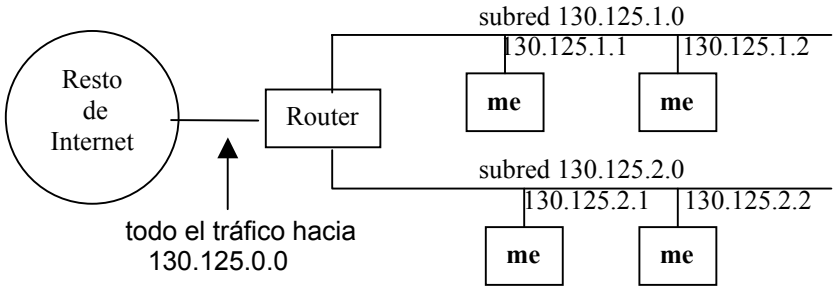


Figura 7.20a.Localidad con dos redes físicas que utilizan direccionamiento de subred.

En este ejemplo la localidad sólo utiliza la dirección tipo B 130.125.0.0 para referirse a **todas** las subredes. Todos los enrutadores de Internet, a **excepción del enrutador local**, la enrutan como si fuese una sola red física la 130.125.0.0, cuando el paquete llega a R, éste debe enviarlo a destino a través de la subred física correspondiente. El administrador asigna a cada máquina de extremo de la primer subred una dirección de la forma 130.125.1.X, a cada máquina de extremo de la segunda subred una dirección de la forma 130.125.2.X, y así sucesivamente, el enrutador R hace su trabajo examinando el tercer octeto de la dirección de destino.

Este es un **direccionamiento jerárquico** similar a los códigos de área del sistema telefónico y tiene la ventaja de que puede incorporar un gran crecimiento pues una ruta no necesita saber muchos detalles sobre destinos distantes.

La asignación de direcciones es muy flexible pues no necesariamente la división en dirección de subred y de máquina terminal debe ser a partes iguales. Si, en una dirección tipo B, dividimos la parte local igualitariamente podemos tener 256 subredes con 256 máquinas de extremo cada una[2],si en cambio utilizamos 3 bits para identificar la subred y 13 para identificar las máquinas de extremo tendremos 8 subredes con 8192 máquinas de extremo, con 11 bits para la subred y 5 para las máquinas de extremo tendremos 2048 subredes con 32 máquinas de extremo cada una[3].

Extraer la parte de la dirección que se refiere a una máquina de la subred es sencillo, el mecanismo consiste en definir una palabra de 32 bits, llamada **máscara**, cuyos bits definirán la interpretación que se dará a la porción local, así: todo bit que se coloque en 1 en la máscara se considerará como parte de la identificación de la subred, y todo el que sea 0 se considerará como parte de la identificación de la máquina extremo, esto lo ilustra la **Figura 7.20b**,donde **me** indica máquina extremo**.**

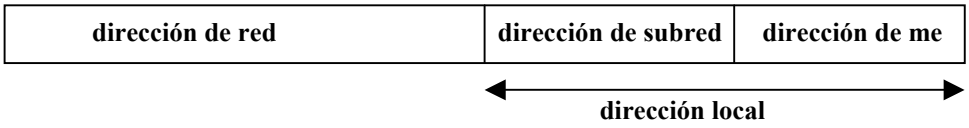


Figura 7.20b.Estructura de direcciones de la subred.

Por ejemplo si tenemos una dirección tipo B 150.186.34.1 con un esquema subred/me, 11/5 la máscara **de la subred** es 255.255.255.224. Al realizar un AND entre la dirección asignada a la máquina extremo y la máscara (150.186.34.1 AND 255.255.255.224)obtendremos la porción que identifica a la subred física (150.186.34.0),si a continuación con el resultado anterior hacemos un Xor(or exclusivo),con la dirección de la máquina extremo(150.186.34.0 XOR 150.186.34.1),obtendremos la porción que identifica a la máquina extremo(en realidad a su interfase como ya se dijo),veamos:

dirección de la máquina extremo	150.186.034.001	10010110.10111010.00100010 00000001
máscara	255.255.255.224	11111111.11111111.11111111.11100000
subred física	150.186.034.000	10010110.10111010.00100010 00000000
dirección de la máquina extremo	150.186.034.001	10010110.10111010.00100010 00000001
máquina extremo	000.000.000.001	00000000.00000000.00000000.00000001

Obsérvese que este mecanismo de subredes simplifica el enrutamiento pero **no aumenta** el número de direcciones disponibles y que utilizando adecuadamente las máscaras una red puede dividirse en varias subredes y estas a su vez en varias subredes y así sucesivamente.

Dado que para algunos usuarios una dirección tipo B es demasiado y una tipo C es muy poco, se trabaja con **superredes** que consiste en otorgar **varias direcciones tipo C** a esos usuarios, ver **[10]**.

[2] en realidad 254 subredes con 254 máquinas de extremo,pues todos 1 y todos 0 están reservadas para la difusión y no se recomiendan.
[3] Aquí también son menos por las mismas razones.

Por ejemplo consideremos la subred de la Universidad de Carabobo que a su vez está dividida en varias subredes, la subred UC pertenece un red denominada **Reacciun**, que es la red de Universidades Nacionales, o sea las Universidades Públicas de Venezuela.

Reacciun tiene asignada una dirección **Clase B,** la 150.186.0.0, cuya máscara es 255.255.0.0, lo que significa que **todos** los enrutadores **excepto los de Reacciun** ven a las Universidades (y entre ellas a la Universidad de Carabobo) como 150.186.0.0 y cualquier paquete destinado esas Universidades, que tendrá los dos primeros octetos como 150.86 será enviado al enrutador de Reacciun.

Reacciun en esa red creó 8 subredes ó grupos, la máscara de estas subredes es 255.255.224.0 que en binario resulta 11111111.11111111.11100000.00000000, son 2^3 subredes con un número máximo de 2^{13} máquinas ó host pues el esquema es 3/13, tal como se describe enseguida:

Grupo	Rango	Dirección Base ó Red
0	0-31	150.186.0.0
1	32-63	150.186.32.0
2	64-95	150.186.64.0
3	96-127	150.186.96.0
4	128-159	150.186.128.0
5	160-191	150.186.160.0
6	192-223	150.186.192.0
7	224-255	150.186.224.0

El enrutador de Reacciun con la máscara 255.255.224.0 enruta hacia una de las 8 subredes ó grupos.

Cada grupo a su vez está constituído por otras subredes, así el subgrupo asignado por Reacciun a la Universidad de Carabobo es la **Red** 150.186.32.0 que consta de un **Rango** de direcciones entre 150.186.32.0 y 150.186.63.255 con la posibilidad de 2^{13} máquinas de extremo ó hosts.

El administrador de esas direcciones es RedUC quien las particiona de acuerdo a las necesidades,la partición escogida de las 2^{13} máquinas de extremo puede ser 5/8, lo que significa 2^5 subredes: de 150.186.32.0 a 150.186.63.0 con $2^8 – 2$ host ó máquinas de extremo cada una, en definitiva en UC pudiera tener 32 subredes con 256 máquinas cada una y la máscara para esas subredes es 255.255.255.0. Sin embargo esquemas 4/9 se escogieron para ciertas subredes, amén de otros que no describiremos aquí.

En el caso de la Facultad de Ingeniería se le asignaron dos direcciones base: 150.186.34.0 y 150.186.35.0, usando el esquema 4/9 con una máscara 255.255.254.0..El enrutador UC usa la máscara 255.255.254.0 para enrutar hacia la Facultad de Ingeniería.

Esas dos direcciones son a su vez particionadas y esto implicaría 16 subredes en cada una con $2^9–2$ máquinas, pero no ha hecho así porque las diversas dependencias tienen necesidades diferentes y las direcciones son escasas, por ello se adoptó el siguiente esquema:

Parámetros de Configuración:

Dirección de la Red: 150.186.34.0
Máscara: 255.255.254.0
Dirección del Gateway: 150.186.34.1
Dirección de Broadcast: 150.186.35.255
Dirección de Administración: 150.186.35.254
Rango de Direcciones para Gateway Internos: 150.186.34.2 – 150.186.34.31

Segmentos: **Rango de direcciones**

- Escuela de Ingeniería Química 150.186.34.32 – 150.186.34.63
- Escuela de Ingeniería Eléctrica 150.186.34.64 – 150.186.34.127
- Biblioteca 150.186.34.128 – 150.186.34.159
- Escuela de Ingeniería Industrial 150.186.34.160 – 150.186.34.191
- Imyca Gateway 150.186.34.4 150.186.34.192 – 150.186.34.255
- Decanato 150.186.35.1 - 150.186.35.32
- Departamentos de Física y Dibujo 150.186.35.33 - 150.186.35.47
- Departamento de Computación
  Gateway 150.186.34.2
  1ra Red: 150-186.35.48 – 150.186.35.63
  2da Red 150.186.35.64 - 150.186.35.95
- Escuela de Ingeniería Civi 150.186.35.96 - 150.186.35.127
- Escuela de Ingeniería Mecánica 150.186.35.128 – 150.186.35.159
- 1er Segmento de Reserva 150.186.35.160 - 150.186.35.191
- Centro de Procesamiento de Imágenes.150.186.35.192 - 150.186.35.223
- 2do Segmento de Reserva 150.186.35.224 - 150.186.35.247
- Apucito 150.186.35.248 - 150.186.35.251
- 3er Segmento de Reserva 150.186.35.252 - 150.186.35.255

Se pudiera abundar más sobre la RedUC y el backbone de Fibra Óptica con sus switches ATM, pero eso escapa a los objetivos de esta Sección y solo diremos que hay subredes en las distintas Facultades, Rectorado y otras dependencias, además RedUc cuenta con cuatro servidores que se encuentran en la LAN 150.186.32.0, ellos son:

Thor

- Servidor de correo electrónico y DNS
- Dirección 150.186.32.2
- Nombre de dominio: thor.uc.edu.ve

Odin

- Servidor de DNS y PPP.
- Dirección 150.186.32.3
- Nombre de dominio: odin.uc.edu.ve

Tyr

- Servidor FTP.
- Dirección 150.186.32.4
- Nombre de dominio: tyr.uc.edu.ve

Hoder

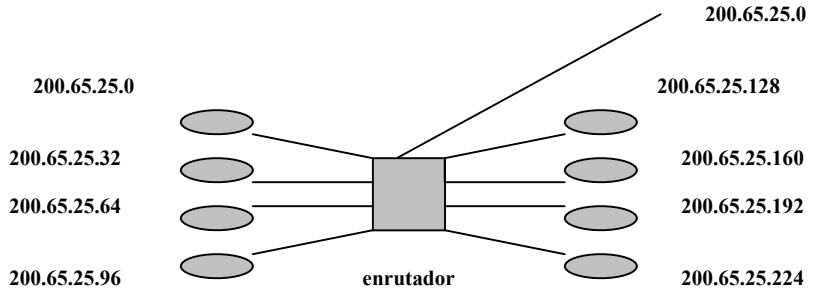
- Servidor WWW y PPP
- Dirección 150.186.32.5
- Nombre de dominio: hoder.uc.edu.ve

Veamos otro ejemplo de uso de máscaras:

Supongamos una dirección Clase C, 200.65.25.0, otorgada a una institución cuya red necesita 8 subredes ó segmentos de red con un máximo de 30 máquinas de extremo en cada subred.

Definimos por lo tanto la siguiente máscara:

255.255.255.224 que corresponde a 11111111.11111111.11111111.11100000



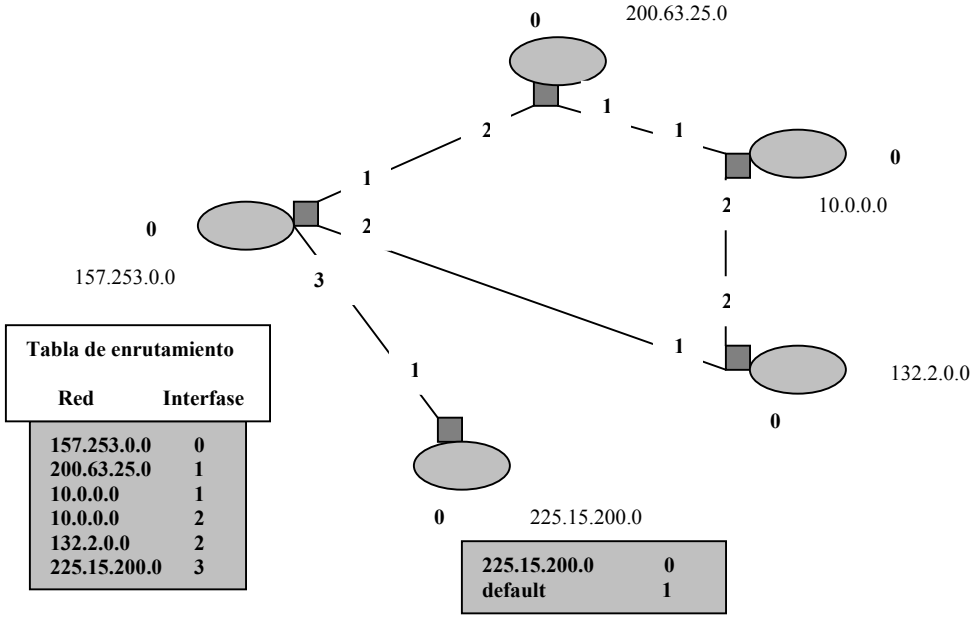
Tenemos entonces las siguientes subredes y grupos de máquinas de extremo:

Subred	Máquinas de extremo	Broadcast
0	1 a 30	31
32	33 a 62	63
64	65 a 94	95
96	97 a 126	127
128	129 a 158	159
160	161 a 190	191
192	193 a 222	223
224	225 a 254	255

El enrutamiento funciona así:

- Supongamnos llega al enrutador un paquete para 200.65.25.102.
- El enrutador determina que la dirección corresponde a la red que él maneja 200.65.25.0.
- El 102 en binario corresponde a 01100110.
- Se aplica la máscara definida (11100000), o sea se realiza un AND lógico.
- El resultado es 01100000 que determina que corresponde a la **subred** 200.65.25.96.
- El enrutador envía el paquete por la interfase respectiva.

Consideremos un ejemplo más, tenemos una red constituída por varias redes interconectadas entre sí por medio de enrutadores cada uno de los cuales tiene **interfases**, de las que las numeradas con 1 o valores superiores están conectadas a **medios físicos** de interconexión.



Supongamos que la máquina de extremo 157.253.48.32 desea enviar información la máquina de extremo 225.15.200.100, ocurre lo siguiente:

- La 157.253.48.32 envía la información al enrutador respectivo, que la recibe por la **interfase 0**.
- El enrutador toma la dirección de destino, determina si es tipo A,B,C ó D y extrae de allí la parte correspondiente a la dirección de red(225.15.200.0).
- Verifica la existencia de una entrada correspondiente a esa dirección de red en la Tabla de Enrutamiento, determina que debe transmitir la información por la interfase 3 y así lo hace.
- El enrutador del otro extremo recibe la información por la interfase 1.
- Extrae mediante la **máscara de subred**(que como se verá se obtiene mediante mensajes ICMP), la información relativa a la dirección de la máquina de destino.
- Determina mediante su Tabla de Enrutamiento que esa máquina está conectada a la **interfase local 0**.
- Transmite la información(como se verá usa ARP para determinar la **dirección física** de la máquina).

Como estas direcciones numéricas son difíciles de recordar, siendo más fácil hacerlo con **nombres** ó **hostnames** que se asocian a empresas, localidades, universidades, etc se ha creado un servicio llamado **DNS**(**D**omain **N**ame **S**ystem),ó **Servidor de Nombres**, que se ocupa de traducir el nombre fácilmente recordable al número ó dirección IP respectivo. Los **nombres** ó **hostnames** son una serie de "etiquetas" **organizadas jerárquicamente** y separadas por puntos, comienza con la etiqueta correspondiente a la máquina de extremo(por ejemplo **labcom**) y sigue con el nombre local de la subred ó **dominio**(por ejemplo **ing**),luego el nombre de la red ó **dominio** de la institución(**uc**) seguido por otras identificaciones(**edu.ve**) para tener como nombre de esa máquina **labcom.ing.uc.edu.ve**, que corresponde al número150.186.34.90.

7.3.2.1.3.-Los paquetes que circulan en la red-

Recordemos además que ya se dijo que la máquina de extremo "arma" en forma de una cebolla el paquete que circula en la red y llega al enrutador, dicho paquete se compone de:

- los **datos**, a ellos se les agrega un **encabezado TCP** y se obtiene el llamado **segmento TCP.**
- a esto se agrega el **encabezado IP**(decimos a veces que "se mete en el **sobre IP"**) dando lugar al **datagrama IP**.
- El datagrama IP se **encapsula** en el protocolo de la red(Ethernet, Token Ring, etc).

Esto lo esquematiza la **Figura 7.21.**

Figura 7.21.Envoltura de los datos.

Veamos como está conformado cada uno de ellos:

Segmento TCP.

0								16	31
Source Port								Destination Port	
Sequence Number									
Acnowledgment Number									
Data offset	Reserved	URG	ACK	PSH	RST	SYN	FIN	Window	
Checksum								Urgent Pointer	
Options									
Data ....next 500 octets									

Figura 7.22.Segmento TCP.

Los campos del **segmento TCP** mostrados en la **Figura 7.22** corresponden **encabezado TCP**(lo que se indica en **Figura 7.22** menos lo datos) y **datos.** Veamos con detalle a:

Source Port y **Destination Port**, identifica los puntos en los que la capa superior fuente y el proceso destino reciben los servicios TCP.

Sequence number, normalmente especifica el número asignado al primer byte de datos del presente mensaje. En ciertas circunstancias puede ser utilizado para identificar un número inicial de secuencia a ser usado por la transmisión venidera.

Acknowledgment number, contiene el número de secuencia del próximo byte de datos que el emisor del paquete espera recibir.

Data offset, indica el número de palabras de 32 bits en el encabezado TCP.

Reserved,reservado para uso futuro.

URG,ACK,PSH,RST,SYN,FIN, son **flags**, banderas que llevan información de control.

Window, especifica la dimensión de la ventana de recepción del emisor, esto es el espacio disponible para datos entrantes.

Checksum, indica si el encabezado TCP fue dañado durante su tránsito.

Urgent Pointer, apunta al primer byte urgente en el paquete.

Options, especifica varios opciones TCP.

Data, los próximos 500 octetos, contiene la información proveniente de las capas superiores.

Datagrama IP.

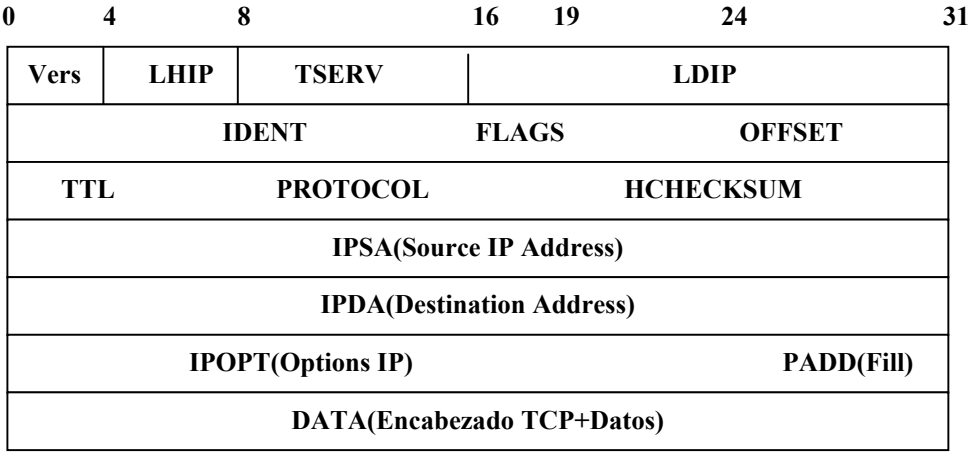


Figura 7.23.Datagrama IP

Veamos el significado de estos campos:

VERS, de 4 bits, contiene **la versión del protocolo IP** que se utilizó para crear el datagrama. Esto se utiliza para verificar que el emisor, el receptor y cualquier enrutador entre ellos proceda de acuerdo al formato del datagrama. El protocolo IP actual trabaja con la versión 4.0.

LHIP, también de 4 bits, proporciona la **longitud del encabezado** del datagrama medida en palabras de 32 bits. Como se puede ver todos los campos del encabezado tienen longitudes fijas, a excepción de los campos **OPTIONS y PADD**.El encabezado más común,que no contiene opciones ni rellenos, mide 20 octetos y su longitud es 5.

TSERV, con 8 bits**,** especifica como una determinada capa superior desea que sea manejado el datagrama. El campo está dividido en 5 subcampos, así se ve en la **Figura 7.24**.

PRECEDENCE	D	T	R	SIN USO

Figura 7.24.Los 5 subcampos del TSERV de 8 bits

PRECEDENCE tiene 3 bits que especifican la **prioridad** del datagrama, con valores que van desde 0(prioridad normal) hasta 7 (control de red).

Los bits **D,T,**y **R** especifican el **tipo de transporte** deseado para el datagrama. El bit **D** activado solicita procesamiento con retardos cortos, el bit **T** solicita un alto desempeño, y el bit **R** solicita alta confiabilidad. Este especificación de tipo de transporte es una indicación para el algoritmo de enrutamiento, que ayuda en la selección de una ruta entre varias hacia un destino, con base en el conocimiento de las tecnologías de hardware disponibles en esas rutas. Una red TCP/IP no garantiza la realización del tipo de transporte solicitado.

LDIP, que es la **longitud del datagrama IP** medida en octetos, este campo tiene 16 bits, por lo que el tamaño máximo del datagrama es de 2^{16} ó 65535 octetos.

IDENT contiene un **número que identifica a este datagrama**, es utilizado para reorganizar el mensaje en el extremo de destino.

FLAGS, es una campo de tres bits en el que los 2 bits de menor orden controlan la fragmentación, un bit especifica si el paquete puede ser fragmentado, el segundo bit especifica si el paquete es el último fragmento en una serie de paquetes fragmentados.

TTL(Time **t**o **L**ive) mantiene un contador que se va decrementando gradualmente, cuando llega a cero el paquete es descartado, esto a fin de evitar paquetes circulando indefinidamente.

PROTOCOL, indica cual de los **protocolos de capa superior** recibe los paquetes entrantes una vez que el procesado IP ha finalizado.

HCHECKSUM, asegura la **integridad del encabezamiento IP**.

IPSA, IP Source **A**ddress, especifica el **nodo de origen**.

DPSA, IP Destination **A**ddress, especifica el **nodo de destino**

IPOPT, IP OPTions, permite a IP soportar **opciones**, por ejemplo seguridad.

PADD, no usado, es de relleno.

DATA, contiene los datos de la capa superior.

Al hablar de FLAGS se mencionó el término **fragmentación**, sin aclarar que significaba, vemos a hacerlo ahora.

Ethernet limita la transferencia de datos a 1500 octetos, FDDI permite cerca de 4470 octetos por trama, estos límites son la **MTU**(**M**aximun **T**ransference **U**nit) ó **Unidad de Transferencia Máxima** de la red, el software TCP/IP selecciona el tamaño del datagrama más conveniente desde el principio y establece una forma para dividir este datagrama en pequeños fragmentos cuando el datagrama necesita viajar a través de una red que tiene una MTU pequeña. Las pequeñas piezas dentro del datagrama dividido se conocen con el nombre de **fragmento** y el proceso como **fragmentación**, la **Figura 7.25**.ilustra este caso.

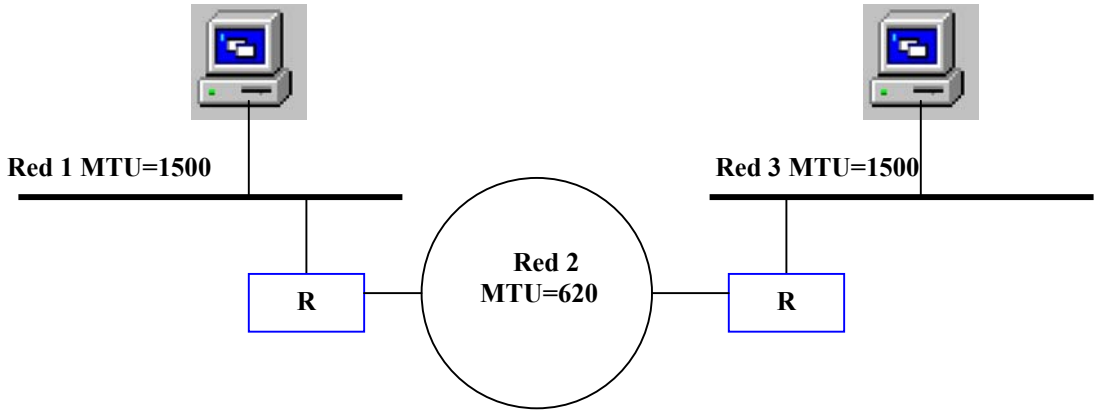


Figura 7.25.Un caso de fragmentación.

Cada fragmento contiene un encabezado de datagrama que duplica el encabezado original, con la excepción de un bit en el campo FLAGS que muestra que este es un fragmento, seguido por tantos datos como puedan ser contenidos en el fragmento siempre y cuando la longitud total se mantenga en un valor menor que el MTU de la red en la que debe viajar..

Aún cuando en su viaje el fragmento encuentre una red física con un MTU superior a que produjo la fragmentación esta será atravesada por fragmentos pequeños.

Los fragmentos se deben reensamblar, para producir una copia completa del datagrama original antes de que pueda procesarse en el lugar de destino, si se pierde cualquier fragmento el datagrama no podrá reensamblarse,la máquina receptora tiene un temporizador de reensamblado que arranca cuando recibe el fragmento inicial, si el temporizador termina antes de que todos los fragmentos lleguen, la máquina receptora descartará los fragmentos sin procesar el datagrama**[13]**.

Interfase de Red con Ethernet

Cuando TCP/IP opera desde una red Ethernet,tal como se explicó más arriba, el datagrama IP es encapsulado en una trama Ethernet(ver **Capítulo 6**),tal como muestra la **Figura 7.26.**

0	16	31
Ethernet Destination Address(first 32 bits)		
Ethernet Destination(last 16 bits)	Ethernet Source(first 16 bits)	
Ethernet Source Address(last 32 bits)		
Type Code		
Data(IP Header+TCP Header+Application Data)		
Ethernet Checksum		

Figura 7.26.Estructura de la trama Ethernet.

7.3.2.1.4.-Servicios de Inter-Red.

Veamos con un poco más de detalle el modelo de capas de TCP/IP, en que parecen ubicados muchos de los protocolos que describiremos en esta subsección y en las siguientes, **Figura 7.27.**

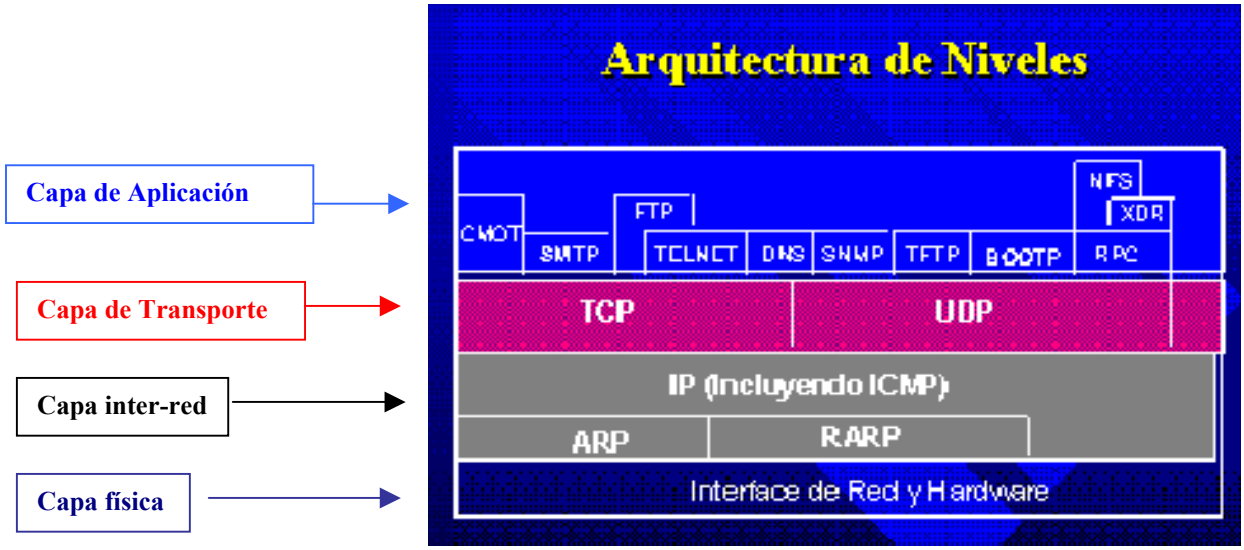


Figura 7.27.Modelo de capas de TCP/IP

Los **Servicios ó Protocolos Inter-red** son **:**

- **IP**(Internet **P**rotocol)
- **ARP**(**A**ddress **R**esolution **P**rotocol)
- **RARP** (**R**everse **A**ddress **R**esolution **P**rotocol)
- **ICMP**(Internet **C**ontrol **M**essage **P**rotocol)

Vamos a verlos con moderado detalle:

IP(**I**nternet **P**rotocol)

En lo precedente hemos dado ciertos detalles de **IP**, que pueden resumirse así:

- **Sistema de distribución o entrega de paquetes**
- **Sistema NO Confiable**
- **Se realiza "el mejor esfuerzo"**
- **No orientado a conexión**
- **No garantiza la entrega**
- **El paquete se puede perder, duplicar, demorar o entregar en diferente orden**
- **Se define la unidad básica de transmisión (DATAGRAMA), el enrutamiento y las reglas de procesamiento de paquetes.**

ARP(**A**ddress **R**esolution **P**rotocol)**[10]**

El esquema de direcciones IP consiste en que cada máquina de extremo tiene asignada por software una dirección de 32 bits, una red de redes entonces es una **red virtual**, en cambio la misma máquina como parte de una **red física**, como Ethernet, tiene **direcciones físicas** que son grupos de 48 bits asignadas desde la fabricación de la tarjeta NIC.

Cualquier datagrama generado por una capa superior(aplicación, transporte ó IP)usa su direccion IP para especificar su origen y destino, pero ocurre que esos datagramas son enviados al medio físico al cual están conectadas todas las interfaces Ethernet de las máquinas de la red y aquellas solo comprenden las direcciones físicas.

El protocolo ARP es usado comunmente **en las redes Ethernet** a fin de determinar la correspondencia entre una dirección IP y una dirección física a fin de que los paquetes puedan alcanzar su destino dentro de esa red.

Cuando la capa física necesita conocer la dirección física que tiene determinada máquina de extremo cuya dirección IP conocemos, envía un requerimiento ARP, en un formato específico que todas las interfaces entienden, y que en nuestro lenguaje diría "necesito la dirección Ethernet de la máquina de extremo cuya dirección IP es <Dir IP>".Todas las interfaces oyen el mensaje, la red es de difusión, pero solo la interfase cuya dirección IP aparece en el requerimiento responde, usando para ello un formato preestablecido por el protocolo, pero que en nuestro lenguaje diría: "<Dir IP> está asociado con la interfase <Dir Ethernet>".

El protocolo ARP guarda en cada máquina de extremo **tablas** con las respuestas obtenidas a fin de que la próxima vez que tenga que solicitarse la dirección física de la misma máquina ya sabe la dirección física, esto contribuye a descongestionar la red.

Decimos entonces que ARP:

- **Permite a una máquina de extremo de una red encontrar la dirección física de otra máquina de la misma red utilizando únicamente la dirección IP.**

Esta idea de ARP es extendida a un esquema denominado **Proxy ARP**, que fue mencionado en la **Sección 7.3.2.1.2.3,**para permitir, mediante un simple artilugio que **dos redes físicamente diferentes** compartan una dirección IP (la porción de red de la dirección),de modo que sean vistas desde el punto de vista del protocolo IP como si estuviesen en la misma red. Para ello supongamos tener inicialmente una red física(principal)conectada a Internet, se agrega luego otra red física(llamada oculta) y se interconectan las redes con un enrutador que ejecuta Proxy ARP.

El enrutador que ejecuta Proxy ARP tiene una interfaz Ethernet para cada una de las redes físicas que conecta, cada interfaz tiene asociadas una dirección física y otra IP. Este enrutador recibe, como todas las máquinas conectadas a la red, los requerimientos ARP(que son locales) de cualquier máquina, cuando uno de esos requerimientos va dirigido a una máquina en otra red el enrutador responde que él es **esa** máquina, la máquina originaria recibe esta respuesta y envía la información al enrutador, éste al recibirla la envía a la otra red identificando a la máquina de destino usando requerimiento ARP ó las tablas previamente obtenidas.

Pudiera parecer extraño que como el enrutador que ejecuta proxy ARP responde a todas las peticiones ARP de las máquinas de la otra red, en la tablas que el protocolo ARP lleva cada máquina aparecerá que una misma dirección física(la del enrutador) le corresponden varias direcciones IP, el protocolo ARP permite eso, sin embargo por seguridad algunas implementaciones de ARP no lo permiten por lo que este mecanismo no puede ser utilizado.

RARP (**R**everse **A**ddress **R**esolution **P**rotocol)

Los diseñadores de TCP/IP se dieron cuenta que la dirección física de la interfase tiene dos ventajas: las direcciones por ser de hardware siempre están disponibles y son únicas, por lo tanto el problema de determinar la dirección IP asociadas a cada dirección física ameritó del desarrollo del protocolo RARP, sobre todo en las máquinas sin disco.

El mensaje RARP se envía de una máquina a otra encapsulado en un trama Ethernet, cuyo tipo de trama es 8035_{16},para identificar el campo I como un paquete RARP, la porción de datos de esta trama es de 28 octetos.

RARP funciona en forma diferente a ARP, la máquina que envía un requerimiento RARP se especifica como destino, todas las máquinas de la red reciben la solicitud, pero solo aquellas autorizadas a proporcionar **servicio RARP** contestan, estas máquinas se denominan **servidores RARP** que asignan direcciones IP.

Diremos entonces que RARP es:

- **Orientado a solucionar el problema de las máquinas de extremo que no cuentan con almacenamiento externo (Disco). Requiere la existencia de computadores autorizados para la asignación de direcciones IP.**

ICMP(Internet **C**ontrol **M**essage **P**rotocol)**[10][11].**

Hemos visto que IP proporciona un servicio de entrega de datagramas, no confiable y sin conexión, al hacer que cada enrutador direccione datagramas, estos viajan de enrutador a enrutador hasta llegar a uno que pueda entregarlo a la máquina final, como no tiene detección y corrección de errores descansa en un módulo llamado **ICMP** para a) reportar errores en el procesamiento del datagrama y b) proveer un medio para los mensajes de estado y administrativos.

Cuando un enrutador no puede enrutar ó entregar un datagrama, ó si el enrutador detecta una situación anormal que afecta su capacidad de enrutamiento(por ejemplo, congestión)necesita informar a la máquina de origen para que evite ó corrija el problema.

ICMP(Internet **C**ontrol **M**essage **P**rotocol)se utiliza para enviar mensajes de control y error,

Los mensajes ICMP son enviados por los enrutadores a las máquinas de extremo para suministrar realimentación a los sistemas transmisores, tales como reporte de errores. Las máquinas de extremo también pueden enviar mensajes ICMP.

Así los enrutadores envían un mensaje ICMP de datagrama descartado a la máquina de origen, indicando que datagrama IP fue descartado y porqué.

Cuando hay varios enrutadores en una red son utilizados mensajes ICMP de redireccionamiento para asegurar que el tráfico sea despachado inicialmente al enrutador apropiado.

Los enrutadores pueden enviar mensajes ICMP de "parada" a las máquinas de extremo a fin de cuando un enrutador esté congestionado, éste solicite a las máquinas de extremo que reduzcan el volumen de tráfico hasta que desaparezca la congestión.

ICMP tiene también mensajes tipo "eco",esto significa que una máquina "interroga" a otra y si obtiene una respuesta(eco) puede saber que esta operativa, conocer su máscara, etc, además puede evaluarse el tiempo empleado, todas estas facilidades han permitido desarrollar utilidades como **ping**(interroga una máquina de extremo) y **trace**(interroga las máquinas de la ruta para detectarlas),que a su vez permiten producir programas para conocer, graficar y supervisar redes.

Resumiendo, ICMP:

- **Hace parte de toda implementación de IP**
- **Permite a los elementos enrutadores de la red enviar mensajes de error y/o control**
- **Utilizado en la parte de administración de las redes para detectar problemas**
- **Aún cuando utiliza los servicios provistos por IP, no es considerado protocolo de nivel superior sino parte de IP**

7.3.2.1.5.-Servicios ó Protocolos de Transporte.

Estos son, ver **Figura 7.27,**:

TCP(**T**ransport **C**ontrol **P**rotocol)
UDP(**U**ser **D**atagram **P**rotocol)

TCP(**T**ransport **C**ontrol **P**rotocol)

El software de IP da un servicio de entrega de datagramas, no confiable y sin conexión, pues cada enrutador direcciona los datagramas. Es necesario agregar algo que proporcione la entrega de un flujo confiable de información, esa es la labor del **Protocolo de Control de Transmisión, ó TCP**(**T**ransport **C**ontrol **P**rotocol). En realidad TCP es un protocolo independiente de propósitos generales que se puede adaptar a otros sistemas de entrega pues supone muy poco de la red subyacente, por ello puede usarse en una sola red como Ethernet ó en una red de redes, al punto que el protocolo TP-4 de OSI derivo de él.

Si bien TCP añade una funcionalidad importante a los protocolos ya descriptos su implementación es compleja**[10]**,y sin extremar el detalle trataremos de dar los aspectos más relevantes de este protocolo del cual ya hemos dado anteriormente ideas generales.

Recordemos que TCP da varios servicios a la capa de aplicación y esta, a su vez, tiene varios programas con diferentes servicios al usuario. La interfaz entre esos programas de aplicación y el servicio TCP, desarrolla cinco funciones llamadas a veces **servicio de transferencia de flujo**:

- **Orientación de flujo**: los programas de aplicación generan un **flujo de bits** dividido en octetos, el servicio de entrega de flujo en la máquina de extremo receptora pasa al ó los programas de aplicación la misma secuencia de octetos que le pasa el ó los programas de origen a la máquina de extremo transmisora.

- **Conexión de circuito virtual**: la transferencia de flujo es como una comunicación telefónica, existen una serie de pasos(llamada, aceptación, etc)que realiza este protocolo para luego informar a los programas de aplicación que se estableció una **conexión** y que pueden transferirse los datos(si ha sido posible, de no serlo lo notifican),durante la transferencia el software del protocolo en las dos máquinas sigue comunicándose para asegurar que los datos se reciban sin errores. Esta conexión se llama de **circuito virtual**, porque los programas de aplicación lo ven como un circuito dedicado cuya confiabilidad está dada por el servicio de entrega de flujo.

- **Transferencia con memoria intermedia**: a fin de hacer eficiente la transferencia y minimizar el tráfico en la red el protocolo puede combinar en un datagrama datos de diferentes programas de aplicación, ó por el contrario dividir los de un programa de aplicación que genera un flujo muy grande.

- **Flujo no estructurado**: el protocolo no forma flujo estructurado de datos, es tarea de los programas de aplicación ponerse de acuerdo en su estructura.

- **Conexión full duplex**: los datos pueden viajar simultáneamente en ambas direcciones, eso tiene la ventaja adicional que el protocolo puede enviar datos de control de flujo al origen mientras fluyen los datos en la dirección opuesta.

Ya se dijo que TCP es un **servicio de entrega confiable**, por lo que garantiza la entrega de una máquina de extremo a otra sin pérdida ni duplicación. Como TCP está sobre IP que es un sistema de transferencia no confiable, para lograr su cometido utiliza, cuando es necesario, **retransmisión**, mediante el uso de ACK con ventana deslizante descrito en un Capítulo anterior.

TCP permite que varios programas de aplicación **se comuniquen de manera concurrente** o sea soporta multitarea, para ello realiza el multiplexado en la máquina de extremo transmisora y el demultiplexado en la receptora, utilizando **números de puerto de protocolo**(cosa que también hace UDP, el otro protocolo de transporte)**[11]**.

Este multiplexado y demultiplexado es simple: cada programa de aplicación debe negociar con el sistema operativo la obtención de un puerto asociado y un número para ese puerto, una vez que es asignado el puerto, cualquier datagrama que envié el programa de aplicación a través de él, tendrá el número de puerto en el primer campo del segmento TCP descripto en Figura 7.22,en el extremo receptor TCP recibe el segmento y lo demultiplexa, o sea lo entrega al puerto de destino señalado en el segundo campo del segmento TCP. Los puertos para los programas de aplicación cliente tienen números superiores a 255 que son asignados dinámicamente y los de los programas servidor son preasignados por la IANA(Internet Assigned Numbers Authority)entre 0 y 255 y no cambian.

La **Tabla 7.1** identifica algunos de los números de puerto "**bien conocidos**", utilizados para identificar los programas de aplicación de servidor más comunes, la lista no es exhaustiva pero contiene las aplicaciones más utilizadas.

Tabla 7.1 Números de puerto de algunos programas de aplicación

Número	Nombre	Descripción
0		Reservado
5	RJE	Remote Job Entry
7	ECHO	Echo
11	USERS	Active Users
13	DAYTIME	Daytime
20	FTP-DATA	File Transfer(Data)
21	FTP	File Transfer(Control)
23	TELNET	Telnet
25	SMTP	Simple Mail Transfer
37	TIME	Time
42	NAMESERV	Host Name Server
43	NICKNAME	Who Is
53	DOMAIN	Domain Name Server
67	BOOTPS	Bootstrap Protocol Server
68	BOOTPC	Bootstrap Protocol Client
69	TFTP	Trivial File Transfer
79	FINGER	Finger
101	HOSTNAME	NIC Host Name Server
102	ISO-TSAP	ISO-TSAP
103	X-400	X-400
104	X-400SND	X-400SND
105	CSNET-NS	CSNET Mail Box Name Server
109	POP2	Post Office Protocol 2
110	POP3	Post Office Protocol 3
111	RPC	SUN RPC Portmap
137	NETBIOS-NS	NETBIOS Name Service
138	NETBIOS-DG	NETBIOS Datagram Service
139	NETBIOS-SS	NETBIOS Session Service
160-223		Reservados

En realidad en TCP se identifican los **puntos extremos** de la **conexión**, cada uno mediante un par de números enteros (Dirección IP Máquina *x* ,Puerto de Máquina *x*).La **conexión** de circuito virtual es el concepto básico de TCP, pero la **conexión** es identificada por dos pares, cada uno correspondiente a un extremo, así una conexión pudiera ser identificada como:

128.9.0.32 , 1184 y 150.186.34.90 , 53

Otra conexión simultánea, pudiera ser:

128.2.254.139 , 1184 y 150.186.34.90 , 53

Parece extraño que las dos conexiones utilicen el mismo puerto 53 en la máquina 150.186.34.90,pero no hay ambigüedad pues TCP asocia los mensajes entrantes a la conexión y no al puerto, y para ello utiliza los dos pares descriptos.

De **TCP** ya hemos hablado extensamente, por ello sintetizaremos sus características:

- **Servicio de entrega de paquetes orientado a conexión**
- **Es confiable y se basa en el establecimiento de Circuitos Virtuales**
- **Maneja el concepto de puertos**
- **Las conexiones se identifican por dos pares :**
  (Dirección IP Máquina 1, Puerto Máquina 1)
  (Dirección IP Máquina 2, Puerto Máquina 2)
- **Se pueden tener varias conexiones simultáneas al mismo puerto en una máquina.**

UDP(**U**ser **D**atagram **P**rotocol)

Este Protocolo de Datagrama del Usuario ó UDP es un mecanismo primario que utilizan los programas de aplicación para enviar datagramas a otros programas de aplicación en un esquema de multitarea.

Este protocolo es más simple que TCP y fue diseñado para soportar aplicaciones menos exigentes, en las cuales la información que intercambian es suficientemente pequeña como para garantizar que no será necesario dividirla en varios bloques y por ello tampoco será necesario el control de secuencia que se usa en TCP para garantizar el reensamblaje del mensaje, pues se supone que la información recibida de la aplicación cabe en un solo datagrama.

Por todo ello es que tiene menos cosas que verificar, su encabezado es más pequeño que el de TCP y resulta más eficiente, pero pone labores como la de división de bloques de información(de ser necesario)en manos de la capa de aplicación.

UDP no provee un esquema de reconocimiento que asegure que los mensajes lleguen a destino, por lo que es posible perder datagramas, recibir datagramas duplicados ó fuera de orden, tampoco provee un mecanismo para controlar el flujo de mensajes(cosa que deja en manos de las aplicaciones).

La idea de disponer de un protocolo de transporte tan elemental y poco confiable, es para permitir que los desarrolladores de aplicaciones, considerando las exigencias específicas de cada una, establezcan los mecanismos necesarios ajustados exactamente a ellas, lo que hará el protocolo mucho más eficiente. Recordemos que muchas aplicaciones son muy elementales y los controles son fáciles de implementar si son necesarios.

UDP utiliza también el concepto de **puertos** y habrá dos números que se incluirán en el encabezado UDP: PUERTO DE ORIGEN UDP y PUERTO DE DESTINO UDP, existen números de puerto UDP reservados, conocidos y disponibles**[10],[13]**,así lo ilustra la **Figura 7.28**,que muestra el multiplexado, el demultiplexado se vería en sentido inverso, en realidad se trata aquí de una cola de salida y otra de entrada y no existe el concepto de conexión de TCP.

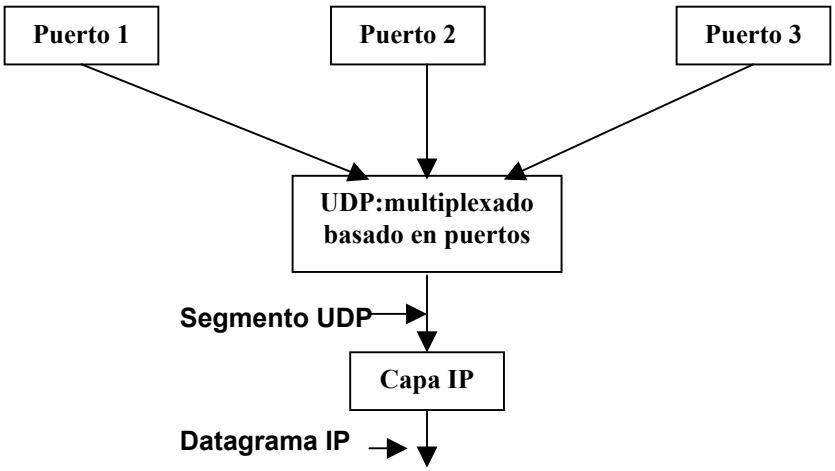


Figura 7.28.Multiplexado UDP basado en puertos.

Resumiendo UDP tiene las siguientes características:

- **Servicio de entrega de paquetes NO orientado a conexión**
  - **Las aplicaciones desarrolladas que utilizan UDP deben ser responsables de la confiabilidad**
  - **Varias aplicaciones pueden utilizar simultáneamente los servicios de UDP**
  - **La forma de diferenciar las aplicaciones consiste en la asignación de PUERTOS**
  - **Algunos puertos se denominan PUERTOS BIEN CONOCIDOS y se asignan a aplicaciones específicas**

7.3.2.1.6.-Servicios de Aplicación.

En la **Sección 7.3.2.1.1** se enumeraron los **servicios de aplicación,** los recordaremos ahora, son:

TELNET
FTP(**F**ile **T**ransfer **P**rotocol)
SMTP(**S**imple **M**ail **T**ransfer **P**rotocol)
NNTP(**N**etwork **N**ews **T**ransfer **P**rotocol)
CMOT(CMip/cmis **O**ver **T**cp (Common Management Information Services/ Common Management Information Protocol)
DNS(Domain **N**ame **S**ystem)
SNMP(**S**imple**N**etwork **M**anagement **P**rotocol)
TFTP(**T**rivial **F**ile **T**ransfer **P**rotocol)
BOOTP(**BOOT**strap **P**rotocol)
NFS(**N**etwork **F**ile **S**ystem)
XDR(e**X**ternal **D**ata **R**epresentation)
RPC(**R**emote **P**rocedure **C**all)

La lista es muy larga, trataremos de resumir las aplicaciones remitiendo a lector que desee más información a las RFC respectivas o a textos dedicados exclusivamente a TCP/IP, algunos de ellos se citan en la bibliografía de este Capítulo.

TELNET(Terminal Access)

Bajo el esquema **cliente-servidor TELNET** suministra un modo de accesar en el servidor **aplicaciones de terminal** desde una variedad de terminales, independientemente de los procedimientos y códigos particulares propietarios de cada uno de ellos.

Así hay un programa **TELNET Server** que reside en el mismo terminal que contiene la **aplicación**. El programa **TELNET Client** está en la máquina de extremo del usuario ó en el servidor de terminales.

TELNET como protocolo define un **network virtual terminal** que es un juego de formatos de caracteres y teclas de función intermedios que utiliza la red, de modo que los formatos de caracteres y teclas de función propietarios de una máquina de extremo(por ejemplo del usuario)son convertidos, por el Telnet Client, en los de la red en el otro extremo estos son a su vez convertidos en los de la máquina respectiva por el programa Telnet Server y allí entregados a la aplicación. En sentido inverso las cosas funcionan del mismo modo.

La **Figura 7.29** ilustra este proceso(S.O. es Sistema Operativo).

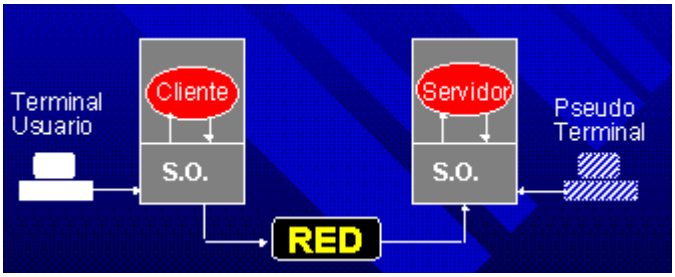


Figura 7.29.TELNET

FTP(File Transfer Protocol)

FTP es un protocolo de para transferir archivos de un sistema a otro que utiliza las facilidades de TCP para asegurar una comunicación confiable extremo a extremo, también utiliza los protocolos de terminal virtual de TELNET para funciones de comando y de control. Existen **FTP Client** ,que reside en la máquina extremo del usuario y **FTP Server** que reside en la máquina que presta el servicio de FTP.

Sus características principales pueden resumirse así:

- **Provee Acceso Interactivo.**
- **Permite especificar la representación de la información con el fin de realizar conversiones, cuando sea necesario.**
- **Se requiere contar con código y palabra clave registrada en el host servidor.**
- **Utiliza dos conexiones paralelas, una para control e interacción con el usuario final y la otra para la transferencia de los datos**

Existen programas de usuario que manejan FTP en forma muy sencilla, aún cuando el propio FTP no es muy complicado de utilizar.

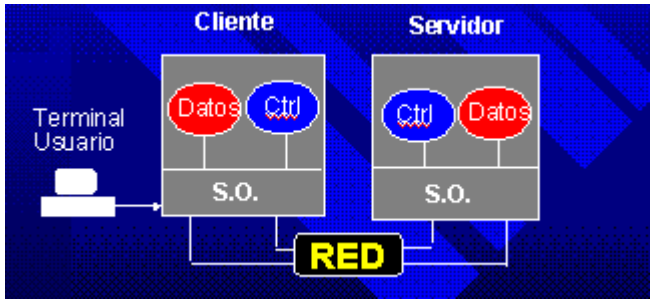


Figura 7.30.FTP

SMTP(**S**imple **M**ail **T**ransfer **P**rotocol)

SMTP es un protocolo de mensajes ó de correo electrónico que utiliza TCP/IP. Existe un **SMTP Sender** ubicado en el usuario, que se ocupa de enviar los mensajes al **SMTP Receiver** del sistema en el **Servidor de Correo** , de donde serán extraídos por el destinatario cuando este lo requiera, cuando el destinatario no pertenece a ese sistema el **SMTP Receiver** actúa también como retransmisor del mensaje hasta su sistema final de donde el destinatario los extraerá oportunamente del **Servidor de Correo** local.

NNTP(**N**etwork **N**ews **T**ransfer **P**rotocol)

NNTP es similar a **SMTP** pero es destinado a noticias

CMOT(**CM**ip/cmis **O**ver **T**cp (Common Management Information Services/ Common Management Information Protocol)

CMOT es un protocolo de gerencia de red basado en el modelo OSI, sin embargo ha tenido muy poco apoyo de la industria**[11].**

DNS(**D**omain **N**ame **S**ystem)

DNS es un protocolo que "traduce" una dirección literal(por ejemplo labcom.ing.uc.edu.ve) en una dirección numérica de TCP/IP, el protocolo es residente en **Servidores de Nombres**, que son máquinas dedicadas a este servicio que mantienen bases de datos de direcciones y las distribuyen a petición.

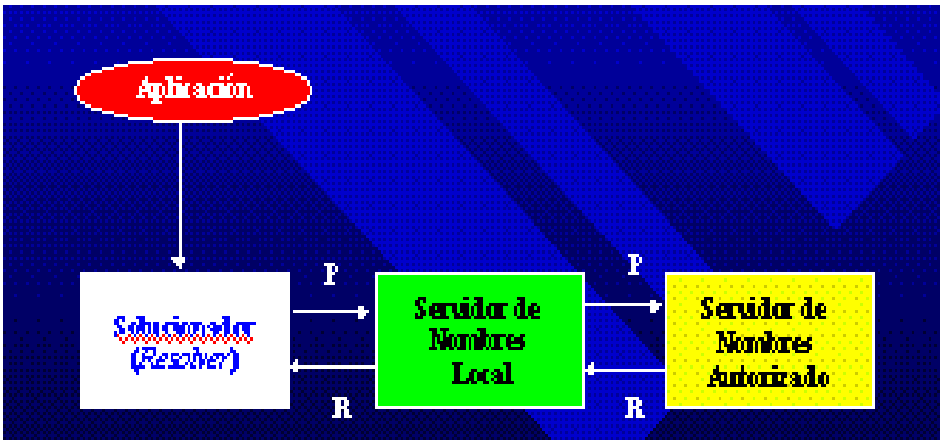


Figura 7.31.DNS

Muchos computadores conectados a grandes redes TCP/IP (y por lo tanto a Internet) tienen un nombre único que se recuerda fácilmente y que se ajusta al esquema jerárquico definido por DNS.

Ejemplo : labcom.ing.uc.edu.ve

significa que en Venezuela(ve),en el grupo educativo(edu),en la Universidad de Carabobo (uc),en la Facultad de Ingeniería(ing),está el Laboratorio de Comunicaciones(labcom).

SNMP(SimpleNetwork Management Protocol)[14]

SNMP es el estándar de TCP/IP para gerencia de red, define un juego de variables de manejo(o gerencia)de red así como un protocolo utilizado para intercambiar información de manejo a través de la red. En **SNMP** una serie de "**manejadores**" controla indirectamente la red a través de "**agentes**" que están ubicados en los equipos(enrutadores, servidores, máquinas de extremo, etc).

Cada **manejador** controla un grupo de **agentes**, los manejadores son aplicaciones que solicitan información a los agentes sobre tráfico, fallas, niveles de tráfico y otros datos operacionales, los correlaciona, notifica a los operadores humanos y cambia parámetros en los equipos, los agentes mantienen una **MIB**(**M**anagenent **I**nformation **B**ase)en la que se almacenan datos de conteo de errores, dimensión de paquetes, tablas de enrutamiento(en los enrutadores),etc.

Bajo **SNMP** los agentes son controlados por los manejadores, suministran información a estos bajo solicitud, aun cuando en ocasiones informan automáticamente eventos como la falla de un enlace .Asimismo los agentes modifican los valores de los MIB según sean instruidos y esos cambios modifican el funcionamiento de los equipos, **RMON**(**R**emote **MON**itoring) se agrega a **SNMP** como un servicio adicional que mejora el manejo de la red.

SNMP utiliza UDP que no es tan seguro como TCP pero si es más eficiente.

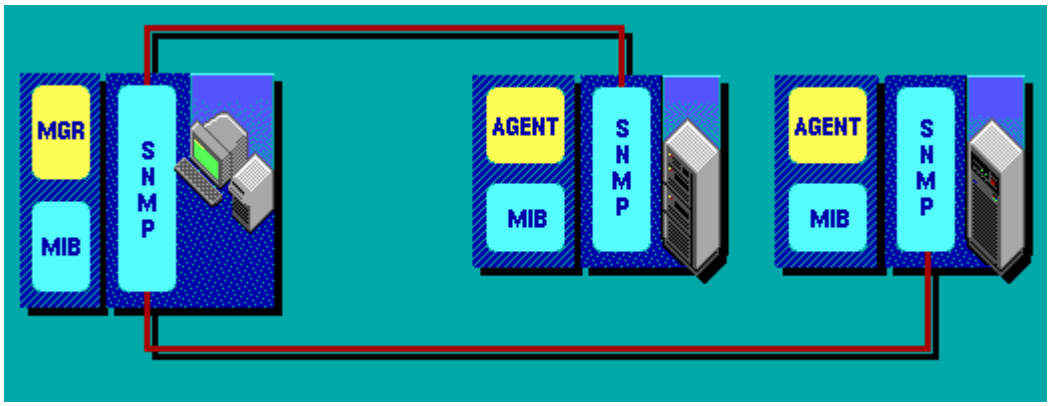


Figura 7.32.SNMP manejador(manager),agente y MIB.

TFTP(Trivial File Transfer Protocol)

TFTP es un sistema de transferencia de archivos diseñado para interacción de poca complejidad entre el cliente y el servidor.

No requiere autenticación, esto es, no se le "exige" al cliente enviar información de código y palabra clave del usuario.

Utiliza los servicios provistos por UDP, usando mecanismos de timeout y retransmisión para asegurar la llegada de los datos.

BOOTP(**BOOT**strap **P**rotocol)

BOOTP corresponde a una alternativa al protocolo RARP que en máquinas sin disco, permite solicitar su dirección IP y otra información al servidor.Puesto que se utiliza UDP y no se conocen las direcciones IP del cliente y tampoco del servidor , en su reemplazo se coloca una dirección de broadcast limitado (255.255.255.255), para que todos los hosts de la red estén en capacidad de recibir el requerimiento y la respuesta.

BOOTP trabaja bajo el esquema cliente servidor y requiere de un solo intercambio de paquetes. En ese solo mensaje **BOOTP** ,que es mucho más eficiente que RARP, especifica muchos datos necesarios para el arranque entre ellos: la dirección IP de la máquina , la de un enrutador y la de un servidor.Los enrutadores pueden ser programados para que permitan el paso de este tipo de paquetes.

BOOTP tiene limitaciones pues fue diseñado para ambientes estáticos. Cuando se usan redes inalámbricas y los usuarios traen laptops esa característica es inconveniente, por ello se diseñó otro protocolo, el **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) , que asigna dinámicamente direcciones IP.**[10],[11].**

NFS(**N**etwork **F**ile **S**ystem)

NFS permite a los computadores compartir archivos a través de la red ó redes, está descripto en la RFC 1094.En realidad consiste de dos protocolos:**mount protocol** y **NFS protocol**.

El mount protocol sirve para identificar un sistema de archivo y la máquina huésped remota que será accesada, en protocolo NSF es responsable de efectuar las operaciones de transferencia de archivos.

XDR(e**X**ternal **D**ata **R**epresentation)

Es un estándar para una representación de datos independiente de la máquina. Para utilizar XDR, un emisor traduce de la representación de una máquina local a la representación externa estándar y un receptor traduce de la representación externa a la representación de la máquina local.

RPC(**R**emote **P**rocedure **C**all)

Es una tecnología en la que un programa invoca servicios a través de una red haciendo modificaciones en los procedimientos de llamada, El protocolo NFS utiliza un tipo específico de RPC.

Algunos autores consideran también otros protocolos de aplicación tales como(no hemos agotado la lista hay muchos otros**[10][11]).**:

X-Windows: que fue desarrollado en el MIT para permitir ver varias ventanas en la misma pantalla ya sean estas de la misma o de distintas máquinas. Windows de Microsoft es similar.

Ping : es un protocolo muy simple que envía un mensaje ICMP y espera la respuesta. Utiliza UDP.

Hostname: usado para recoger información de redes, máquinas, gateways, y dominios.

Kerberos, es un programa de seguridad criptográfico que permite la autenticación de usuarios de una red y autorización de acceso. El nombre viene de un perro de tres cabezas que guarda la entrada de Hades(de quien ó que no aparece claramente).

En los protocolos de transporte no mencionamos **SLIP** que permite el acceso a redes a través de líneas discadas(telefonía),este protocolo ha sido sustituido por **PPP**(**P**oint to **P**oint **P**rotocol) que es el estándar para acceso telefónico a redes.

7.3.2.1.7.-Enmascaramiento de IPs de LINUX ó Linux IP Masquerade.

El **Enmascaramiento IP** ó **IP Masquerade** es una función de redes de Linux muy similar a **uno-a-varios NAT** (**N**etwork **A**ddress **T**ranslation) utilizado en muchas firewalls y enrutadores comerciales.

Por ejemplo si un servidor de Linux está conectado a Internet vía PPP, Ethernet, Token Ring,FDDI, etc, el IP Masquerade permite que máquinas de extremo "internas" conectadas a esta "caja" Linux vía PPP, Ethernet, etc puedan también conectarse Internet. El enmascaramiento IP (IP Masquerading) hace que esto ocurra aún cuando estas máquinas internas ***no tengan direcciones IP válidas asignadas.*** Esas máquinas *internas* ***no tienen porque operar en LINUX*** *y* se hace usando ingeniosamente el concepto de puertos de TCP y UDP.

MASQ permite a un grupo de máquinas de extremo internas acceder a Internet a través del **MASK Gateway,** para las demás máquinas en Internet todo el tráfico saliente aparecerá como generado **por el servidor IP MASQ Linux** y no por las máquinas internas.

IP Masquerade es el mecanismo que permite crear un ambiente de redes **muy** seguro, en una "firewall" bien construída, romper la seguridad de un sistema de enmascaramiento (masquerading) y de las LANs internas es muy difícil.

IP Masquerade es soportado desde el Kernel Linux 1.3.x, en este momento estamos en la versión 2.4,usos corrientes como: Navegación en la Red, TELNET, FTP, PING, TRACEROUTE, etc funcionan sin problema IRC y Real Audio también lo hacen cuando se usan los módulos apropiados de IP MASQ, otros programas como los de audio(MP3, True Speech, etc) y videoconferencia funcionan sin problemas. Funciona bien con Windows 95/98/Me/2000/XP, Windows NT y Windows for Work Groups así como con IBM OS/2, Sun Solaris y otros.

Vamos a dar un ejemplo de cómo trabaja el **enmascaramiento IP**(IP Masquerading), supongamos tener una red Ethernet, que llamamos **red interna** y para las que **no tenemos**(ó no deseamos usar, pues se trata de un recurso limitado y caro)**direcciones IP válidas**, las máquinas de esta red Ethernet pueden operar en cualquier sistema operativo que hable TCP/IP(Windows 95/98//Me/00 es un caso muy común).Tenemos también un servidor de LINUX(una máquina que utiliza LINUX como sistema operativo) que funciona como **LINUX Masquerading Gateway(LMG)** y que esta conectado a Internet vía un ISP(Internet Service Provider) directamente ó mediante una conexión discada(PPP, que adicionalmente requiere modems)**.**

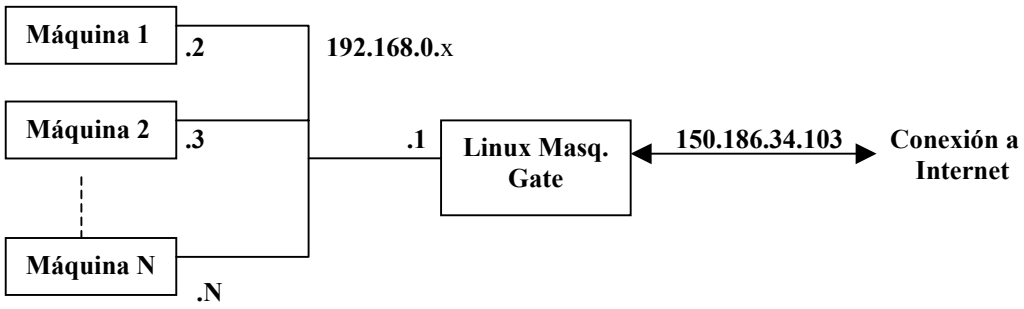


Figura 7.33. Enmascaramiento IP.

Las máquinas de extremo(192.168.0.x con x que va de 2 a N)están configuradas con la máquina Linux Masq Gateway(192.168.0.1)como gateway, ninguna de esas direcciones son válidas, sólo se usa una dirección válida, la 150.186.34.103.

Recordemos que cuando una máquina de extremo envía un paquete a Internet el paquete este lleva en su encabezado TCP un número de puerto(asignado al establecer TCP la conexión correspondiente al programa de aplicación),por ejemplo en la máquina de extremo 2 la conexión del programa TELNET es identificada como 192.168.0.2 , 1184(dirección y número de puerto de la conexión TELNET),al llegar el paquete al Linux Masq. Gateway, este cambia esa parte de la identificación de la conexión colocando **su** dirección(150.186.34.103)y un **nuevo número de puerto,** que para el mundo exterior serán la mitad de la identificación de esa conexión.

Cuando un paquete llega de Internet a la LMG, esta lee el número de puerto, cambia la dirección de destino y el numero de puerto al que uso originalmente la máquina 2 para esta conexión, así para el mundo exterior solo hay aquí una dirección, la 150.186.34.103.

7.3.2.2.-Netware(IPX).

Netware es un sistema operativo de red (NOS) bajo el concepto **cliente-servidor** ya descrito, y fue creado por la empresa Novell a principios de los 80,en esos tiempos las redes eran pequeñas y generalmente homogéneas pues el concepto de redes locales era nuevo, y como ya se ha dicho promovido por la exitosa introducción de las PCs.

A principios de los 90, Netware tenía entre el 50 y el 75 % del mercado con más de medio millon de redes instaladas, en la actualidad su participación ha disminuido pero existen muchas redes Netware en funcionamiento, que coexisten en el mismo canal físico con TCP/IP y otros protocolos. Novell ha lanzado versiones actualizadas de su NOS.

Una característica básica del esquema cliente-servidor de Netware es que el acceso remoto es transparente al usuario, esto se hace mediante llamadas a **procedimientos remotos,** este es un proceso mediante el cuál un programa local que corre en el cliente envía una **llamada** de procedimiento remoto al servidor, este ejecuta lo solicitado y retorna la información solicitada al cliente que la requirió.

La **Figura 7.33** muestra el modelo de capas de Netware y el modelo de OSI, en él se observa que Netware está definido para las capas 3 y superiores, debajo de esas capas puede estar Ethernet/802.3, Token Ring/802.5/FDDI, y ARCnet, Netware también trabaja sobre enlaces síncronos WAN usando PPP(Point to Point Protocol).

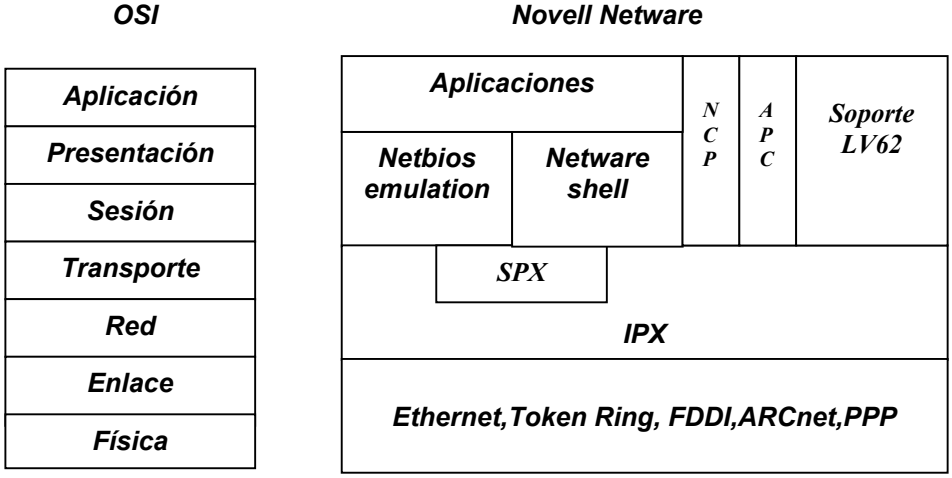


Figura 7.33.Modelo de capas de Netware y de OSI.

IPX(Internetwork Packet Exchange) es un protocolo multipropósito de red y de transporte que puede llevar una serie de **protocolos de servicio** incluyendo el protocolo **SPX**(Sequenced Packet eXchange).IPX es un protocolo de datagramas "sin conexión" que no garantiza la entrega de los mismos pues cada paquete es una entidad individual con su direccionamiento y sin ninguna relación lógica o secuencial con otro paquete, SPX por el contrario es un protocolo "orientado a conexión" que corre como una extensión a IPX y suministra confirmación(ó negación) de la entrega extremo a extremo de los paquetes.

Los protocolos de servicio corren sobre IPX o sobre la combinación IPX/SPX, estos servicios incluyen:

- **NCP**(Netware Core Protocol),este protocolo maneja el grueso de los servicios de Netware, incluyendo el acceso a archivos e impresoras de los servidores.
- **Burst Mode** protocol, es una variación del NCP, que permite a un cliente solicitar y recibir más datos en un mensaje que bajo NCP, fue diseñado para aplicaciones con grandes volúmenes de datos.
- **SAP**(Service Advertising Protocol),los servidores de archivo, de comunicaciones, impresoras y otros tipos de servidores se anuncian a intervalos regulares. Los "clientes" escuchan a este protocolo a fin de saber que recursos están disponibles en ese momento.,los clientes también pueden usarlo para interrogar sobre las capacidades de un servidor específico. Este SAP no tiene nada que ver con el IEEE SAP (Service Access Point) .
- **RIP**(Routing InformationProtocol),es utilizado para ayudar a mover un paquete de una red Netware a otra red Netware. Estos protocolos de enrutamiento son un factor importante en el funcionamiento de los routers o enrutadores.

Recordemos que en el **Capítulo 4** hablamos de **protocolos de acceso**, que son aquellos que se ocupan de las tareas de las capas 1 y 2, por encima de ellos hablamos de **protocolos de red** estos a su vez se dividen por encima de la capa 4, como ya se ha mostrado en el modelo de capas, **protocolos de servicio**. Cada uno de estos últimos tiene formatos de datos y de "hand-shaking" propios, tal como ilustra la **Figura 7.34.**

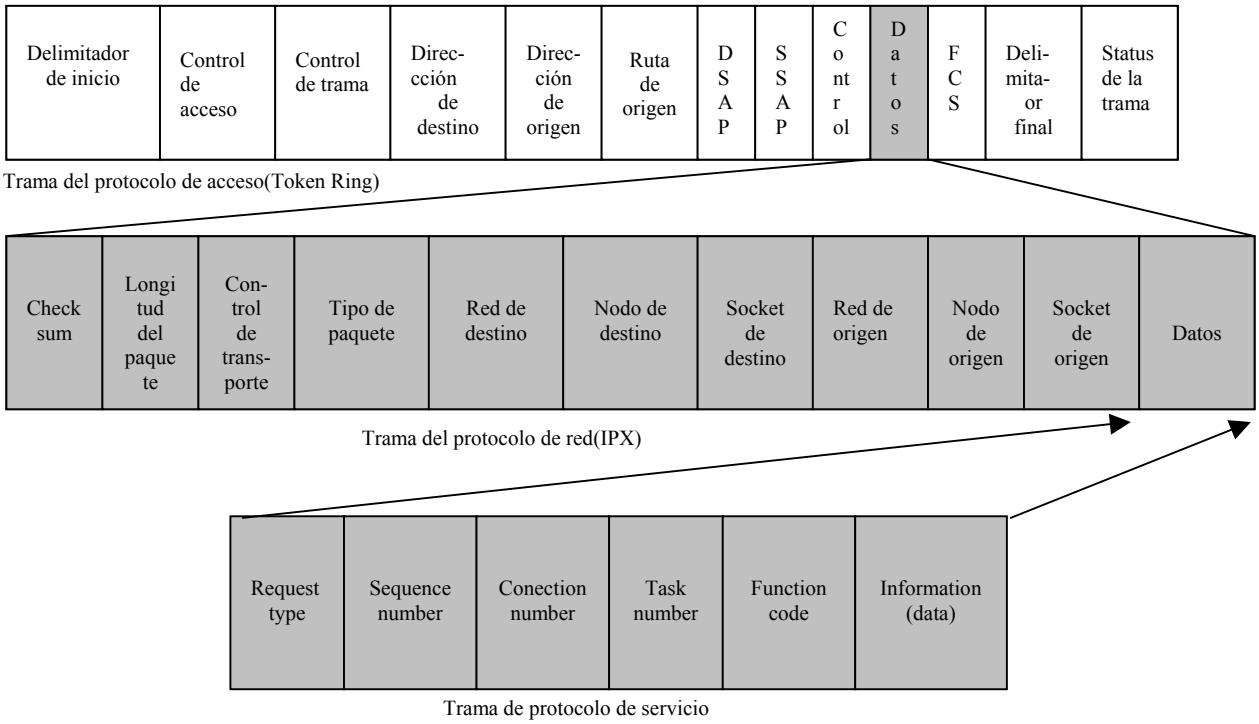


Figura 7.34.Protocolos de acceso, de red y de servicio en Netware.

BIBLIOGRAFÍA

[1] "THE ALOHA SYSTEM-Another Alternative for Computer Communications",AFIPS Conf.Proc., Vol 37,AFIPS Press,Montvale,N.J.,1970,pp 281-285.

[2] Freeman Roger L. ,"Telecommunication Transmission Handbook", Third Edition, John Wiley & Sons,1991.

[3] Minoli Daniel, "Telecommunications Technology Handbook", Artech House,1991.

[4] Enk J. & Beckman M.,"LAN to WAN Interconections", Mc Graw-Hill,1995.

[5] SIEMENS,"Telecomunicación Digital",Tomo 1,"Información Básica", Marcombo.

[6] SIEMENS,"Telecomunicación Digital",Tomo 2,"Tecnología crossconect y multiplexado", Marcombo.

[7] Hioki Warren, "Telecommunications", Second Edition, Prentice Hall,1995.

[8] Minoli Daniel, "Telecommunications Technology Handbook", Artech House 1991.

[9] Tanenbaum Andrew,"Redes de Ordenadores",Segunda Edición, Prentice Hall 1991.

[10] Comer Douglas, "Redes Globales de Información con Internet y TCP/IP",Tercera Edición ,Prentice-Hall.

[11] Black Ulises, "TCP/IP and Related Protocols", Mc Graw-Hill,1992.

[12] Hunt Craig, "Networking Personal Computers with TCP/IP", O'Reilly & Associates Inc.

[13] Ponzo R. y Reyes J.,"Redes de Datos, Capítulo 1",versión UC sin publicar.

[14] Ponzo R. y Reyes J.,Implementación de un Sistema de Supervisión y Administración para la Red de Datos de la Universidad de Carabobo, Trabajo especial de Grado presentado a la Universidad de Carabobo en 1998.

