

38
2ej.



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

CAMPUS
A R A G Ó N

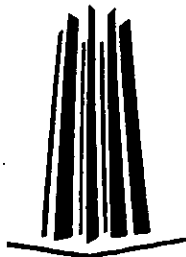
“CONECTIVIDAD EN REDES CON
ARQUITECTURAS TCP/IP, SNA Y OSI.”

TESIS PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN

P R E S E N T A

JUAN CARLOS LOPEZ ZUÑIGA.



ENEP ARAGON

MÉXICO, D.F. 1998.

TESIS CON
FALLA DE ORIGEN

258219



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

DERECHOS RESERVADOS © PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis está protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

DEDICATORIAS

A MIS PADRES Y HERMANAS.

Que siempre me brindaron todo su apoyo para conseguir lo que en un principio parecía inalcanzable...

A MI ESPOSA.

Quién con su comprensión, ayuda y confianza me permitió continuar con mis objetivos.

EN MEMORIA DE MI PADRE.

Quién siempre me brindo todo su apoyo, me dejó en el camino que yo seleccione libremente, a quién debo todo lo que he conseguido y a quién recordaré por siempre.

“CONECTIVIDAD EN REDES CON ARQUITECTURAS TCP/IP, SNA Y OSI.”

INTRODUCCIÓN	1
--------------	---

CAPÍTULO I. TIPOS DE REDES.

1.1. REDES.	3
1.1.1. RED DE COMPUTADORAS.	3
1.1.2. ELEMENTOS QUE COMPONEN UNA RED.	4
1.2. REDES DE ALTA VELOCIDAD.	7
1.2.1. RED SATELITAL.	7
1.2.2. RED DIGITAL INTEGRADA (RDI).	8
1.2.3. RED DIGITAL TERRESTRE.	9
1.2.4. RED DE LARGA DISTANCIA.	10
1.2.5. RED SATELITAL MULTIUSUARIO.	10
1.3. CLASIFICACIÓN DE LAS REDES.	10
1.3.1. CLASIFICACIÓN DE REDES POR SU ADMINISTRACIÓN.	11
1.3.2. CLASIFICACIÓN DE REDES POR SU SERVICIO.	12
1.3.3. CLASIFICACIÓN DE REDES POR SU TÉCNICA DE CONMUTACIÓN.	13
1.3.4. CLASIFICACIÓN DE REDES POR SU COBERTURA.	15
1.4. TOPOLOGÍA DE UNA RED.	17
1.5. MEDIOS DE TRANSMISIÓN.	20

CAPÍTULO II. MODELO DE REFERENCIA OSI.

2.1. NIVELES DEL MODELO DE REFERENCIA OSI.	26
2.1.1. NIVEL FÍSICO.	29
2.1.2. NIVEL DE ENLACE.	30
2.1.3. NIVEL DE RED.	31
2.1.4. NIVEL DE TRANSPORTE.	32
2.1.5. NIVEL DE SESIÓN.	34
2.1.6. NIVEL DE PRESENTACIÓN.	35
2.1.7. NIVEL DE APLICACIÓN.	36
2.2. CONECTIVIDAD DENTRO DE LAS CAPAS OSI.	37
2.3. CONECTIVIDAD EN EL PROTOCOLO X.25.	48

CAPÍTULO III. SISTEMAS SNA.

3.1. SISTEMAS SNA.	54
3.2. ARQUITECTURA SNA.	55
3.3. SESIÓN ENTRE UL-UL, PCSS-UF, UL-PCSS, UF-UF Y ENTRE PCSS-PCSS.	61
3.4 CONTROL DE TRAYECTORIA.	70
3.5. RUTA VIRTUAL .	76
3.6. TRANSMISIÓN SNA.	76

CAPÍTULO IV. PROTOCOLO TCP/IP.

4.1. SERVICIOS DE INTERNET.	82
4.1.1. NIVEL DE APLICACIÓN .	83
4.1.2. NIVEL DE RED.	84
4.1.3. CARACTERÍSTICAS DE TCP/IP.	85
4.2. ARQUITECTURA TCP/IP.	86
4.2.1. INTERCONEXIÓN DEL NIVEL DE APLICACIÓN	87
4.2.2. INTERCONEXIÓN DEL NIVEL DE RED.	88
4.2.3. PROPIEDADES DE INTERNET.	88
4.2.4. ARQUITECTURA DE INTERNET.	89
4.3. DIRECCIONES INTERNET.	90
4.4. PROTOCOLO ARP.	93
4.5. PROTOCOLO ICMP.	95
4.6. PROTOCOLO UDP.	98
4.7. PROTOCOLO TCP.	101
4.7.1. CARACTERÍSTICAS.	102
4.7.2. TELNET.	103
4.7.3. FTP.	105
4.8. PROTOCOLO SMTP.	107
4.9. CONECTIVIDAD EN TCP/IP.	108
4.9.1. LA CONECTIVIDAD ENTRE CAPAS DEL PROTOCOLO.	108
4.9.2. CONECTIVIDAD DE PROTOCOLOS.	113

CAPÍTULO V. ANALISIS COMPARATIVO ENTRE OSI, SNA Y TCP/IP.

5.1. ANÁLISIS COMPARATIVO ENTRE SNA Y TCP/IP.	116
5.2. ANÁLISIS COMPARATIVO ENTRE SNA Y OSI.	118
5.3. ANÁLISIS COMPARATIVO ENTRE TCP/IP Y OSI.	121
CONCLUSIONES.	127
BIBLIOGRAFÍA.	128

CONECTIVIDAD EN REDES CON ARQUITECTURAS TCP/IP, SNA Y OSI.

Objetivo:

Realizar un estudio de conectividad entre arquitecturas TCP/IP, SNA y OSI, describiendo sus características.

INTRODUCCIÓN

Durante la última década, las computadoras y las redes informáticas han producido en nuestra sociedad un impacto de enormes consecuencias; para solventar la necesidad de hacer más eficiente el uso de recursos de computación en organizaciones de todo tipo, surgieron las redes de cómputo como un elemento fundamental en el mundo actual, la tendencia continuará, incorporando tecnologías cada vez más novedosas para obtener mayor velocidad de transferencia y seguridad de los datos, así como la interoperabilidad de elementos de diversos fabricantes.

Una de las aplicaciones más interesantes de los sistemas computacionales radica en el área de las comunicaciones, ya que por medio de una red, puede conseguirse que todas las computadoras que se encuentran en diferentes lugares, intercambien información y datos, para que estén al alcance de todos.

Las redes de cómputo también significan conexión dentro de un marco de libertad como trabajar en el hogar o en la oficina, permiten al usuario trabajar mientras viaja, ya que el estilo de las redes es informal, abierto y despreocupado, donde se crea una atmósfera favorable a la inventiva y la creatividad.

Esto hace que la sociedad avance hacia el almacenamiento de información sin panel. Con ello podemos teclear datos y visualizarlos en la pantalla de una computadora; almacenar la información en un disco magnético o inclusive mandar los datos a una impresora. Entonces el empleo de redes es una de las nuevas aplicaciones más dinámicas de la tecnología en materia de

cómputo. La interconexión de computadoras permite que varias computadoras compartan los mismos recursos, que la información este disponible para más personas.

Como resultado podemos decir que las redes tienen la finalidad de transferir, compartir e intercambiar datos entre computadoras, es el intercambio de datos lo que permite funcionar a los múltiples servicios telemáticos que ya consideramos parte de nuestra vida.

Es necesario destacar que la interconexión se da entre redes que operan bajo medios heterogéneos a diferencia de la conectividad que se da en medios homogéneos dentro de una red que opera bajo el mismo protocolo de comunicación.

Después de un pequeño énfasis sobre las necesidades del intercambio de información entre usuarios, lo cual trajo consigo el surgimiento de las redes digitales, y el análisis de las principales Arquitecturas actuales de estas, son el objetivo de la presente TESIS, la cual consta de cinco capítulos, entre los que destacan el modelo de referencia OSI, la arquitectura SNA, y los protocolos de comunicaciones TCP/IP. Aquí cabe destacar que la relevancia de este trabajo es la Conectividad en OSI, SNA y TCP/IP. Definiendo la conectividad como: la habilidad que posee una red para poder mover un paquete de información desde un punto A, a un punto B dentro de una misma red de comunicación.

CAPÍTULO I. TIPOS DE REDES.

Objetivo:

Describir los tipos de redes de alta velocidad, así como sus distintas clasificaciones.

CAPÍTULO I. TIPOS DE REDES.

1.1. REDES.

Con los avances tecnológicos que se han tenido en los sistemas de comunicación; paralelamente se ha tenido la necesidad de intercambiar información entre computadoras, con un grado mayor de velocidad, rapidez y exactitud, lo cual trajo consigo la necesidad de que dos o más equipos terminales de datos pudieran compartir e intercambiar recursos. Después, se tuvo la necesidad de interconectar dos o más redes para acceder información entre estas, lo cual dio lugar a la interconectividad entre redes, esto en un principio solo se podía llevar a cabo entre redes del tipo homogéneo, es decir sólo se podía interconectar computadoras en Red cuyo Sistema Operativo fuera idéntico, hoy en día no es así, gracias a los protocolos de comunicación que establecen compatibilidad entre Sistemas Operativos diferentes. Durante los capítulos subsecuentes abordaremos el tema de Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP) que permite la comunicación entre redes y entre computadoras que posean distintas arquitecturas de hardware, y diferentes sistemas operativos. El protocolo TCP/IP se considera el protocolo de conexión de redes más completo y extendido disponible, y prácticamente cualquier sistema operativo moderno es compatible con él.

1.1.1. RED DE COMPUTADORAS.

El término red por lo general significa conjunto de computadoras y periféricos (impresoras, módem, graficadores, escaners, etc.) que se

interconectan por algún medio. La conexión puede ser directa (a través de un cable) o indirecta (a través de un módem). Los distintos dispositivos en la red se comunican entre sí utilizando un conjunto predefinido de reglas llamado protocolo.

La distancia entre los dispositivos de las redes, puede ser desde menos de un metro hasta miles de kilómetros, interconectados mediante algún medio de comunicación. Al diseño de una red, es decir los dispositivos reales y la forma de cómo se conectan unos con otros, se le denomina topología de red.

1.1.2. ELEMENTOS QUE COMPONEN UNA RED.

Los elementos que componen una red se abordan a continuación los cuales son el Servidor, Estaciones de trabajo, Medios de transmisión y el Sistema Operativo.

a) EL SERVIDOR .

El servidor es una computadora (mini micro- Main frame) en la que reside el software de red, (sistema operativo de red), además de que contiene todas las aplicaciones y archivos a compartir.

Su función es la de regular las comunicaciones de las computadoras que se encuentran conectadas a él, así como también de los equipos periféricos con los que se cuenta la red (impresora, plotter, etc.).

El servidor de archivos (Fs. File Server), cuenta por lo menos con un disco duro, en ocasiones se le adicionan otros de manera interna o externa; también debe contar con una tarjeta de red como mínimo. Se recomienda que el Servidor cuente con una capacidad mínima de memoria RAM de 4 Mbytes.

Los servidores pueden ser de dos tipos:

- Servidores dedicados. En estos servidores sólo residen las funciones de comunicación y control de la red.
- Servidores no dedicados. Estos servidores además de contar con las funciones anteriores, pueden trabajar como estaciones de trabajo.

Los servidores también se pueden clasificar a su vez de acuerdo a las funciones que estos desempeñan, de los cuales se conocen los siguientes:

- Los servidores de comunicaciones (front-end) y que se encargan de controlar los puertos, empaquetar la información, etc.
- Los servidores de base de datos, son en general todas las computadoras, minicomputadoras y microcomputadoras de almacenamiento de datos. En un proceso centralizado este debe tener una buena capacidad de disco.

b) ESTACIONES DE TRABAJO.

Se le denomina estación de trabajo a una computadora que se conecta al sistema de red y opera como parte de él, por lo general son microcomputadoras.

No puede generalizarse una sola máquina para este propósito, ya que depende de la aplicación que se le dará.

Desde la estación de trabajo se puede hacer uso de los programas de aplicación y las utilerías que residen en el servidor. No es necesario que las estaciones de trabajo cuenten con un disco duro.

c) MEDIOS DE TRANSMISIÓN.

Este es el encargado de llevar la información de un nodo a otro de la red, forma parte del hardware de la red, existe una variedad de estos Par Trenzado, Cable Coaxial, Micro Ondas y Fibra Óptica.

d) SISTEMA OPERATIVO.

El sistema operativo de red, es quien rige y administra los recursos (archivos, periféricos, usuarios, etc.) y lleva todo el control de seguridad de éstos, en pocas palabras es la columna vertebral de la red.

El sistema operativo constituye la parte medular dentro de la red. El hardware del sistema proporciona las trayectorias de datos y las plataformas de la red, pero el sistema operativo es el encargado de controlar todo lo demás. La funcionalidad de uso, el rendimiento, la administración, la seguridad de los datos, todo esto depende del sistema operativo.

El sistema operativo de la red se engloba en dos componentes básicos. El sistema operativo de la red del servidor mismo y el sistema de estación de trabajo; el sistema operativo del servidor de red se ejecuta dentro de la máquina

del servidor y procesa todos los servicios. El sistema operativo de red normalmente es proporcionado por el fabricante. Los programas propios de la estación de trabajo se ejecutan en ella, por medio de estos se establece la conexión con la red y el servidor, y controlan el flujo de las comunicaciones.

1.2. REDES DE ALTA VELOCIDAD.

Se utilizan como superportadora para manejar las comunicaciones de diferentes tipos de información de datos.

- FDDI/CDDI (Fiber Optic Distribution Interface) emplea fibra óptica (100Mbps).
- ATM (Asynchronous Transfer Mode) emplea fibra óptica (155 Mbps para multimedia).

La solución a esta heterogeneidad en protocolos se ha dado mediante el empleo de equipos activos como puentes (briges), ruteadores (routers), etc., que comunican redes entre sí a base de analizar tramas de diferentes protocolos emitidas por los dispositivos de la red y realizando operaciones de traducción, encapsulamiento o selección a otras redes involucradas.

1.2.1. RED SATELITAL.

Debido a las limitaciones propias del satélite, sus anchos de banda por usuario son reducidos (típicamente a 64 Kbps). Cuando se emplea la transmisión de datos debe utilizarse equipo complementario para compensar los

tiempos de demora de "salto" al satélite y evitar estado ocioso. Es conveniente este tipo de comunicación en localidades remotas donde no se dispone de vías terrestres de alta calidad. Si esta red es privada, su costo de mantenimiento es muy alto, por eso existen redes compartidas donde cada usuario emplea sólo parte del canal y una empresa administra centralmente la calidad de transmisión.

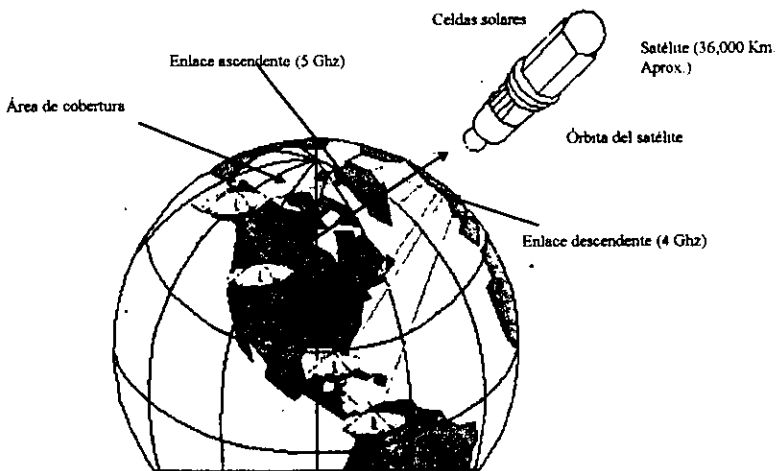


FIGURA 1.1. RED SATELITAL.

1.2.2. RED DIGITAL INTEGRADA (RDI).

Es un sistema muy flexible debido a la velocidad que ofrece de 2 Mbps, utiliza fibra óptica para los enlaces, lo que da alta seguridad y enlaza las principales ciudades en México con redes en otros países. Confiabilidad y eficiencia en el manejo de voz, datos e imágenes. Un sistema de comunicación digital que se transforma en el pasaporte comercial de los grandes usuarios. (ver Fig 1.2)

1.2.3. RED DIGITAL TERRESTRE.

La red digital terrestre esta formada por centrales de comunicación y medios de transmisión totalmente digitales de tecnología avanzada. Esta red permite establecer conexiones digitales desde el domicilio del usuario por medio de fibra óptica y radio de microondas urbanos manejando todo tipo de señales de telecomunicaciones en diversas velocidades. Además, a través de esta red es posible obtener servicios de troncales digitales, número de grupo de gran capacidad, marcación directa a extensión, circuitos digitales privados (nacionales e internacionales) sin necesidad de pasar por la red pública.

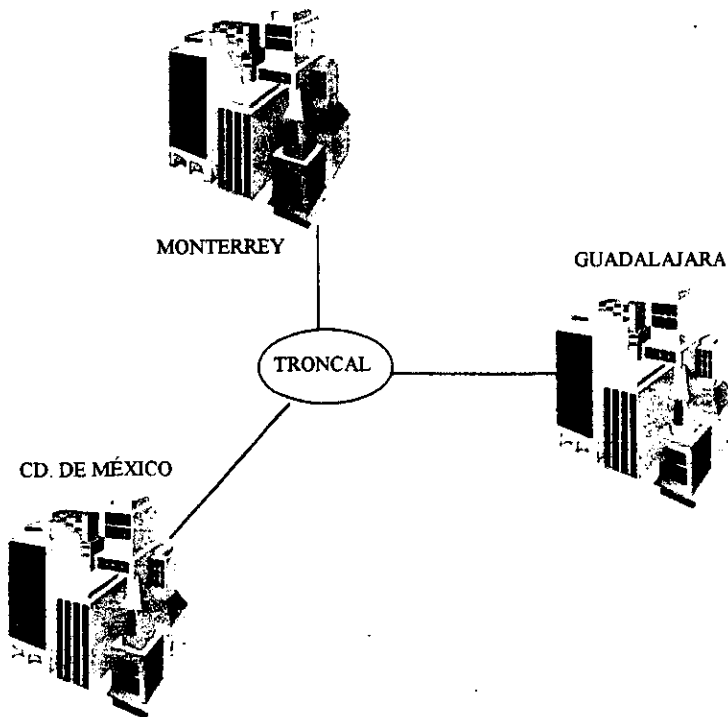


FIGURA 1.2. RED RDI.

1.2.4. RED DE LARGA DISTANCIA.

En el lugar donde se concentran los enlaces provenientes de centrales locales y los de centrales en otras ciudades. Debido a que las distancias de estas comunicaciones son grandes, el modo más eficiente de enviarlas es con el uso de enlaces de alta velocidad. Las salidas de las centrales en forma de tramas digitales de 2 Mbps son reprocesadas en equipos concentradores donde la información dirigida a una misma ciudad se encuentra en un mismo grupo de tramas, separándola así en canales destinados a otras ciudades. Una vez hecho esto, se multiplexa la información y según la importancia del segmento, o el riesgo del enlace, se hace la transmisión por fibra óptica o por radio digital.

1.2.5. RED SATELITAL MULTIUSUARIO.

Esta formada por estaciones satelitales de usuario que se ubican en los domicilios de los clientes que no son cubiertos por la red terrestre, es decir, los lugares geográficamente accidentados que la red terrestre no cubre pero que requieren servicios de comunicación por su importancia, como es el caso de las mismas. Para estos lugares, la red satelital cuenta con estaciones de control donde se enlaza a la red terrestre.

1.3. CLASIFICACIÓN DE LAS REDES.

Como ya hemos mencionado, una red se puede definir como la interconexión de dos o más equipos terminales de datos, de forma que puedan comunicarse entre sí y compartir recursos (programas, bases de datos,

periféricos, capacidades de procesamiento y almacenamiento, etc.), cada uno de los equipos terminales conectados a la red recibe el nombre de nodo de la red y las uniones de estas se denominan enlaces, los cuales se realizan mediante interfaz física y lógica.

1.3.1. CLASIFICACIÓN DE REDES POR SU ADMINISTRACIÓN.

Este tipo de redes se dividen en redes públicas y redes privadas las cuales se conectan en las capas de red bajas.

REDES PÚBLICAS.

Las redes públicas son las ofrecidas por una infraestructura gubernamental de cada país, por lo que tiene una cobertura nacional. Por lo general la velocidad de transmisión es de 10 Kbps, aunque pueden ser mayores de 64 Kbps. El número de usuarios que pueden conectarse a estas redes es limitado, por lo cual se utilizan nodos intermedios de concentración y/o conmutación para acceder a la red.

REDES PRIVADAS.

Una red privada se conforma por usuarios que pertenecen a una misma organización o corporación, para poderse comunicar entre sí. Una línea privada es un conductor que puede adquirirse en diferentes longitudes y tamaños. En términos de una arquitectura de red en capas, la línea opera en el nivel bajo

(nivel físico), como ejemplo de estas redes se puede citar las redes Bancarias, Pemex, etc. Para una línea privada con módem, no importa el protocolo bajo el cual se transmitan los datos.

1.3.2. CLASIFICACIÓN DE REDES POR SU SERVICIO.

Otra de las clasificaciones de las redes es por su servicio que brindan y estas son redes portadoras y redes de valor agregado o especializadas.

REDES PORTADORAS.

Las redes de datos portadoras sólo conducen señales de datos de un punto de origen a uno destino sin realizar algún cambio especial a la información que llevan, estas manejan una gama de velocidades que van desde 300 bps. Hasta los Mbps. Ejemplo de este tipo de redes son: TELEPAC en México, TRNSPAC en Francia y TELENET en Estados Unidos.

Las de valor agregado además de conducir la señal realizan algún cambio en la información de los usuarios ofreciendo servicios adicionales como el correo electrónico, almacenamiento y procesamiento remoto, compartición de bases de datos, conversión de protocolos, entre otros. Este tipo de redes son las de área local a nivel privado como las de INFONET, PEMEX, TELERESERVACIONES, etc.

REDES DE VALOR AGREGADO O ESPECIALIZADAS.

Por último las redes especializadas sólo ofrecen un único servicio, como sucede con la red TELEX. Este tipo de red se utiliza típicamente para empresas que requieren comunicaciones (generalmente datos) directas entre diferentes sucursales. Dependiendo de los requerimientos de una empresa, se utilizan redes satelitales, transmisión por microondas o red pública de alta calidad (RDI).

1.3.3. CLASIFICACIÓN DE REDES POR SU TÉCNICA DE CONMUTACIÓN.

Este tipo de redes comúnmente utilizan líneas telefónicas para la transmisión de información.

CONMUTACIÓN DE CIRCUITOS .

Para un uso menos frecuente, el circuito conmutado comparte los recursos de la red telefónica entre muchos usuarios y disminuye los costos entre ellos. El circuito constituye la operación normal del teléfono.

La mayor parte de las desventajas que se derivan de utilizar la red telefónica conmutada para comunicación de datos, surge a partir del hecho de que la red telefónica se ha optimizado para comunicaciones de voz. La voz humana tiene un rango de frecuencia que va de los 300 a los 3000 Hz. Por lo tanto, el cable de cobre de ancho de banda bajo es adecuado para la transmisión

de voz inteligible. Esto limita considerablemente el ancho de banda disponible para los datos. Debido a que las conexiones por circuito conmutado pasan a través del equipo de conmutación, por líneas de calidad más baja que las conexiones de línea privada, la calidad de la línea por circuito conmutado puede variar, lo que aumenta los errores de bits. Ejemplos de estas redes son: las telefónicas y las telex.

RED CONMUTADA.

Las señales a ser transmitidas viajan desde el punto de acometida hasta la central telefónica local. En el punto de acometida se puede tener un teléfono o un conmutador cuya salida puede ser por circuitos analógicos o digitales (como RDI). La señal telefónica funciona como un gran conmutador, donde los abonados son las extensiones y el enlace a otras centrales son las troncales.

CONMUTACIÓN DE PAQUETES.

A principios de los sesenta; Paul Baran de Rand Corporation introdujo el concepto de las comunicaciones conmutadas en paquetes. La propuesta de Baran aprovechó que en la transmisión de voz se intercalan espacios y pausa, que éstos podrían separar el contenido audible de la voz en paquetes.

El concepto era simple, cada paquete recibiría una dirección de destino y un número de secuencia hacia la red a través de diversas trayectorias o direcciones y se volvería a ensamblar en la secuencia original por el nodo de destino. Si hubiera interrupciones en la dirección o el nodo, cada uno de estos contará con un buffer o inteligencia suficiente para volver a orientar

dinámicamente los paquetes en una nueva dirección, sin pérdida de datos. Ejemplo de esta red es la TELNET.

1.3.4. CLASIFICACIÓN DE REDES POR SU COBERTURA.

La característica principal por la cuál se clasifican cada red es por la distancia o zona geográfica en la que operan cada una de estas. Otras de sus características son: su velocidad de transmisión, la aplicación direccionada de cada caso, los medios físicos de transmisión y el equipo involucrado.

REDES LAN.

Red de área local (local area network). La tecnología en que se basa empezó a adquirir interés a partir de los años setenta, y es en la actualidad uno de los sectores de más rápido crecimiento dentro de la industria de comunicación de datos. Lo que impulsa a las empresas hacia las redes locales es el incremento de la productividad.

La idea básica de una red local es facilitar a todos los equipos terminales de datos de una oficina o edificio. El acceso a otros dispositivos como son ordenadores, faxes, módems de alta velocidad, impresoras láser, y de color, archivos electrónicos y bases de datos. Una red local se configura de modo que proporcione los canales y protocolos de comunicación necesarios para el intercambio de datos entre ordenadores y terminales.

Estas redes locales proporcionarán los enlaces de transmisión de un edificio grande o un grupo de edificios cercanos. Estas redes proporcionan una

herramienta para la comunicación entre los componentes del grupo de trabajo a través del empleo del correo electrónico y otras aplicaciones. Los mensajes se envían instantáneamente a través de la red y pueden actualizarse tan pronto como ocurran los cambios.

Las redes locales como su nombre lo indica cubren distancias en un área determinada la cual no es muy grande esta puede ser desde algunos metros hasta varios kilómetros, pero generalmente no exceden más de 10 kms. y no utilizan otro protocolo de comunicación. La conexión de estas mismas usualmente es por medio de cables entrelazados, cables coaxiales y en algunos casos fibras ópticas.

Las redes LAN tienen velocidades de transmisión desde 1 Mbps hasta 100 Mbps con una tasa de error mínima, por lo cual proporciona o determina la confiabilidad de la red.

REDES MAN.

Las redes de área metropolitana (Metropolitan Area Network) generalmente son la que interconectan a las redes LAN. Estas principalmente cubren o enlazan ciudades, es decir, unen conjuntos de edificios u organizaciones. Las MAN's están facultadas para transportar simultáneamente y de manera integrada: voz, datos y vídeo, permitiendo comunicarse a un mayor número de estaciones entre si, a mayores velocidades que las que ofrecen las redes locales de datos. Las características generales de este tipo de red son: velocidades de transmisión mayores a 100 Mbps, gran cobertura de área geográfica (desde unos cuantos hasta cientos de Kms), soporte para un

gran número de estaciones, una tasa de error mínima y capacidad para cursar tráfico síncrono y asíncrono.

REDES WAN.

Red de área amplia (Wide Area Network). Las redes de gran extensión conectan ciudades, países y continentes, las cuales usan muchos tipos de medios de comunicación tales como: alambres telefónicos, cables submarinos, cables coaxiales, fibras ópticas, microondas y enlaces vía satélite. Estas redes usualmente son públicas. El propósito de estas es proporcionar una conexión fiable para todos sus usuarios independientemente de la aplicación de cada uno de ellos.

1.4. TOPOLOGÍA DE UNA RED.

Los enlaces pueden ser líneas telefónicas, líneas privadas, canales de satélite, etc. Cuando se dibuja un mapa de los enlaces de comunicación entre nodos, se tiene una topología de red. Los enlaces pueden ser de dos tipos básicos: físicos y virtuales.

Las redes usan enlaces virtuales para permitir el comportamiento de líneas físicas por programas de red múltiples y transferencia de datos. Se conoce también como topología: la forma física en la que es posible conectar estaciones de trabajo dentro de una LAN, en la actualidad las topologías son consecuencia del tipo de tarjeta de red que se utiliza, por ejemplo: Token-ring, Arcnet, etc.

TOPOLOGÍA EN ESTRELLA.

En este tipo de conexión el elemento central es el servidor (server) con sus periféricos. Se mantiene preguntando constantemente a cada estación de trabajo, mediante comunicación exclusiva y por turno si se desea transmitir información de ser afirmativo atiende la petición y, al terminar, prosigue su interrogatorio permanentemente con otra estación de trabajo. Todas las estaciones de trabajo están unidas mediante medios bidireccionales a un modulo o nodo central que efectúa las condiciones de comunicación. El nodo central asume además las labores de control y de gran parte de los recursos informáticos comunes.

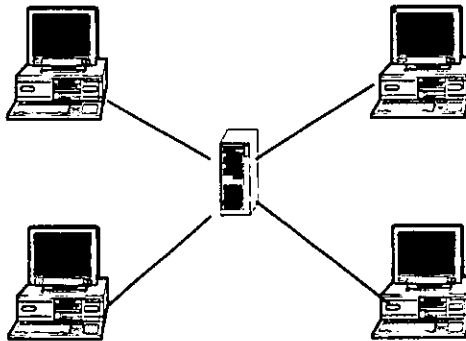


FIGURA 1.3. TOPOLOGÍA DE ESTRELLA.

TOPOLOGÍA DE BUS.

Esta conexión se considera la más sencilla de todas, donde las microcomputadoras incluyendo el servidor (server), están enlazados por un solo cable y la información viaja en ambos sentidos, por lo que es necesario

prevenir las colisiones. Dentro de la topología de bus distinguiremos entre bidireccional y unidireccional.

- Bus bidireccional. Se transmite en ambas direcciones por el mismo medio o medios conductores. La transmisión suele efectuarse por división espectral, asignación secuencial en el tiempo o menos frecuente, mediante transformadores híbridos o duplexores.
- Bus unidireccional. Con amplificadores sencillos permite alcanzar distancias mayores. A cambio requiere aumentar la longitud de cable utilizado.

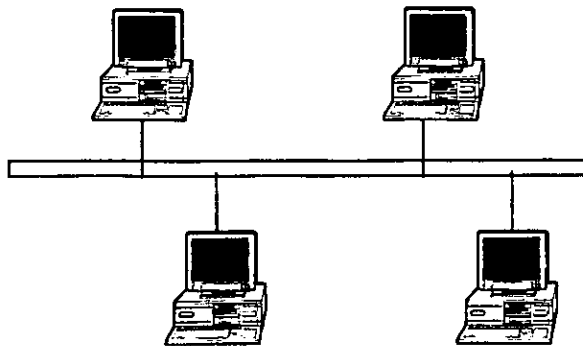


FIGURA 1.4. TOPOLOGÍA DE BUS.

TOPOLOGÍA EN ANILLO.

En este tipo de conexión la información viaja ordenadamente en un solo sentido, a través de un solo cable, describiendo un ángulo de 360° a cuyo anillo imaginario están conectadas en serie las estaciones de trabajo y el servidor. Una

señal llamada Token (receptáculo a modo de estafeta), va circulando por la red y va pasando por cada estación, si la primera resulta ser la solicitante, previa identificación entrega la información, de lo contrario la deposita en un “sobre cerrado”, para que este a su vez, la envíe a la siguiente estación, llevando la consigna de entregarla hasta encontrar la solicitante.

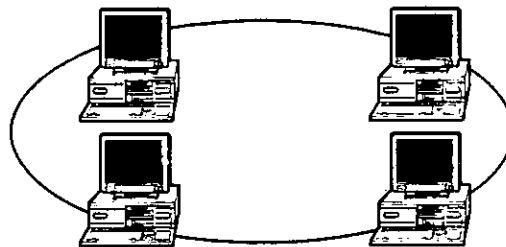


FIGURA 1.5. TOPOLOGÍA DE ANILLO.

1.5. MEDIOS DE TRANSMISIÓN.

Existen muchos medios de transmisión pero posteriormente solo se enunciarán los más comunes, que son, par trenzado, cable coaxial, fibra óptica, enlace vía microondas y enlace vía satélite.

PAR TRENZADO.

Consisten en alambres de cobre, a través de este par de hilos se transporta una conversación telefónica sin etapas de amplificación. Este sistema para la comunicación de datos es muy susceptible a interferencias de campos eléctricos y magnéticos que afectan gravemente a la transmisión.

CABLE COAXIAL.

Estos pueden transmitir a frecuencias mucho más altas que un par de alambres debido a que estos se produce el efecto *Skin*, que establece que las señales de alta frecuencia fluyen sobre la superficie de los hilos conductores ocasionando gran atenuación, consiste en un cilindro hueco de cobre u otro conductor cilíndrico que rodea a un conductor concéntrico de alambres simple, el espacio entre el cilindro hueco de cobre y el conductor interno se rellena con aislante que separa el conductor externo del interior, estos aislantes están espaciados a pocos centímetros.

Las ventajas del cable coaxial como medio de comunicación podemos resumirlas en las siguientes:

- Mayor número de canales de comunicación
- Bajos problemas de inducción de señales.
- Transmisión a mayores velocidades.

FIBRA ÓPTICA.

Los desarrolladores recientes en el campo de la tecnología óptica ha hecho posible la transmisión de información mediante pulsos de luz. Un pulso de luz puede utilizarse para indicar un bit de valor de 1, la ausencia de la luz puede utilizarse para indicar un bit de valor 0. La luz visible tiene una frecuencia de alrededor de 10^8 Mhz, por lo que el ancho de banda de un sistema de transmisión óptica presenta un potencial enorme.

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

Este sistema de transmisión tendría fugas de luz y prácticamente sería de poco uso, excepto si no existiera un principio de física. Cuando un rayo de luz pasa de un medio a otro, el se refracta (se desvía) en la frontera. En donde la cantidad de refracción dependerá de las propiedades de los medios. Por tanto el rayo de luz no se saldrá de la fibra óptica y lograra propagarse a lo largo de varios kilómetros sin tener, virtualmente ninguna pérdida.

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

Las fibras ópticas también forman la base de LAN, aunque su tecnología es más compleja.

ENLACE VÍA MICROONDAS.

Este tipo de sistemas de comunicación consiste en trasladar la información a bandas de frecuencias muy altas, permitiendo manejar grandes volúmenes de canales de voz (*información*) y a la vez no requieren que se tienda un cable como es el caso de cable coaxial. Esta transmisión se logra a través de la atmósfera entre satélites de microondas de las cuales cada satélite toma la señal y la transmite a la antena de microondas y esta la amplifica y la transmite a la siguiente antena de microondas.

El sistema es un método de transmisión alineado con precisión y de naturaleza visual el receptor debe ver al transmisor, estos repetidores cuentan con una antena transmisora y otra receptora, una antena típica para un equipo de microondas tiene unos tres metros de diámetro, aunque pueden ser más pequeñas para distancias más cortas.

ENLACE VÍA SATÉLITE.

Esto no es otra cosa que un sistema de microondas colocado en órbitas muy altas (de unos 35, 680 Kms). Sobre la superficie de la tierra generalmente sobre el ecuador, viajando a la misma velocidad que la rotación de la tierra, de esta manera puede transmitir señales a distancias mayores que las posibles sobre la superficie terrestre debido a que la cobertura, montañas y otros obstáculos de la tierra bloquean la transmisión de microondas sobre línea visuales entre las torres terrestres.

CAPÍTULO II. MODELO DE REFERENCIA OSI.

Objetivo:

Describir la conectividad con el modelo de referencia OSI, así como sus características y niveles.

CAPÍTULO II. MODELO DE REFERENCIA OSI.

A continuación se mostrará un breve resumen acerca del modelo de referencia OSI así como la importancia de sus capas, como opera cada una de ellas y la conectividad dentro de este sistema, por otra parte se estudiará la conectividad dentro de la recomendación X.25 y la similitud con el modelo de referencia OSI.

Actualmente las redes de computadoras están diseñadas de una forma estructurada y modular que permite una fácil manipulación en lo que se refiere a mantenimiento y actualización.

La mayoría de las redes se organizan en una serie de capas o niveles, con objeto de reducir la complejidad de su diseño. Cada uno de estos niveles se construye sobre su predecesor. El número de niveles, el nombre, contenido y función de cada uno varían de una red a otra; sin embargo, en cualquier red, el propósito de cada nivel es el mismo a saber: ofrecer ciertos servicios a los niveles superiores, liberándolos del conocimiento detallado sobre cómo se realizan dichos servicios.

El nivel n en un sistema conversa con el nivel n de otro sistema. El conjunto de reglas y convenciones usado en esta conversación se denomina protocolo de la capa n . En la figura 2.1, se muestra el caso para una red de siete niveles. A los entes que forman capas correspondientes en sistemas diferentes se les denomina procesos pares (peer-to-peer). En otras palabras, mediante el uso del protocolo se comunican entre sí los procesos pares.

Cada nivel pasa la información de datos y control al nivel inmediato inferior, esto se continúa sucesivamente hasta que se alcanza el nivel más bajo de la estructura. En este nivel se ubica el medio físico, a través del cual se realiza la comunicación real. En la figura 2.1 se muestra mediante líneas punteadas, la comunicación virtual, en tanto que las líneas solicitadas indican la comunicación física.

Entre cada par de niveles adyacentes existe una interfaz, la cual define los servicios y operaciones primarias que el nivel inferior ofrece al superior. Cuando los diseñadores de redes deciden el número de niveles a incluir en la red, así como lo que cada uno de ellos deberá hacer, una de las actividades más importantes es definir claramente las interfaces entre niveles. El mantener un conjunto de funciones bien definidas para cada nivel y diseñar clara y limpiamente las interfaces, logra dos cosas muy importantes: minimizar la cantidad de información que debe pasar entre niveles y hacer más simple la sustitución de un nivel por otro distinto que realiza la misma función (por ejemplo que todas las líneas telefónicas se reemplacen por canales satelitales). Como se ve lo que se necesita del nuevo nivel es que ofrezca el mismo conjunto de servicios al nivel superior contiguo, tal como lo hacía la anterior realización.

Al conjunto de niveles y protocolos se llama arquitectura de red, y las características de modularidad proporcionan las facilidades de apertura de la misma. Las especificaciones de ésta deberán contener la información suficiente que le permita al diseñador escribir un programa o construir el hardware correspondiente a cada nivel, y que siga en forma correcta el protocolo apropiado. Los detalles de realización y las especificaciones de las interfaces,

no forman parte de la arquitectura, porque se encuentran escondidas en el interior de la máquina y no son visibles desde el exterior. Incluso, no es necesario que las interfaces de todas las máquinas en una red sean iguales, basta con que cada una de las máquinas utilice correctamente todos los protocolos.

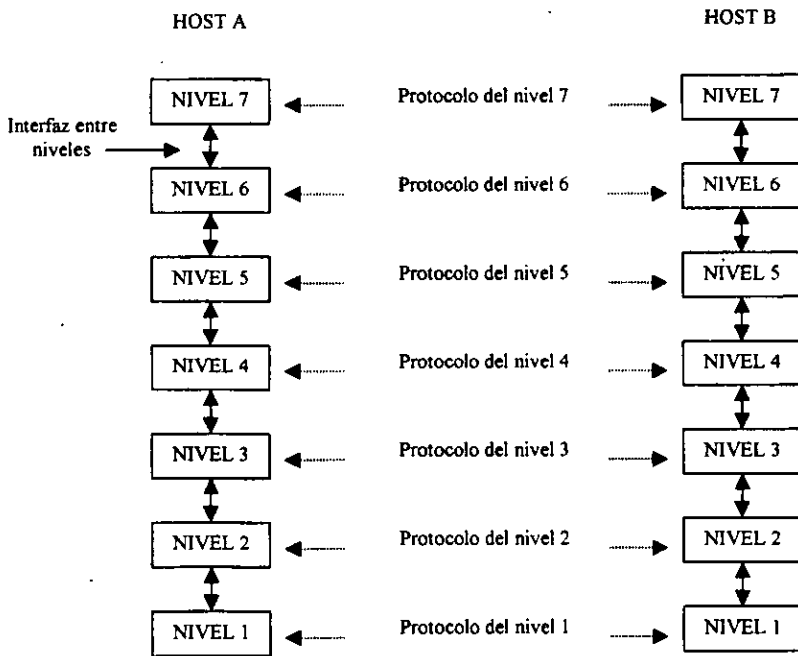


FIGURA 2.1. ARQUITECTURA DEL MODELO OSI.

2.1. NIVELES DEL MODELO DE REFERENCIA OSI.

En la figura 2.2. se muestra un modelo, basado en una propuesta desarrollada por la Organización Internacional de Estándares (ISO), como un primer intento de normalización internacional de varios protocolos. A este

modelo se le conoce como Modelo de referencia OSI (Open Systems interconnection) de la ISO, y se refiere precisamente a la conexión de sistemas heterogéneos, los cuales deben establecer comunicación con otros distintos. El modelo OSI está constituido por siete niveles, y estos fueron los principios para establecerlos:

- 1. Se crea un nivel en situaciones en donde se necesita un estrato diferente de abstracción.*
- 2. Cada nivel debe efectuar una función bien definida.*
- 3. La función que cada nivel realiza, debe seleccionarse con la intención de definir protocolos normalizados internacionalmente.*
- 4. Los límites de los niveles deberán seleccionarse tomando en cuenta la minimización del flujo de información a través de las interfaces.*
- 5. El número de niveles debe ser lo suficientemente grande para que funciones diferentes no tengan que ponerse juntas en la misma capa y, por otro lado, también debe ser lo suficientemente pequeños para que su arquitectura no sea difícil de manejar.*

La figura 2.2 incluye un ejemplo de arquitectura de comunicaciones por niveles, el modelo de referencia para la interconexión de sistemas abiertos (OSI), aprobado en 1983 como estándar internacional por la Organización Internacional de Estándares (ISO), y por CCITT. Las tres capas inferiores de esta arquitectura proporcionan la capacidad de interconexión en red, mientras

que las cuatro superiores llevan a cabo, en cada extremo, el procedimiento que se requiere para presentar los datos al usuario final de manera apropiada y reconocible.

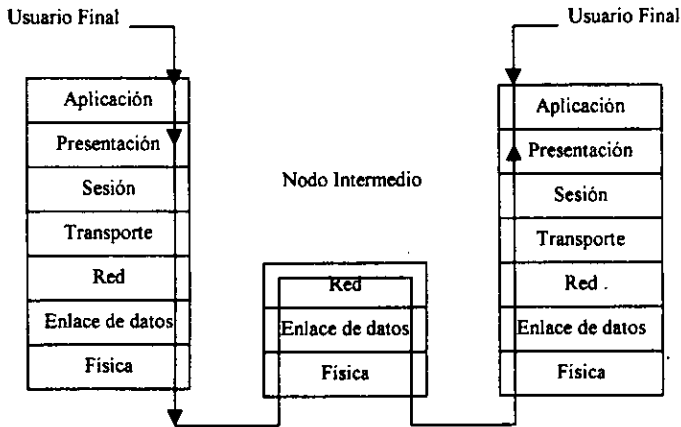


FIGURA 2.2. ARQUITECTURA OSI DE SIETE CAPAS.

Se distinguen dos grupos de niveles, el conjunto de niveles bajos y el de niveles más altos, los niveles de red, son usados por los nodos de la red para dirigir los datos de un usuario final (mostrado como una computadora central) a otro. Los niveles más altos mostrados se encargan de proporcionar los datos a los usuarios finales de manera que estos puedan reconocerlos y usarlos. Estos niveles más altos residen en las computadoras. Las computadoras centrales que están fuera de la red propiamente dicha contienen ambos niveles, los más altos y los más bajos (de red). En algunas redes (ARPAnet es un ejemplo) las computadoras centrales sólo tienen los niveles más altos; los niveles de red únicamente aparecen en los nodos de red. En algunos casos los nodos de comunicación a los que se muestran conectados las computadoras centrales son en realidad parte de éstos. Los tres casos se presentan en la práctica,

(recuérdese “nodo intermedio” podría ser una red, o una serie de redes, en situaciones más complejas que involucren interconexión de redes).

A continuación se estudiarán cada uno de los niveles, comenzando por el inferior, debe considerarse que el Modelo OSI, por sí mismo, no es una arquitectura de red, dado que no especifica, en forma exacta, los servicios y protocolos que se han de utilizar en cada uno de los niveles. Sólo indica lo que cada nivel debe hacer. Sin embargo, La ISO también ha generado normas para todas las capas o niveles, que aunque no forman parte de modelo son reconocidas como normas internacionales independientes.

2.1.1. NIVEL FÍSICO.

El nivel físico se ocupa de la transmisión de bits a lo largo de un canal de comunicación. Su dueño debe asegurar que cuando un extremo envía un bit con valor, éste se reciba exactamente como un bit con ese valor en el otro extremo.

Preguntas comunes son; cuantos volts debe usarse para representar un bit de valor 1 ó 0; Cuantos microsegundos debe durar un bit; la forma de establecer la conexión inicial y como interrumpirla cuando ambos extremos terminan su comunicación; y aún, cuantas puntas terminales (pines) tiene el conector de la red y cual es el uso de cada una de ellas. Los problemas de diseño que se consideran aquí son los aspectos mecánicos, eléctricos, de procedimientos de interfaz y el medio físico de transmisión, que se encuentran bajo el nivel físico.

2.1.2. NIVEL DE ENLACE.

La tarea primordial del nivel de enlace consiste en partir de un medio de transmisión común y corriente, y transformarlo en una línea sin errores de transmisión para el nivel de red. Esta tarea la realiza al hacer que el emisor fragmente la entrada de datos en tramas de datos (generalmente de algunos cientos de bytes de longitud) y las transmita en forma secuencial, procesando adicionalmente las tramas de aprobación, devueltas por el receptor. Como la capa física básicamente acepta y transmite un flujo de bits sin tener en cuenta su significado o trama, esto se lleva a cabo mediante la inclusión de un patrón de bits especial tanto al inicio como al final de la trama. Si estos patrones de bits pueden aparecer entre los datos, debe tenerse un cuidado especial para evitar cualquier confusión al respecto.

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

Otro de los problemas que aparecen en el nivel de enlace (y también en la mayoría de los niveles superiores) es el referente a como evitar que un transmisor muy rápido saturar con datos a un receptor lento. Se debe emplear un

mecanismo de regulación de tráfico que permita que el transmisor conozca el espacio de memoria que en ese momento tiene el receptor. Frecuentemente, y por conveniencia, los procedimientos de regulación de flujo y control de errores se tratan en forma conjunta.

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

2.1.3. NIVEL DE RED.

El nivel de red se ocupa del control de la operación de subred. Un punto de mucha importancia en su diseño, es la terminación sobre como enrutar los paquetes del origen al destino. Las rutas pueden basarse en tablas estáticas que reflejan cómo se encuentran cableadas las diferentes vías en la red y que difícilmente pudieran cambiarse. También pueden determinarse al inicio de cada conversación, por ejemplo en una sesión de terminal, por último, puede ser de tipo dinámico, determinándose en forma diferente para cada paquete, en función de la carga de tráfico actual de la red.

Si en un momento dado hay demasiados paquetes en las subred, ellos mismos se pueden obstruir mutuamente dando lugar a un cuello de botella. El control de tal congestión depende de la capa de red.

En ocasiones se introduce una función de contabilidad en la capa de red. El software debe saber, por lo menos, cuántos paquetes o caracteres o bits se

envían a cada usuario, con objeto de producir información de facturación. También puede surgir otros problemas cuando un paquete tenga que desplazarse de una red a otra para llegar a su destino. El direccionamiento utilizado en la segunda red puede ser diferente al empleo en la primera. La segunda podría no aceptar el paquete en su totalidad, por ser demasiado grande. Los protocolos podrían ser diferentes, etcétera. En todo caso, la responsabilidad para resolver problemas de interconexión de redes heterogéneas recae en el nivel de red.

2.1.4. NIVEL DE TRANSPORTE.

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

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

El nivel de transporte determina que tipo de servicio debe dar al nivel de sesión, y en última instancia a los usuarios de la red. El tipo más popular de conexión de transporte corresponde al canal punto a punto sin error, por medio del cual se entregan los mensajes aislados sin garantizar el orden de distribución y la difusión de mensajes a destinos múltiples es otra posibilidad de servicio de transporte. El tipo de servicio se determina cuando se establece la conexión.

El nivel de transporte es uno del tipo origen-destino o extremo; es decir, que un programa en la máquina origen lleva una conversación con un programa parecido que se encuentra en la máquina destino. Para tal efecto utiliza los encabezados de los mensajes y los mensajes de control. Los protocolos de los niveles inferiores son entre cada máquina de origen y destino. Sin embargo, para la técnica de conmutación de paquetes, existe un criterio, que cada vez cobra más consenso, que le concede reconocimiento al nivel de red en cuanto a que efectúa comunicación extremo a extremo, desde el enfoque de la subred, desde un nodo origen hasta un nodo destino.

El encabezado correspondiente del nivel de transporte, es particularmente útil, para cuando tomemos en la red máquina multiproceso, lo que significa que se tendrán múltiples conexiones entrando y saliendo de algún host, el cual necesitará algún método para determinar qué mensaje pertenece a qué conexión.

Además de multiplexar varios flujos de mensajes en un canal, el nivel de transporte se debe ocupar del establecimiento y liberación de conexiones a través de la red. Para esto se requiere un mecanismo de denominación, tal que

un proceso en máquina tenga manera de describir con quién desea conversar. Adicionalmente debe tener un mecanismo de control de flujo de información, de tal forma que un host muy rápido no pueda desbordar a otro más lento, cabe mencionar que el control de flujo aquí es diferente a aquel de nivel de red.

2.1.5. NIVEL DE SESIÓN.

El nivel de sesión permite que los usuarios de máquinas diferentes puedan establecer sesiones entre ellos. A través de una sesión se puede llevar a cabo un transporte de datos ordinario, tal como lo hace el nivel de transporte, pero mejorando los servicios proporcionados y que algunas aplicaciones pueden utilizar. Una sesión podría permitir a un usuario tener acceso a un sistema de tiempo compartido a distancia, o transferir un archivo entre dos máquinas.

Uno de los servicios del nivel de sesión consiste en manejar el control del diálogo. Las sesiones permiten que el tráfico vaya en ambas direcciones al mismo tiempo, o bien, en una sola dirección en un instante dado. Si este es el caso entonces, el nivel de sesión ayudará al seguimiento de quien tiene el turno.

El manejo de testigo es otro servicio relacionado con el nivel de sesión. Para el caso de algunos protocolos resulta esencial que ambos lados no traten de realizar la misma operación en el mismo instante. Para manejar estas situaciones, el nivel de sesión proporciona testigos que pueden ser intercambiados, y solamente el extremo con el testigo puede realizar la operación crítica.

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

2.1.6. NIVEL DE PRESENTACIÓN.

El nivel de presentación realiza ciertas funciones que a menudo se necesitan y para lo cual conviene más tener una solución general, que dejar que cada uno de los usuarios resuelva los problemas. En particular y, a diferencia de los niveles inferiores, que únicamente están interesados en el movimiento fiable de bits de un lugar a otro, el nivel de presentación se ocupa de los aspectos de sintaxis y semántica de la información que se transmite.

Un último ejemplo típico de servicio del nivel de presentación es lo relacionado con la codificación de datos conforme a previos acuerdos. La mayor parte de los programas de usuario no intercambian hileras de bits aleatorios, sino, más bien, cosas como nombres de personas, datos, cantidades de dinero, y facturas. Estos artículos están representados por hileras de caracteres, números enteros, números de punto flotante, así como por estructuras de datos constituidas por varios elementos más sencillos. Las

computadoras pueden tener diferentes códigos para representar las hileras de caracteres (ASCII y EBCDIC), enteros (complemento a uno, complemento a dos), etc. Para hacer posible la comunicación de computadoras con diferentes representaciones, las estructura de los datos que se van a intercambiar pueden definirse en forma abstracta, junto con alguna norma de codificación establecida. El trabajo de manejar estas estructuras de datos abstracto y la convención de representación utilizada en el interior de la computadora a la representación normal de la red, se lleva a través del nivel de representación.

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

2.1.7. NIVEL DE APLICACIÓN.

El nivel de aplicación contiene una variedad de protocolos que se necesitan frecuentemente. Por ejemplo, hay cientos de tipos de terminales incompatibles en el mundo. Piense en la situación de algún programa editor orientado a pantalla, que se desea que trabaje en una red con diferentes tipos de terminales, cada una de ellas con distintas formas de distribución de pantalla, de secuencias de escape para insertar y borrar texto, de movimiento de cursor, etc. Una forma de resolver este problema es definiendo una terminal virtual de red abstracta, con la cual puedan tratar el programa editor y probablemente algunos otros. Con objeto de transferir funciones de la terminal virtual de una red a una terminal real, se debe escribir un software que permita el manejo de

cada tipo de terminal. Por ejemplo, si el editor mueve el cursor de la terminal virtual al extremo superior izquierdo de la pantalla, dicho software debe emitir una serie de comandos que hagan lo propio en la terminal real. El software completo de la terminal virtual se encuentra en el nivel de aplicación.

Otra función del nivel de aplicación puede ser la transferencia de archivos. Distintos sistemas de archivo tienen diferentes convenciones para denominar un archivo, así como diferentes formas para representar las líneas de texto, etc. La de éstas y otras incompatibilidades. Este trabajo, así como el correo electrónico, la entrada de trabajo a distancia, el servicio de directorio, y otros servicios tanto de propósito general como específico, también pueden corresponder al nivel de aplicación.

2.2. CONECTIVIDAD DENTRO DE LAS CAPAS OSI.

Se habrá notado que muchos de los términos usados en la descripción de los diversos niveles OSI parecen duplicados de capa. Por tanto, un nivel representativo ofrece un conjunto de servicios a la entidad de la capa superior. La capa superior se llama *usuario del servicio*; la capa inferior, *proveedor del servicio*. En el caso orientado a conexión, estos servicios incluyen condiciones para el establecimiento y la liberación de la conexión, además de la transferencia de datos. Estas tres fases secuenciales de operación de los protocolos en un nivel dado se muestran de manera esquemática en la figura 2.3. En ella se identifican dos sistemas, A y B, que desean comunicarse. Las entidades de la misma categoría en cada nivel de la arquitectura OSI primero deben establecer una conexión, luego transferir los datos como se requiere finalmente cerrar o liberar la conexión.

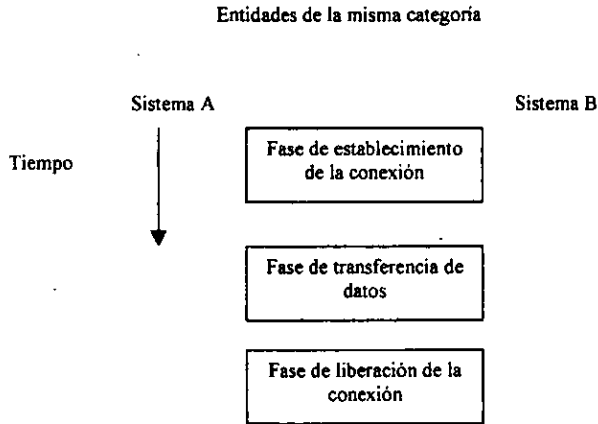


FIGURA 2.3. TRES FASES DE UNA COMUNICACIÓN EN UNA CAPA, EN UNA TRANSMISIÓN ORIENTADA A CONEXIÓN.

En la fase de establecimiento de la conexión, las dos entidades de igual categoría en cada extremo de la conexión negocian el conjunto de parámetros que se deben usar durante esta fase, es necesario detectar los errores y ejercer alguna forma de control de ellos. Esto constituye otro conjunto de servicios que ofrece el proveedor. También se pueden proporcionar otros servicios durante la transferencia de datos. Los bloques o unidades de datos generalmente deben estar dispuestos en secuencia numerada. Se deben segmentar los bloques o, por el contrario, encadenarse para incrementar su tamaño. Se puede ejercer control de flujo para evitar que una entidad transmisora en un extremo de la conexión sobresature a la entidad receptora del otro extremo. Se puede usar la multiplexación o división para mejorar las características del rendimiento y del tiempo de retardo (calidad de servicio). Se puede utilizar la sincronización. Se puede tener transmisión dúplex. En el último caso se debe pasar una señal

(permiso para transmitir) de una entidad a otra. Los datos se pueden transmitir normalmente o de una manera expandida.

Los requerimientos específicos y los servicios difieren del nivel, pero los conceptos son similares. Por tanto, los errores en el nivel de enlace de datos generalmente se refieren a errores en la secuencia de numeración; en un nivel más alto se podría referir a una falla en la red o a una desconexión. Eso lleva a un concepto de unificación, aquel en que el nivel N de la arquitectura proporciona un servicio al nivel $N+1$ arriba de él. Puede existir concepto OSI. Si corresponden a entidades en sistemas diferentes, los protocolos de la categoría gobiernan su cooperación. Las líneas discontinuas con flechas que conectan dos entidades en el mismo nivel (N) dan un ejemplo de entidades en diferentes sistemas comunicándose por medio de protocolos de la categoría; el protocolo de presentación en el nivel de presentación, el protocolo de transporte en el nivel de transporte, y así sucesivamente.

Las entidades N en el nivel N dan servicio a las entidades ($N+1$) en el nivel superior ($N+1$), por tanto, la entidad N es la proveedora del servicio a la entidad ($N+1$), usuaria del servicio. Ya se han mencionado ejemplos de tales servicios al describir cada uno de los niveles OSI incluyendo control de errores, control de flujo, multiplexación y segmentación. La figura 2.4. muestra dos entidades en el nivel ($N+1$) que comparten los servicios de una sola entidad en el nivel N . Esto podría corresponder a una conexión multiplexada. La misma entidad N del nivel N se muestra segmentando su conexión entre dos entidades en el nivel ($N+1$). Los servicios del nivel N al nivel ($N+1$) se dan en la interfaz entre los niveles, en los llamados puntos de acceso al servicio deben establecer conexiones entre entidades al mismo nivel. Por tanto, como uno de sus

servicios, el nivel N . Las conexiones pueden ser de uno a uno, de uno a muchos (comunicaciones de difusión), o de muchos a uno.

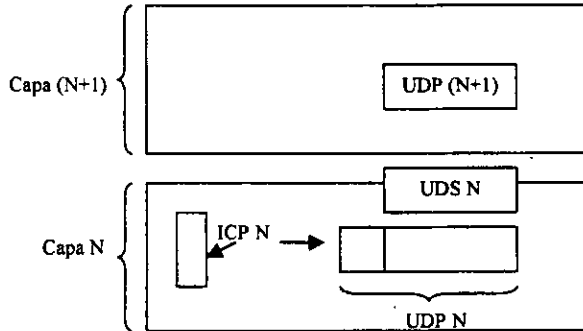


FIGURA 2.4. UNIDADES DE DATOS EN LA ARQUITECTURA OSI.

Los datos que se transfieren entre unidades iguales contienen datos del usuario, que se pasan del nivel superior, e información de control de protocolo que se añade al nivel en cuestión (véase fig. 2.4.). UDP significa unidades de datos de protocolo (PDU un inglés), el bloque de datos que contiene información de control de protocolos ICP (en inglés, PCI), añadida al nivel en cuestión, como se muestra, y datos del usuario, que se originan en la capa superior. La $UDP (N+1)$, al cruzar la interfaz entre los niveles $(N+1)$ y N , se hace corresponder con la unidad de datos del servicio N , $UDS N$, como se muestra. Esta correspondencia puede ser uno a uno como se muestra, o si las $UDS N$ son demasiado largas, se pueden segmentar para formar varias $UDS N$ después de añadir información de control apropiada, $ICP N$. También es posible concatenar unidades de datos para formar unidades de datos más largas.

La longitud de la $UPD N$ transmitida entre las entidades de categoría N se negociaría durante la fase de conexión. Cuando una $UDP N$ llega a su

destino, la entidad de categoría N en el nivel N en el destino, se procede a quitarle el encabezamiento, el ICP N , antes de enviarse al nivel $(N+1)$ del destino. También se podría invertir la segmentación o concatenación.

Además de las unidades de datos del protocolo N que se intercambian entre unidades de la misma categoría en el nivel N , se intercambia información de control de interfaz N entre una entidad $(N+1)$ y una entidad N en el nivel inferior para coordinar su operación. El control de flujo de las unidades de datos se puede ejercer entre entidades de la misma categoría en el mismo nivel, así como entre unidades $(N+1)$ y N a través de la interfaz en el punto de acceso al servicio.

Siguiendo con el concepto de entidades N que ofrecen un servicio a los usuarios, las entidades $(N+1)$, OSI ha establecido estándares sobre el uso de cuatro primitivas básicas de servicio a cada nivel de la arquitectura para proporcionar la interacción entre el usuario del servicio en un nivel y el proveedor del servicio en un nivel y el proveedor del servicio en el nivel inferior. Estas primitivas de servicio ofrecen los elementos básicos para definir el intercambio entre usuarios del servicio; los cuatro tipos son solicitud, indicación, respuesta y confirmación. No necesariamente se usan los cuatro tipos en los diferentes niveles; no se pueden usar todos en las diferentes fases de un intercambio entre entidades iguales en un nivel dado. Las cuatro primitivas se presentan de modo esquemático en la figura 2.5. algunas de estas primitivas, o todas, se puede usar en cada una de las tres fases del proceso de comunicación. Más adelante se darán ejemplos.

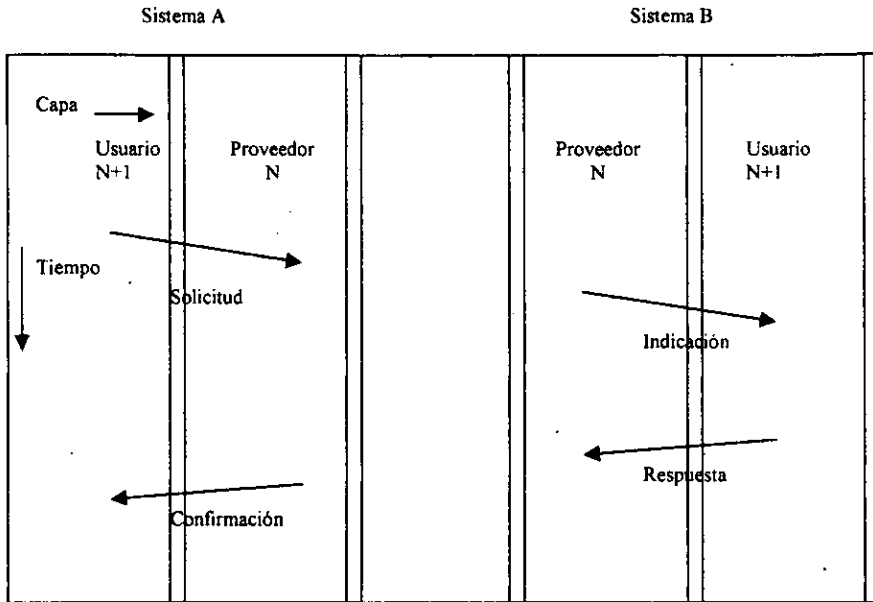


FIGURA 2.5. CUATRO PRIMITIVAS BÁSICAS DE LA ARQUITECTURA OSI.

Nótese en la figura 2.5. que la *solicitud* es emitida por un usuario del servicio en un nivel ($N+1$) dado en el sistema A, para invocar un procedimiento del protocolo del servicio del proveedor en el nivel N inferior, lo que da como resultado un mensaje del nivel N , que se envía como una UDP N (o conjunto de UDP N) al sistema B. La recepción de la UDP N en el nivel N del sistema B a veces causa la emisión de una primitiva de *indicación* por parte del proveedor del servicio en ese nivel. Esta primitiva de indicación se emite en cualquiera de estos dos casos: puede indicar que el usuario del servicio en B está a punto de invocar un procedimiento del protocolo en su nivel ($N+1$) o que el proveedor de servicio en el nivel N invocó un procedimiento en el punto de acceso del servicio de la categoría. En resumen, la primitiva de indicación en el sistema B

se emite, en este ejemplo, como respuesta a la primitiva de solicitud emitida antes en el sistema A.

Como se muestra en la figura 2.5., el proveedor del servicio emite la primitiva de *respuesta* en el nivel $(N+1)$ del sistema B como respuesta a la indicación que aparece antes en el punto de acceso al servicio entre los niveles N y $(N+1)$ del sistema B. Esta primitiva de respuesta es una directiva al protocolo del nivel N para completar el procedimiento invocado previamente por la primitiva de indicación. El protocolo en el nivel N genera una unidad de datos del protocolo que se transmite a través de la red, aparece en nivel N en el sistema A y resulta en una primitiva de *confirmación* emitida por el proveedor del servicio en el sistema A. Esto lleva a la culminación, en el punto de acceso al servicio entre N y $(N+1)$ en el sistema A, del procedimiento invocado previamente por la solicitud en el punto.

Para resumir, una solicitud del usuario del servicio en el nivel $(N+1)$ del sistema A resulta, en un momento posterior, en una primitiva de indicación dirigida al usuario de la categoría del servicio en el sistema B. Este usuario consta con una primitiva de respuesta que termina por alcanzar al usuario que indica el servicio en el sistema A como una primitiva de confirmación.

Como ejemplo concreto de la posibilidad de aplicación de estas primitivas, considérese el nivel de enlace de datos. La segunda capa de la arquitectura OSI. Su propósito es ofrecer servicios al nivel de la red. Estos servicios se agrupan en las tres fases descritas antes y mostradas en la figura 2.4: establecimiento, transferencia de datos y liberación. En la notación de los niveles de red y de enlace de datos, los servicios de establecimiento se usan

para llevar a cabo una conexión lógica entre dos entidades de la red en cualquier extremo del enlace, los servicios de transferencia de datos aseguran que las unidades de datos de la red (los *paquetes* a que se ha hecho referencia) lleguen correctamente y en secuencia al otro lado del enlace, una vez que se ha establecido. Los servicios de liberación y terminación manejan la liberación de la conexión lógica una vez concluida la transferencia de datos. Para simplificar, el texto se circunscribe al uso de las primitivas en tales fases el protocolo HDLC. El protocolo X.25 incorpora también una subclase de este protocolo como su protocolo de enlace de datos.

Se distinguen y etiquetan tres diferentes categorías de las cuatro primitivas básicas, que corresponden a cada una de las tres fases de la comunicación en ese nivel. En la figura 2.3. aparecen en un intercambio común a través del enlace. Nótese el uso de los términos solicitud de CONEXIÓN, solicitud de DATOS, solicitud de DESCONEXIÓN con los modificadores correspondientes usados con cada una de las otras tres primitivas. Hay modificadores similares en cada una de las capas en la arquitectura OSI en las que se usan estas primitivas.

HDLC incorpora varios modos de operación y sus correspondientes clases de procedimiento. El modo deseado en particular, que en este ejemplo es un modo balanceado asíncrono apropiado para los protocolos de enlace de datos en ambos extremos del enlace punto a punto, se transporta en la primitiva solicitud de CONEXIÓN. Por lo general, las primitivas de conexión llevan parámetros de operación (indica con quién se tiene que hacer la conexión, la calidad de servicio requerida, etc.). En el caso de HDLC, se usan números secuenciales para numerar las unidades de datos del protocolo de enlace de

datos durante la fase de transferencia. Hay un modo normal de numeración secuencial con módulo 8 y un modo extendido de numeración secuencial con módulo 128. El modo de numeración deseado también debe aparecer como un parámetro puesto en la primitiva solicitud de CONEXIÓN.

Después de recibir y procesar la primitiva solicitud de CONEXIÓN, el protocolo de enlace de datos en el sistema A causa que se emita una unidad de datos del protocolo de enlace de datos para transmisión a B, el otro extremo del enlace HDLC incorpora varias unidades de control de datos dentro de su repertorio de operación. Una de ellas, llamada unidad de datos de establecimiento del Modo Balanceado Asíncrono (SABM, *Set Asynchronous Balanced Mode*), se aplica aquí al modo de operación, y se muestra transmitiéndose a la estación B. Otras unidades de datos de control se usan para establecer los otros modos de operación de HDLC.

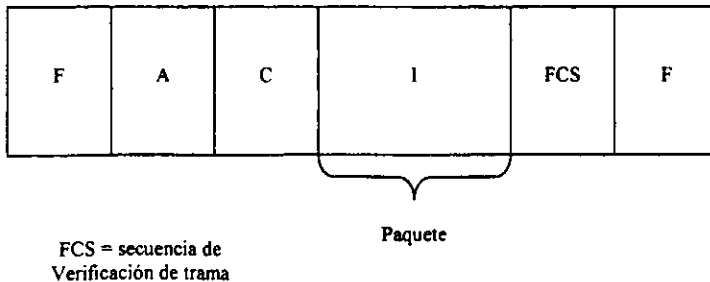


FIGURA 2.6. FORMATO DE LA TRAMA HDLC.

Las unidades de datos del nivel de enlace de datos del protocolo HDLC representativa se muestra en la figura 2.6. El principio y el final de la trama se denotan con un campo de sincronía de ocho bits especial *F*, 01111110. *A* es un

campo de dirección; C, un campo de control, y FCS, un campo que se usa para la detección de errores. El campo I, o de información, lleva los datos (el empaque) transferidos del nivel de red, las tramas de control como SABM no llevan un campo Y. Se distingue a cada uno colocando los bits apropiados en el campo C.

La trama SABM, cuando llega al lado B del sistema, causa que la entidad de enlace de datos asigne un valor inicial a sus variables y emita una primitiva indicación de CONEXIÓN. La entidad del nivel de red, al estar de acuerdo con la petición de comunicación, contesta con una primitiva respuesta de CONEXIÓN. Esto provoca que el protocolo de enlace de datos en el sistema B transmita una trama de aceptación sin numeración. (UA, *unnumbered acknowledgement*) a la entidad emisora de enlace de datos en la estación A, a su vez, ésta emite una primitiva confirmación de CONEXIÓN que completa la conexión. Ahora, el nivel de red puede iniciar la transmisión de datos en cualquier extremo. En la figura 2.8 se muestra la estación A comenzando la fase de transferencia de datos con la emisión de la primitiva solicitud de DATOS. Ahora se pueden transferir una o más tramas de información a la estación B. Estas contienen, como ya se ha señalado, campos I (fig. 2.9), las unidades de datos o *paquetes* tomados del nivel de red superior. Estos, a su vez, llevarán por lo general los datos del usuario desde el nivel de aplicación, más información de control pasada de las capas anteriores (fig. 2.6). Por tanto, la longitud del campo I es variable.

El formato específico de la trama HDLC (fig. 2.6) permite que la entidad de enlace de datos localice precisamente el campo I y elimine todo, excepto ese campo proveniente de una trama I, habiendo determinado que se recibió sin

errores. Después el campo *I* se envía, sin modificarse, a la entidad receptora de nivel de red que se encuentra arriba.

HDLC requiere de una aceptación positiva en el sentido de que las tramas *I* se recibieron correctamente a fin de enviarla de regreso a la entidad emisora de enlace de datos. (También se necesita una aceptación negativa si una trama se recibe fuera de secuencia o con bits con error). Las primitivas indicación de DATOS y respuestas de DATOS mostradas en la figura 2.9 se usan para denotar la correcta recepción de una trama *I*. Una aceptación positiva que llega al lado emisor ocasiona que la entidad de enlace de datos emita una primitiva confirmación de DATOS. Este proceso continúa mientras los dos sistemas deseen continuar la fase de transferencia de datos. Si cualquier par desea liberar la conexión, se debe emitir una primitiva solicitud de DESCONEXIÓN. La trama DISC mostrada es otra trama de control HDLC que se usa para enviar la solicitud de desconexión. La primitiva respuesta de DESCONEXION enviada no siempre se tiene que usar en protocolos de enlace de datos. En algunos protocolos la entidad de enlace de datos *local* (es decir, la que inicia la desconexión) emite la confirmación de DESCONEXIÓN en respuesta a una solicitud de DESCONEXIÓN. Como se puede apreciar, también inicia la transmisión de un mensaje de control al otro sistema, notificándole que la conexión debe terminar.

Aunque no se ha establecido explícitamente, en la exposición anterior se supone que ha hecho una exitosa de la trayectoria física antes de iniciar la fase de conexión del enlace lógico. El nivel físico interior proporciona este servicio de conexión. Las cuatro primitivas básicas en este nivel se usan de manera

similar para establecer la conexión al nivel físico. Los detalles de los protocolos estándar del nivel físico se incluyen en:

Las capas de transporte y de sesión de la arquitectura OSI dan otros dos ejemplos del uso de las cuatro primitivas básicas en las tres fases del proceso de transmisión de la información. Considere primero el nivel de transporte. Recuerde, de la breve exposición anterior, que hay cinco clases definidas para los protocolos OSI en este nivel y que las cinco usan las cuatro primitivas básicas en su fase de establecimiento de la conexión. Nótese cómo esta secuencia sigue precisamente la forma de la figura 2.5. La fase de establecimiento de las primitivas correspondientes en el nivel de enlace de datos. La fase de establecimiento de la conexión se usa para establecer la clase por usar, así como para negociar las opciones dentro de las clases, y la calidad de servicio deseada. Las entidades de transporte eligen la clase basadas en los requerimientos del usuario incorporados en las primitivas solicitud y respuesta de CONEXIÓN T, más la calidad de servicio de la red. La primitiva solicitud de CONEXIÓN T del nivel de sección (el usuario del servicio), lleva la dirección de transporte receptora a la dirección de transporte opcional y los parámetros de calidad de servicio y opcionales, más algunas clases, los datos de servicios de transporte. La indicación de CONEXIÓN T lleva la dirección de respuesta de CONEXIÓN T y la confirmación de servicio, para algunas clases, los datos del usuario de servicio de transporte.

2.3. CONECTIVIDAD EN EL PROTOCOLO X.25.

La recomendación de la interfaz de red X.25 de la CCITT se aprobó por parte de ese cuerpo en 1976. En 1980 apareció una versión revisada, y en

1984, una segunda revisión. La recomendación X.25 cubre la conexión de terminales de datos, computadoras y otros sistemas de usuario o dispositivos para redes de comunicación de paquetes. Los sistemas de usuario o dispositivos para redes de conmutación de paquetes. Los sistemas de usuario se llaman genéricamente *equipo terminal de datos* (ETD). Su conexión a la red se hace por medio de un equipo de red llamado *equipo de terminación de circuitos de datos* (ETCD). Normalmente, un ETD desea establecer comunicación con otro ETD (otro sistema de usuario) y utiliza la red con ese propósito. A su vez, ese ETD se conectará a un ETCD que controla su acceso a la red, y ésta será responsable de administrar las comunicaciones entre los ETD. El protocolo X.25 regula el flujo de datos entre ETD y ETCD sólo en cada extremo de la red. En la figura 2.7. se muestra este concepto en forma gráfica.

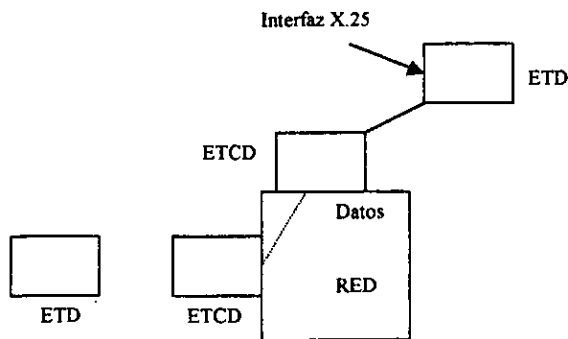


FIGURA 2.7. CONCEPTO X.25

Por tanto, X.25 es sólo una especificación de *interfaz*. Gobierna las instrucciones entre un ETD y el ETCD al que está conectado. Los detalles de la comunicación entre ETCD, usando la red que los conecta, se dejan al dueño u

operador de ésta. Tales detalles quedan ocultos a los ETD, que son los usuarios del servicio de conmutación de paquetes.

El protocolo X.25 está organizado como una arquitectura de tres niveles, que corresponden a los tres niveles de (red) del modelo OSI la figura 2.8 ilustra los tres niveles de X.25, en tanto que la figura 2.7 ilustra los tres niveles de X.25, en tanto que la figura 2.8 muestra la relación, nivel por nivel, con la arquitectura OSI. Se incluye X.25 en este punto debido a que brinda un ejemplo útil de una arquitectura por niveles que se ha usado durante muchos años, antes del anuncio de ISO del modelo OSI; Aunque X.25 es anterior a la arquitectura OSI, los esfuerzos realizados por el CCITT, con la cooperación de la ISO, han redundado en una compatibilidad entre X.25 y las tres capas más bajas de la arquitectura OSI, como se muestra de manera esquemática en la figura 2.8.

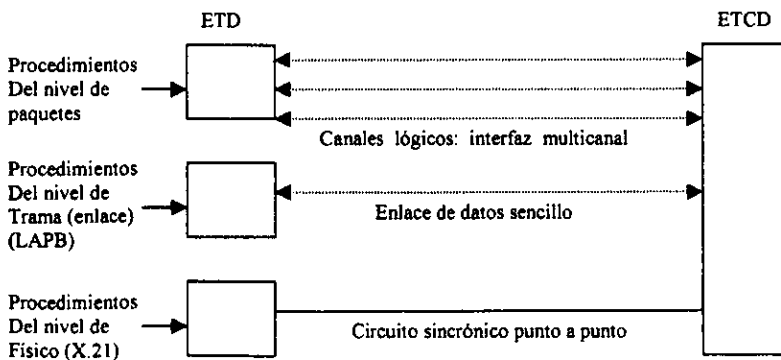


FIGURA 2.8. CAPAS X.25.

Al retomar la figura 2.7, se verá que en este ejemplo aparece un ETD en comunicación con dos ETD diferentes y dispersos geográficamente. En un principio, las especificaciones de X.25 incluían un modo de operación de

datagrama además del servicio de circuito virtual. En la versión de 1984 se desechó el servicio de datagrama debido a la falta de interés de quienes lo implantaban. Por tanto, se da mayor atención aquí al servicio de circuitos virtual. Existen varias redes de conmutación de paquetes de datagramas que *internamente* manejan los paquetes como datagrama, pero que *externamente*, en las interfaces X.25 con los ETD de los usuarios, convierten la operación en una de circuitos virtuales.

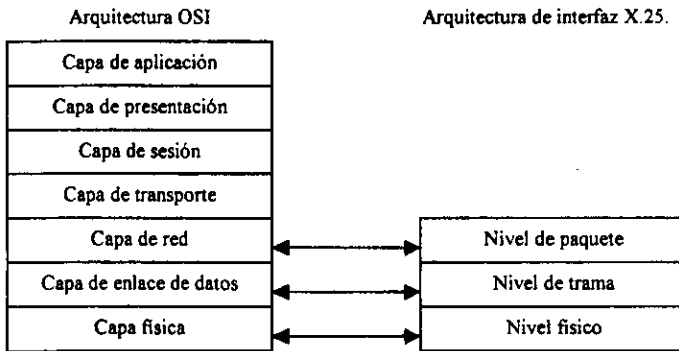


FIGURA 2.9. RELACIÓN ENTRE LAS ARQUITECTURAS OSI Y X.25.

Ahora el interés se encuentra en los niveles X.25 mostrados en la figura 2.8. como en la arquitectura OSI de la figura 2.2, el nivel físico más bajo asegura la existencia de una conexión física válida entre el ETD y el ETC. La recomendación de protocolo X.25 de CCITT se usa para este propósito. antes en este capítulo se hizo ver que el protocolo de nivel de enlace en el nivel de enlace de datos es un subconjunto de HDLC, etiquetado como LAPB (*balanced link acces procedure*, procedimientos balanceados de acceso al enlace). Las unidades de datos o tramas que atraviesan el enlace en cualquier dirección, de

ETD a ETCD, tienen precisamente el formato de la figura 2.6, descrito con anterioridad.

Es en el tercer nivel de red donde el protocolo X.25 se distingue como una arquitectura de interfaz. A esta capa se le llama *nivel de paquetes* en la terminología de X.25. Como ya se mencionó, X.25 se enfoca a conexiones de circuitos virtuales (CV, virtual circuit). Para este propósito, se asignan números de canal lógico en una conexión X.25 en particular (Fig. 2.8, nivel de paquetes). Hay disponibles hasta 4095 de estas conexiones entre cualquier ETD y el ETCD que tiene como interfaz. Para ello, se usan un campo de dirección de 12 bits. Esto implica que hasta el mismo número de llamadas de CV puede realizarse simultáneamente entre un ETD y los otros ETD de la red. Una vez establecida la llamada, cada paquete de datos que sale de un ETD lleva su propio número de canal lógico de 12 bits. Todos se multiplexan o comparten el mismo enlace de datos y usan el mismo proveedor de servicios, el nivel de enlace de datos inferior.

Cada interfaz ETD-ETCD asignan su propio conjunto de números de canales lógicos. Así, un CV completo, de extremo a extremo entre dos ETD que se comunican entre sí, pueden usar diferentes números de canales lógicos en las dos interfaces en cada extremo del circuito virtual.

Como sucedió con los diversos niveles de la arquitectura OSI, se requieren tres fases de comunicación para la operación de CV. Estas son, en orden: la fase de establecimiento de la llamada o, simplemente, fase de establecimiento; la fase de transferencia de datos, y la fase de desconexión o

liberación de la llamada (se puede usar CV permanentes, en cuyo caso no se necesita establecer la llamada).

CAPÍTULO III. SISTEMAS SNA.

Objetivo:

Definir los modelos de transmisión SNA y sus características.

CAPÍTULO III. SISTEMAS SNA.

3.1. SISTEMAS SNA.

En este capítulo se abordarán aspectos generales de SNA, también se hablará de la red donde opera la arquitectura SNA (System Network Architecture), y de la conectividad en esta arquitectura, así como del manejo de la información en el nivel de control de trayectoria.

La Arquitectura de Red de Sistemas de IBM, es una arquitectura de siete niveles diseñada para ofrecer interconexión entre productos de IBM, representa un conjunto común de estándares de interconexión, para la familia de Hardware y Software, entre sus objetivos iniciales estuvo la necesidad de hacer compatibles la amplia gama de productos de teleprocesamiento de comunicaciones de datos de IBM. Se anunció en 1974, después de un intenso desarrollo que comenzó a fines de la década de 1960. Esta versión de 1974 solo permitía redes centralizadas, es decir, redes en forma de árbol con un solo host y sus terminales. Su versión de 1976 ya permitía tener múltiples host con sus respectivos arboles, con la posibilidad de tener comunicación entre árboles, solamente a través de sus raíces. La versión de 1979 eliminó esta restricción, teniendo ya la capacidad para comunicarse de manera más general. Por último, en 1985 incluyó la aparición de topologías arbitrarias de host y LAN. La SNA precedió a los desarrollos de ISO, y por tanto no se ajusta estrictamente, nivel por nivel, a las características de la arquitectura OSI, sin embargo hay similitudes.

3.2. ARQUITECTURA SNA.

Como en el caso de otras arquitecturas por niveles, incluyendo el estándar OSI, el propósito SNA es ofrecer una comunicación confiable y oportuna entre usuarios finales diferentes, posiblemente localizados lejos uno de otro. La arquitectura SNA también se puede visualizar agrupada en dos categorías: la primera en un grupo de 4 niveles más altos que intervienen en el establecimiento y mantenimiento de la conexión (llamada sesión en la terminología de SNA) entre usuarios finales, así como en la sintaxis y la semántica de los datos que se intercambian, el segundo grupo de tres niveles más bajos que dan a la red la capacidad de transporte de extremo a extremo.

Los usuarios finales de SNA son, el usuario de terminal, las estaciones de trabajo, los programas de aplicación, las impresoras y dispositivos de despliegue gráfico, así como los dispositivos de almacenamiento de memoria. Los usuarios finales tiene acceso a una red SNA por medio de puertos de acceso o administradores de recursos de conexión, llamados unidades lógicas o UL (logical units, LU). A su vez, las UL establecen la sesión o conexión lógica a lo largo de la cual se transportan los datos del usuario final. Una UL puede apoyar a varios usuarios finales y también sesiones para diversas UL.

Dentro de la arquitectura SNA se tienen otros dos administradores de recursos de red, una Unidad física (UF), physical units, (PU), que administra los recursos de comunicación en un nodo dado, esto incluye los enlaces de datos y los canales de comunicación que sirven al nodo, y el Punto de Control de Servicios del Sistema (PCSS), (system services control point, SSCP), que administra todos los recursos dentro de un subconjunto de la red llamado

dominio. Las tres unidades [UL, UF y PCSS] forman el grupo de unidades direccionables de red UDR, (Network addressable units, NAU) de SNA. Cada unidad tiene su dirección de red única y es susceptible de dirigirse desde cualquier lugar dentro y fuera de la red.

Las UF, junto con un PCSS que las vigila, asegura que los enlaces de comunicación están disponibles y listos para ser usados. El PCSS ayuda a establecer y a dar de baja una sesión, controla y da soporte de mantenimiento para su dominio, mantiene un directorio y tablas de encadenamiento, se comunica con los otros PCSS a través de la red, etcétera. Sirve esencialmente como un control centralizado para todos los nodos de su dominio.

La red SNA está constituida por nodos interconectados; la cual puede contener muchas UL, existen cuatro tipos de nodos, cada uno designado con una UF de diferente tipo (ver figura 3.1). La UF-T1, es la clase más baja y suele estar compuesta de terminales de funciones bajas y controladores. La UF-T2 es la segunda clase y consiste por lo general de terminales de función superior, procesadores distribuidos y controladores de grupo; es decir, dispositivos que controlan terminales, sistemas de despliegue y otros dispositivos de funciones más bajas. El UF-T1 y el UF-T2, forman el grupo de nodos periféricos, como se indica en la figura 3.1. Ellos no participan de manera directa en la operación de la red de transporte (columna vertebral). En cambio siempre están conectados a los nodos UF-T4 y UF-T5 que se definen en seguida. El nodo tipo UF-T4 suele ser un controlador de comunicaciones (un ejemplo es el 3705, que ejecuta sobre NCP [Network Control Program], Programa de Control de Red. El nodo UF-T5 generalmente es un computador central. Los nodos UF-T4 y UF-T5 se llaman nodos subárea; ambos se

encuentran interconectados para formar la red de transporte. Un UF-T4 o un UF-T5, junto con los nodos periféricos conectados a ellos, forman una subárea. En la práctica, las redes suelen constituirse principalmente por controladores de comunicaciones, UF-T4, con los UF-T5 proporcionando control de red pero sin involucrarse en forma directa con el transporte o la función de columna vertebral de la red. La red de la figura 3.1, contiene cinco subáreas.

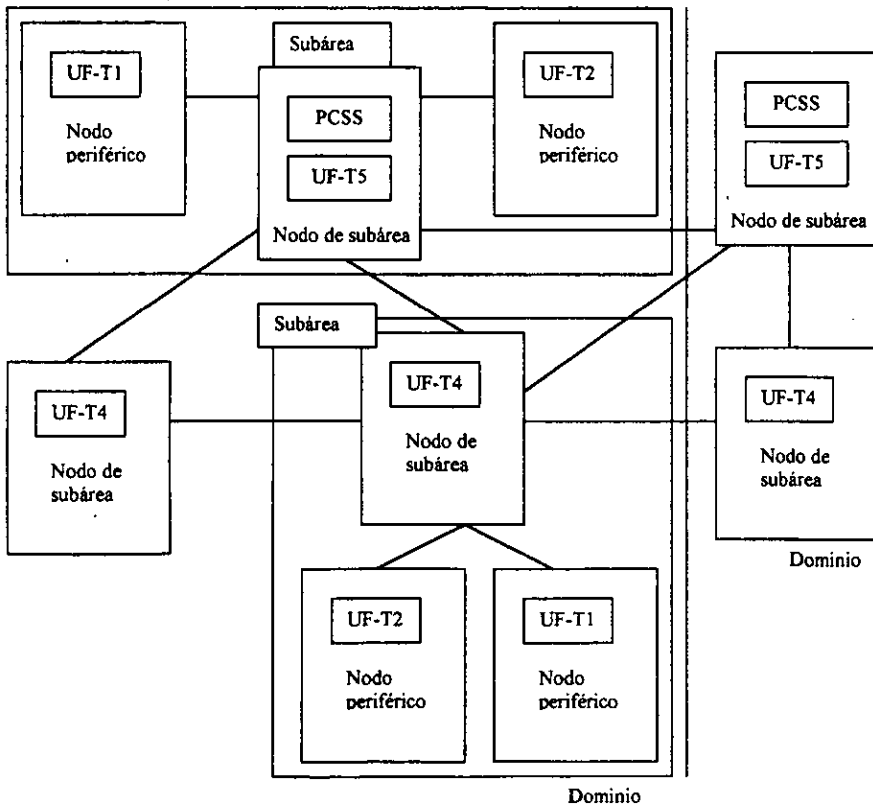


FIGURA 3.1 RED SNA.

El PCSS reside en UF-T5 o nodo central. Cada PCSS controla un dominio, constituido por nodos UF-T4, UF-T2 y UF-T1. Los nodos UF-T2 y UF-T1 siempre están conectados a nodos UF-T4 y UF-T5, como ya se mencionó anteriormente. Un nodo UF-T4 puede residir en dos dominios a su vez, una red está constituida por uno o más dominios; la red de la figura 3.1 contiene dos dominios. La parte de transporte o columna vertebral de esta red consiste en los cinco nodos subárea y siete enlaces que los interconectan. El PCSS de cada dominio es responsable de controlar todos los recursos de su dominio.

Por lo general, un nodo puede corresponder a un sistema o dispositivo, aunque es posible tener más de un nodo (varias UF) en una caja física dada, las realizaciones de los usuarios pueden proporcionar variaciones al respecto, como ejemplo el sistema de procesamiento distribuido, realizado originalmente como un nodo UF-T2, ahora puede contener tanto un UF-T2 como un UF-T5 en una caja, esta realización más reciente se usa para combinar dos redes SNA. En una red, el 8100 sirve como nodo periférico, ya que contiene un UF-T4 o un UF-T5, y puede comunicarse con otros sistemas o usuarios por medio del nodo subárea al que está conectado. En la otra red, el 8100 actúa como computador central, contiene el PCSS y puede participar plenamente como nodo subárea. Por tanto, la comunicación entre un usuario final en una red y un usuario final en otra red pasará a través del 8100.

La arquitectura SNA como ya se mencionó, es una arquitectura de 7 niveles, cuyo objetivo es el de establecer compatibilidad entre diferentes productos de IBM. En seguida se muestra la figura SNA y se explica el funcionamiento de cada nivel.

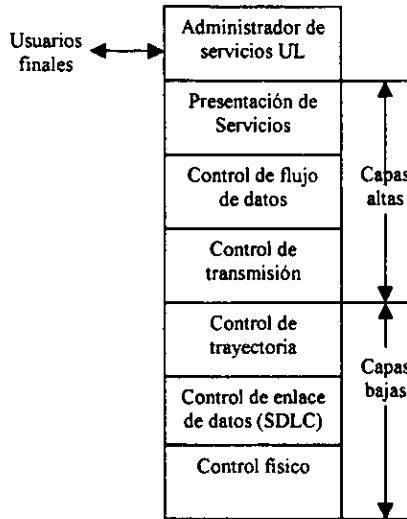


FIGURA 3.2. ARQUITECTURA SNA

ADMINISTRADOR DE SERVICIOS UL.

El nivel de administración de servicios de UL, al cual se conecta el usuario final, participa al establecer y dar de baja la sesión (también está involucrado el UF y el PCSS, como se verá en la sec. 3.3), y administra los servicios de aplicación.

SERVICIOS DE PRESENTACIÓN.

Este nivel ofrece la transformación de datos, efectúa la codificación y compresión de datos, y da formato al despliegue.

CONTROL DE FLUJO DE DATOS.

Este nivel asigna números secuenciales al encadenamiento lógico de los mensajes del usuario y lo maneja. Proporciona correlación de peticiones y respuestas entre usuarios, controla la multiplexación serial "agrupada" de transacciones mientras el periodo de transmisión está activo, etc.

CONTROL DE TRANSMISIÓN.

Este nivel maneja el control de flujo de extremo a extremo (llamado paso de sesión en la nomenclatura de IBM), lleva a cabo el cifrado y descifrado de datos, y verifica el número secuencial.

CONTROL DE TRAYECTORIA.

Este nivel es el encargado de controlar el encadenamiento y el flujo de mensajes a lo largo de la red.

CONTROL DE ENLACE DE DATOS SÍNCRONO (SDLC).

Este nivel es el responsable de la transmisión de datos sin errores sobre las conexiones entre los nodos.

CONTROL FISICO.

Este nivel es el responsable de la transmisión física mediante las señales apropiadas para las interfaces RS-232, 802.5, etc.

3.3. SESIÓN ENTRE UL-UL, PCSS-UF, UL-PCSS, UF-UF Y ENTRE PCSS-PCSS.

La conectividad en SNA como en otras arquitecturas, se refiere a la forma en la cual se transfiere la información entre sus niveles, desde un usuario fuente hasta un usuario destino.

Suponiendo que un usuario final desea comunicarse con otro usuario final ambos del mismo nodo o de cualquier otro nodo, esto se realiza por medio de una UL que establece una sesión con otra UL a la que tiene acceso el otro usuario. Siempre se designa una UL como primaria y otra UL como secundaria, con media sesión establecida en cada extremo. La comunicación entre los dos usuarios finales se lleva a cabo utilizando la arquitectura por niveles (SNA) que se muestra en la figura 3.3.

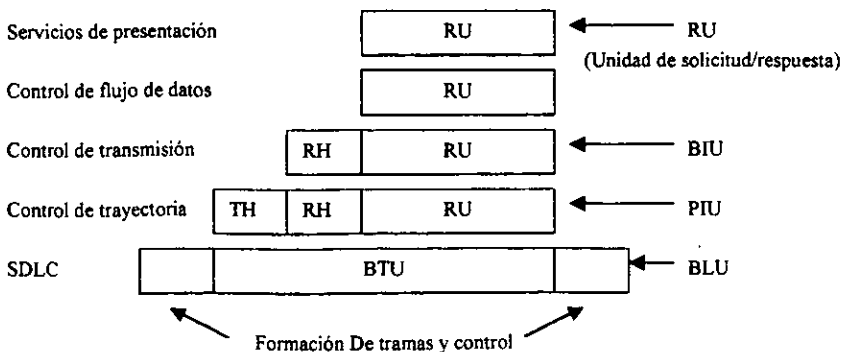


FIGURA 3.3. SNA Y SUS UNIDADES DE DATOS.

El administrador de servicios de la UL al que se conecta el usuario final, participa al establecer y dar de baja la sesión, y administra los servicios de la aplicación. En general el administrador de servicios de UL puede administrar varias UL. Cada UL y la media sesión establecida por ella se asocian con los tres niveles hacia debajo de la arquitectura, nivel de servicios de presentación, control de flujo de datos, y control de transmisión.

El nivel de servicios de presentación ofrece transformación de datos, efectúa la codificación y compresión de datos, y da formato al despliegue. El nivel de control de flujo de datos asigna números secuenciales al encadenamiento lógico de los mensajes del usuario, y lo maneja, proporciona correlación de peticiones y respuestas entre usuarios, controla la multiplexación serial (agrupada) de transacciones mientras el periodo de transmisión esta activo. El control de transmisión maneja el control de flujo extremo a extremo (llamado paso de sesión en la nomenclatura de IBM), lleva a cabo el cifrado y descifrado de datos, y verifica el número secuencial. Los niveles de control de flujo de datos y control de transmisión de SNA efectúan en forma conjunta algunas de las funciones y proporcionan algunos de los servicios de protocolos de sesión y de transporte de la arquitectura OSI.

El control de trayectoria de la figura 3.3, ofrece funciones de encadenamiento y control de congestión (flujo), en cada nodo solo hay un control de trayectoria, con las medias sesiones de todas las UL del modo multiplexadas en él, en la sección 3.4, se incluye un análisis detallado del control de trayectoria de SNA. El control de enlace de datos, es el responsable de la transmisión de unidades de datos sin errores sobre las conexiones entre

nodos, el control de enlace de datos de IBM se llama SDLC (*synchronous data link control*) o control de enlace de datos síncrono.

En la figura 3.3 también se muestran las unidades de datos transmitidas a través de las capas y entre capas iguales en las UL, en cualquier extremo de la sesión. La unidad de datos básica que un usuario final transmite, se llama unidad de solicitud o respuesta (*request or response unit, RU*). Esta puede ser una unidad de datos que lleve datos del usuario o una unidad de datos de control introducida como parte del control de una sesión. La RU se mueve hacia abajo hacia el nivel de control de flujo de datos, en donde se le añade el encabezamiento RH, al combinarse el RU y el RH forman una unidad básica de información o BIU (*basic information unit*), que se envía al control de trayectoria. En este punto se añade el encabezamiento de transmisión TH. La combinación de BIU y TH forman la unidad de información de trayectoria resultante PIU (*path information unit*), puede enviarse al nivel de enlace de datos sin cambios, segmentada o en bloques, la unidad de datos que se pasa al control de enlace de datos, se llama unidad básica de enlace de SNA.(BLU)

Además de la comunicación entre las UL, se requiere de comunicación entre PCSS y UF, entre UL y PCSS, y entre PCSS y PCSS. Se deben establecer sesiones para cada una de estas interacciones. Aquí también se aplica la arquitectura por niveles, por ejemplo un nodo PCSS, tendrá tres tipos de sesiones diferentes al mismo tiempo. Esto se demuestra en la figura 3.4, de un nodo SNA de 1981, desde entonces se han hecho algunas modificaciones, especialmente en el nivel de administración de servicios. En la figura 3.4 se muestran usuarios finales asociados con una UL, también se indica que un usuario final o UL dado, puede tener muchas medias sesiones, como ya se

había mencionado antes, cada una toma en cuenta los tres niveles: servicio de presentación, control de flujo de datos y control de transmisión. La UF y el PCSS tiene administradores de servicios asociados con ellos y pueden contar con varias sesiones al mismo tiempo. Sin embargo todos los tipos de sesiones se multiplexan en una capa de control de trayectoria. En este punto es donde se llevan a efecto las decisiones de encadenamiento. Los mensajes (PIU) generados localmente y aquellos que llegan de otros nodos de la red sobre las líneas de control de enlace de los datos entrantes, se distribuyen usando información contenida en el encabezamiento de la transmisión. Un PIU se puede encaminar en forma local hasta una de las medias sesiones que terminan en el control de trayectoria, o pueden enviarse al control de datos usando un enlace o canal de salida en particular, para transmitirlo hacia otro nodo. En la figura 3.4 también se muestra una función de frontera que conecta este nodo subárea con nodos periféricos unidos a él.

Como pudimos ver en la figura 3.3 que las unidades de datos del usuario, las RU, se generan para la sesión UL a UL en el nivel de servicios de presentación, este nivel entre los servicios que proporciona esta el de dar formato a la información que se exhibirá en pantalla o se imprimirá. SNA para ayudar a las UL, ha definido varios tipos de UL, cada uno estableció para llevar a cabo un tipo particular de sesión [SNA 1982]. La UL tipo 1 está diseñada para apoyar la comunicación entre un programa de aplicación y las terminales de procesamiento de datos. La UL tipo 2 se usa para la comunicación de un programa de aplicación con una sola terminal de exhibición en pantalla en un modo interactivo. La UL tipo 3 corresponde al caso de un programa de aplicación que se comunica con una sola impresora. La UL tipo 4 permite comunicarse a las terminales de procesamiento de datos, conectadas como

nodos periféricos. La UL tipo 6 corresponde a la comunicación programa con programa. Cada tipo de UL tiene su propio protocolo de comunicación.

Estos tipos de UL, con sus formatos de datos anexos, proporcionan las relaciones semánticas y las descripciones sintácticas para que los usuarios finales se comuniquen de manera significativa y confiable. El método SNA (que agrupa distintas clases de programas de aplicación, sistemas y dispositivos en categorías, para las cuales estén prescritos protocolos y formatos de datos).

Para controlar las sesiones PCSS-UL, PCSS-PCSS y PCSS-UF, requeridas para el funcionamiento adecuado de la red física y de las construcciones de SNA insertadas en ella. La UL tiene también un componente de servicios de red, el agrupamiento de servicios en este nivel en SNA. Independientemente de los tipos de servicios de presentación o de red de las tres unidades direccionables por la red (UL,UF, PCSS), se llaman, de manera genérica, servicios de función de administración de datos FAD (function management data). Esta capa se conoce como nivel de servicios FAD, y las RU generadas o recibidas por ella son unidades de datos de la función de administración.

Así que las unidades de solicitud/respuesta son de dos tipos: RU que contienen datos del usuario, cuyo formato se debe a los servicios de presentación UL y RU de control, que interviene en la operación de los protocolos de servicio de la red, una de las razones de la filosofía de SNA es que desde el principio se planteó para la interacción de sistemas subordinados y dispositivos con un sistema central grande, esto exigía siempre el control y el concepto PCSS. Los tipos de UL, la mayoría de los cuales siempre tiene que

ver con la comunicación entre los programas de aplicación y las terminales o dispositivos, lo cual refleja también la orientación hacia un control centralizado o una relación primaria- secundaria.

La figura 3.4. [SNA de 1982], indica de manera gráfica como se establece una sesión UL-UL, la secuencia de mensajes (RU) transmitidos suelen llamarse triángulo ligado, una sesión puede ser inicializada por una UL primaria o por una UL secundaria, o una UL tercera puede tratar de activar una sesión entre otra dos UL. En los tres casos, el RU iniciador envía una iniciación o INIT RU al PCSS. Este RU de control funciona de dos formas distintas, dependiendo de si el UL indicador desea establecer una sesión por si mismo o lo esta haciendo en cooperación con otro UL. El INIT RU, se identifica como tal por un encabezamiento de 3 bytes, lleva los nombres de los UL de fuente y de destino. Un nombre de modo que identifica el conjunto de protocolos y papeles que se usaran al conducir la sesión, la clase de servicio CDS (*class of service COS*) para el camino de extremo a extremo (continua en la sección 3.4), y una indicación sobre si la UL de destino será la primera o la secundaria. También se transmiten otros parámetros como la indicación de que si la UL indicadora será la primaria o la secundaria, significa que la UL iniciadoras será la que seleccione a la UL primario en el caso de dos UL que tratan de comunicarse, ya que en el caso de la comunicación entre un programa de aplicación que reside en un computador central y un dispositivo o terminal, la UL central es normalmente la primaria.

Al recibir el INIT RU, el PCSS determina si la solicitud es valida (ambas UL deben de ser capaces de apoyar el tipo de sesión, es decir, el tipo de UL requerido, quiere decir que las contraseñas deben de ser validas, etc.). Si es así

el PCSS devuelve el nombre de la UL de destino para una dirección de la red, determina si existe una trayectoria y si la UL de destino está disponible y luego selecciona los parámetros que usarán las UL cuando su sesión se haya activado.

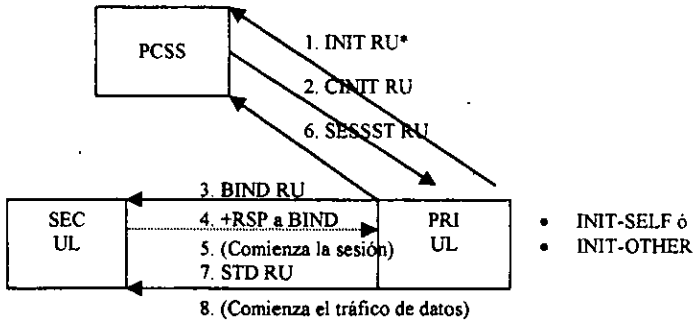


FIGURA 3.4A. INICIO DE UNA SESIÓN UL-UL EN EL MISMO DOMINIO.

La UL primaria inicia la sesión UL.

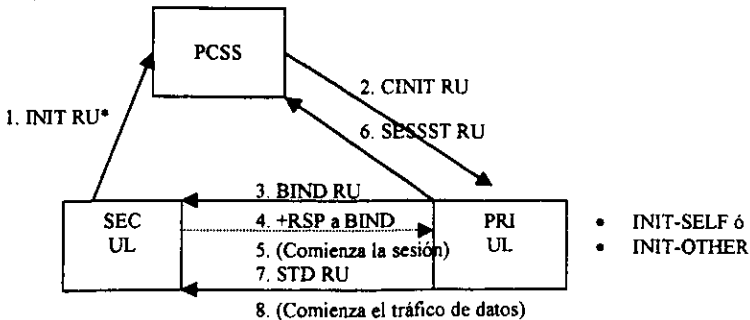


FIGURA 3.4B. INICIO DE UNA SESIÓN UL-UL EN EL MISMO DOMINIO.

La UL secundaria inicia la sesión UL.

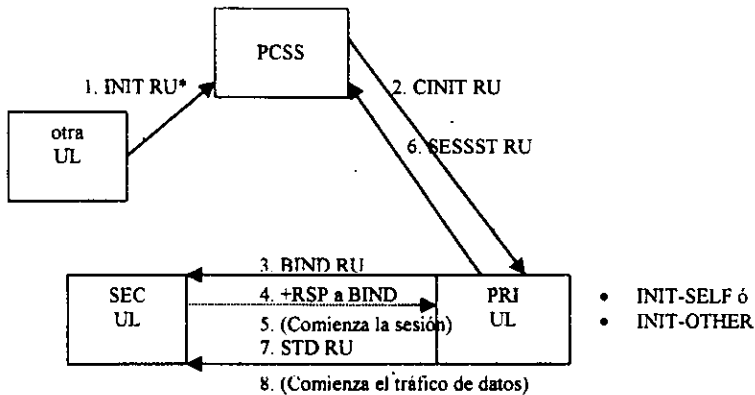


FIGURA 3.4C. INICIO DE UNA SESIÓN UL-UL EN EL MISMO DOMINIO.

Una tercera UL inicia la sesión UL-UL

Después los servicios de la red en el PCSS preparan y envían la CINIT RU a la UL primaria. Nótese que esta función se lleva a cabo en los tres casos de la figura 3.5. La UL primaria responde enviando un BIND RU a la UL secundaria. Esta es la solicitud de la activación de la sesión. La BIND RU establece los protocolos para la sesión, estas se basan en el modo especificado por la UL iniciadora y en parámetros establecidos por el PCSS. El tipo de UL por ejemplo, se hace corresponder con un conjunto de campos de perfil en la BIND RU.

La RU secundaria puede aceptar la solicitud, contestando con una respuesta positiva (+ RSP en la figura 3.5), o puede rechazarla. Algunos de los diferentes tipos de sesiones pueden permitir un enlace negociable. En este caso, la +RSP devuelta a la UL primaria puede llevar ya sea los mismo parámetros del BIND, indicando que la UL secundaria los acepta, o parámetros distintos, que la UL primaria a su vez, puede aceptar o rechazar. Por ejemplo la transmisión de información comprimida durante la sesión, la UL primaria puede proponer si no es negociable y la UL secundaria debe aceptar o rechazar esta solicitud. Si es negociable y la UL secundaria no maneja la información comprimida, contestará con una negativa, dando a la UL primaria la oportunidad de aceptarla o rechazarla.

La operación exitosa de este procedimiento de iniciación de sesión UL-UL requiere de la existencia de sesiones UL-PCSS, por lo que estas deben establecerse con anterioridad también deben establecerse sesiones PCSS-UF, para efectuar las conexiones físicas de la red.

Las RU restantes de la figura 3.5 se explican por si mismas: la RU de sesión comenzada (SESSST sesión started) es una notificación de la UL primaria a la PCSS en el sentido de que la sesión UL-UL se activó con éxito. (Si el proceso de iniciación de la sesión fracasa, se envía en su lugar una RU de falla de enlace (BIND F). La RU de datos de inicio (SDT, stard data), con una respuesta positiva esperada, completa la activación de la sesión UL-UL.

Una de las ventajas de usar una arquitectura SNA es que la organización lógica de la red es independiente a la implementación física. Esto significa que los cambios pueden hacerse en los métodos que son usados para transmitir

datos o en los dispositivos y facilidades de transmisión en la red sin tener que cambiar la organización lógica de la red o las aplicaciones que usa. SNA tiene Sistema de Comunicación modular que puede ser modificado sin tener que modificar programas de aplicación que hacen uso de las facilidades de transmisión proporcionadas por la red. Un sistema SNA está habilitado para responder a las demandas de nuevas aplicaciones y puede acomodar relativamente un crecimiento impredecible de nuevos sistemas.

Las operaciones de la Red SNA son transparentes para los usuarios, para los desarrolladores de aplicaciones, todo el personal de procesamiento de datos debe tener conocimientos básicos de conceptos y terminología de SNA.

3.4 CONTROL DE TRAYECTORIA.

Como ya se mencionó en la sección 3.2, el nivel de control de trayectoria es la encargada del encadenamiento y el flujo de mensajes a lo largo de la red.

Como se muestra en la figura 3.5, el control de trayectoria recibe una unidad básica de información (*basic information unit, BIU*), del control de transmisión, y añade un encabezamiento de transmisión (*transmission header, TH*) para formar una unidad de información de trayectoria (*path information units, PIU*).

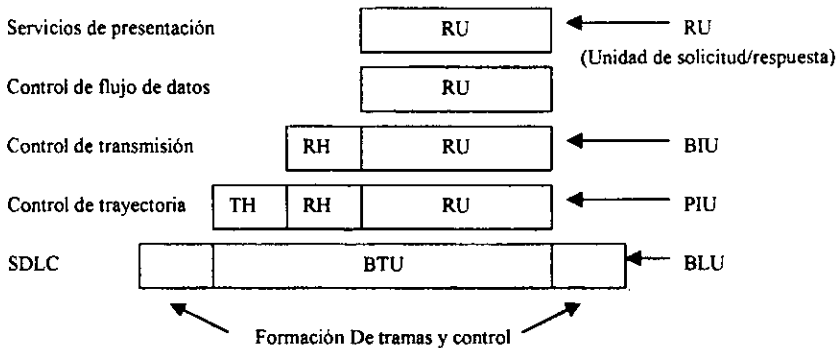


FIGURA 3.5. UNIDADES DE DATOS SNA.

La PIU puede pasarse al control de enlace de datos sin cambios, se puede llevar a cabo primero su segmentación o conformación en bloques (encadenamiento). Aquí las BIU se segmentarán en PIU múltiples si son demasiado largas, véase la figura 3.6(a) o las PIU pueden conformarse o combinarse en una unidad más larga si son muy cortas, véase figura 3.6b, esto solo se hace en casos especiales. En todos los casos, la unidad final que se envía al control de enlace de datos se llama unidad básica de transmisión (*basic transmission unit BTU*). La BTU a su vez, forma el campo de las unidades básicas de enlace (*basic link units, BLU*), del control de enlace de datos síncrono (*synchronous data link control, SDLC*), que transmite entre nodos adyacentes en redes SNA. Los campos específicos que comprenden al encabezamiento de transmisión agregado a la capa de control de trayectoria se describirá más adelante. Después de que las funciones de control de trayectoria se comenten y analicen con detalle.

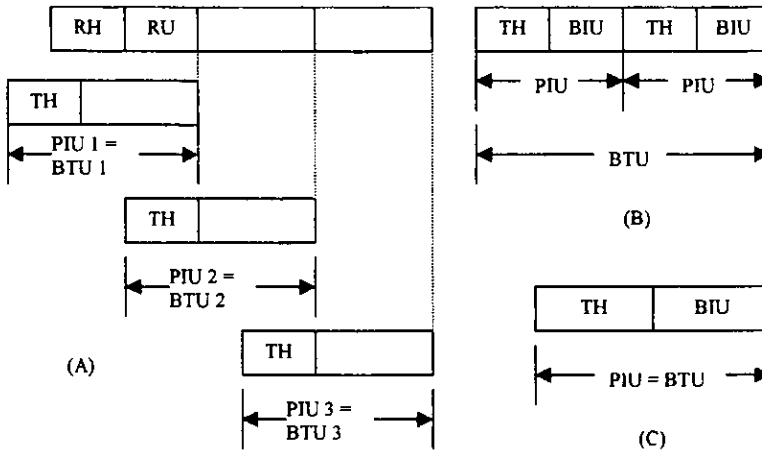


FIGURA 3.6. TIPOS DE BTU.

1. Segmentado (BIU muy larga)
2. Conformación de bloques (PIU muy cortas)
3. Sin cambios (PIU normales)

Como se hizo ver anteriormente, en la terminología SNA dos usuarios o unidades lógicas (*logical units, LU*) se comunican por vía de una sesión, media sesión en cada extremo, establecida entre dos UL. Los mensajes para una sesión dada se encaminan por el control de trayectoria sobre una trayectoria física que se conoce como ruta explícita RE (*explicit route, ER*). Dicha ruta consiste en un grupo de nodos con varios GT (Gateway) conectados entre ellos. A cada RE se le asigna un número llamado número de ruta explícita NRE (*explicit route number, ERN*). Los mensajes asignados a un GT específico de un enlace múltiple, como parte de una ruta explícita que usa GT, puede usar diferentes enlaces y por tanto llegar en desorden al nodo en el otro extremo del

GT. Por esta razón, tales mensajes deben reordenarse antes de enviarse de nuevo a lo largo de la ruta explícita. Los mensajes entre los nodos fuente y destino generalmente son obligados por la arquitectura SNA a seguir la misma trayectoria física. Sin embargo, las trayectorias en las dos direcciones pueden tener números diferentes (o sea diferentes NRE).

Además de tener rutas explícitas que comprenden trayectorias físicas entre nodos fuente-destino en una red. SNA define trayectorias lógicas dúplex entre nodo fuente-destino. Estas se llaman rutas virtuales RV (*virtual route, VR*) y corresponden a los circuitos virtuales. Se puede definir un máximo de RV entre pares de subárea y las sesiones múltiples pueden usar la misma RV. El control de trayectoria de SNA multiplexa las sesiones de los controles de transmisión individuales, uno para media sesión, en el nivel que esta arriba de él en los dos extremos de una ruta virtual. Las RV múltiple pueden compartir una ruta explícita. La ruta virtual solo se conoce en los dos extremos de los nodos subárea, de una trayectoria dada. En el encadenamiento a lo largo de una trayectoria específica, la ruta explícita se determina por el NRE y por la dirección del destino (subárea). Un nodo intermedio a lo largo de la ruta explícita usa estos dos campos, llevados en el encabezamiento de transmisión, para dirigir los mensajes al grupo de transmisión de salida apropiado.

Las 48 posibles rutas virtuales entre pares de subárea que comprenden los nodos de fuente y destino se obtienen definiendo 16 números de RV y 3 capas de prioridad en cada uno. El número de RV y la prioridad se combinan para formar el IDR (Identificador específico de Ruta Virtual). Cada entrada en una tabla IDR en un nodo subárea fuente se asocian a su vez con una especificación de usuario de clase de servicio COS (class or service, COS). La

clase de servicio depende del tipo de datos que van a transmitirse (por ejemplo, en lotes o interactivos) y del servicio deseado como (alto rendimiento, con poco retardo, o criptográfico, entre otros). Se especifica una correspondencia en un nodo fuente entre la clase de servicio y el IDRV. La lista de IDRV aparece en orden de funcionamiento, y se asigna una sesión al primer RV en la lista que esta accesible.

La correspondencia global, que se usa al establecer una trayectoria entre nodos subárea en el proceso de establecimiento de una sesión entre ellos, se muestra de esta forma:

COS → IDRV → RV → RE

La ruta o la trayectoria explícita para usarse entre cualquiera de dos nodos subárea no esta actualmente especificada por SNA, sino que depende del usuario. En la figura 3.7. se muestra un diagrama simplificado de flujo de mensajes (unidades de datos) dentro del control de trayectoria, con segmentación o conformación de bloques, así como encadenamiento. También se muestra un elemento de control de RV (CRV) conectado a un control de RE (CRE) que a su vez esta conectado a un control de grupo de transmisión (GGT). Las tres funciones aparecen dentro del control de trayectoria, y por tanto tienen contador de paso (PC) en sus etiquetas.

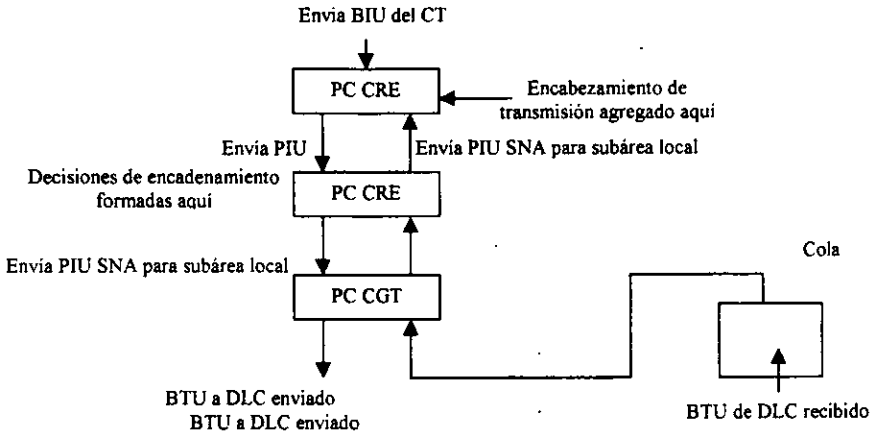


FIGURA 3.7. DIAGRAMA SIMPLIFICADO, CONTROL DE TRAYECTORIA SNA.

En el extremo más alto el CRV se comunica con el control de transmisión IC. Si se requiere, la segmentación es realizada por el CRV. También aquí se agrega el encabezado de transmisión (*transmission header, TH*). La PIU resultante (figura 3.7) se pasa al control de ruta explícita (CRE), este control lleva a cabo el encadenamiento para el nodo, y es el que decide, basado en el campo de encadenamiento de transmisión, cual GT se va a utilizar para la transmisión. De manera análoga, las decisiones de encadenamiento son hechas por el CRE en las PIU que se envían hacia arriba desde el control de grupo de transmisión (CGT): los mensajes pueden enviarse hacia abajo a un grupo de transmisión apropiado, en caso de que estén asignando a otra subárea, se procede a enviar los mensajes al CRV. Si es necesario, el control de grupo de transmisión conformará bloques de PIU para formar la unidad básica de transmisión, pero solo en grupos de transmisión de enlace único.

3.5. RUTA VIRTUAL .

El control de congestión en la capa de control de trayectoria de SNA, cuenta con mecanismos de control de flujo, llamados controles de paso, contruidos en múltiples niveles de la arquitectura. El paso de la sesión, en el nivel de control de transmisión (TC), se usa para controlar la velocidad de recepción de los mensajes entre los dos extremos de una sesión. SDLC, en el nivel de enlace de datos, tiene el control de paso del nivel de enlace construido con el uso de tramas. El control de congestión de extremo a extremo, que se lleva a cabo en cada ruta virtual en el nivel de control de trayectoria, se denomina control de paso de ruta virtual. El mecanismo es en si muy complejo y se describe con detalle en el manual SNA (*SNA 1980, cap. 3*), así como en un documento básico elaborado por J. D. Atkins [ATKI].

3.6. TRANSMISIÓN SNA.

Se hizo notar antes que el control de trayectoria o nivel de red SNA añade un encabezamiento de transmisión (TH) a la unidad de datos desde el control de transmisión (fig. 3.7). La unidad de datos resultante se llama unidad de información de trayectoria (PIU). El encabezamiento de información se usa para llevar a cabo funciones de encaminamiento y control de flujo en cada nodo a lo largo de una ruta virtual. Se describe brevemente el encabezado de este formato.

Byte		
0	Identificación de formato, F1: 0100 Indicador de barrido GT (0 ó 1) Indicador de soporte RE y RV (0 ó 1) Prioridad de red (0 ó 1)	Byte *reservado
2	Número de ruta explícita inicial (4 bits) Número de ruta explícita N RE (4 bits)	Número de ruta virtual (4 bits) 2 bits de reserva Campo de prioridad de transmisión (2 bits)
8 4	Campo de dirección de la subárea de destino Indicador de cambio de ventana de RV (0 ó 1) Indicador de no PEPS en gt (0 ó 1) Indicador de secuencia y tipo de RV (2 bits) Campo de número de secuencia de GT (bits 4 a 15)	
6	Solicitud de control de paso de RV (0 ó 1) Respuesta de control de paso de RV (0 ó 1) Indicador de respuesta a cambio de ventana de RV (0 ó 1) Indicador de restablecimiento de ventana RV (0 ó 1) Campo de envío de número de secuencia de RV (bits 4 a 15)	
12	Campo de dirección de la subárea de origen (4 bytes)	
16	Bits 0 a 2 reservados indicador de SNA (0 ó 1) Campo de mapeo (2 bits) bit 6 reservado indicador de flujo expedito (0 ó 1)	Byte * Reservado
18	Campo del elemento de destino	
20	Campo del elemento de origen	
22	Campo del número de secuencia	
24	Campo de conteo de datos	

FIGURA 3.8. ENCABEZAMIENTO DE TRANSMISIÓN, FORMATO FID4 SNA.

SNA define 6 tipos de formatos de encabezamiento de transmisión. Aquí solo se analiza el que tiene que ver con la comunicación entre nodos subárea adyacentes que comprenden una red de comunicaciones de SNA. El formato de

este encabezamiento, identificado por la etiqueta IDF4 y que consiste de 26 bytes, se representa en la figura 3.8., y solo se abordarán porciones de este formato.

La ruta virtual se identifica por el número de ruta virtual y por el campo 2 bits de prioridad de transmisión. El patrón del bit de prioridad 00 se usa para representar prioridad baja; 01 significa prioridad media, y 10 se refiere a prioridad alta. El número de ruta explícita (NRE) sobre el cual se hace corresponder el CV (solo en esta dirección), está dado por los 4 bits del byte 2. Las direcciones del destino y de la fuente de la subárea, se proporciona por los bytes 8-11 y 12-15, respectivamente.

El control de paso de ruta virtual se asigna a varios bits. La PIU se identifica colocando el bit 1 (el bit de solicitud de paso de RV) del byte 6 de su encabezamiento de transmisión a 1. A su vez la unidad de datos VRPRS se identifica colocando el bit 2 de respuesta de paso de la RV en el byte 6 a 1. Al mismo tiempo, el bit de prioridad de red en el byte 0 se coloca en 1, lo que proporciona un regreso rápido del VRPRS al nodo fuente.

Se usan otros bits para llevar a cabo los aspectos de variación de la ventana del mecanismo de control de paso. Por ejemplo, la forma de indicar una congestión menor en un grupo de transmisión a lo largo de la RE en la cual viaja la PIU es colocando a 1 el indicador de cambio de ventana de la RV del byte 4. Los grupos de transmisión subsecuentes a lo largo de la RE dejan encendido el indicador. A su vez, el indicador es devuelto por el VRPRS, colocando en 1 el bit indicador de respuesta a cambio de ventana en su byte 6. Cuando el VRPRS llega al nodo fuente (origen), la ventana decrecerá en 1. Si

se experimenta tráfico pesado en cualquier punto a lo largo de la RE, el nodo que experimenta la congestión colocaría en 1 bits indicador de restablecimiento de ventana de la RV del byte 6 en el primer PIU que atravesará en dirección hacia la fuente. Al llegar, ahí este PIU causaría que la ventana se cambiara al mínimo especificado. Nótese que estas acciones afectan a todas las RV que pasan a través de un nodo que experimenta congestión. Los nodos intermedios no distinguen entre las RV que los usan.

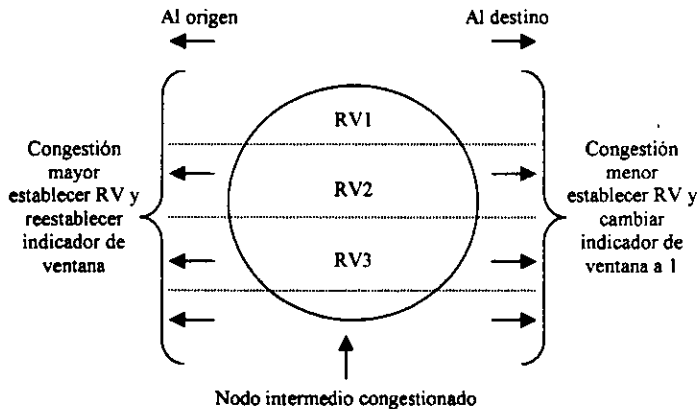


FIGURA 3.9. ACCIONES TOMADAS EN UN NODO SNA CONGESTIONADO.

Estas acciones, tomadas en un nodo intermedio que experimenta congestión, se muestra en la figura 3.9. SNA no describe claramente como medir la congestión y, por tanto, esta especificación se deja al implantador de la red. Una media simple podría consistir en medir una congestión menor a través de un límite de área de almacenamiento temporal en un grupo de transmisión de salida que esté siendo excedido. Una congestión pesada (mayor) podría

manifestarse por un límite de área de almacenamiento temporal más alto que hubiese excedido. Otra medida podría incluir la velocidad de salida del paquete en un grupo de transmisión que excede cualquiera de dos límites.

CAPÍTULO IV. PROTOCOLO TCP/IP.

Objetivo:

Destacar las propiedades del protocolo TCP/IP, sus ventajas y desventajas en la transmisión de datos.

CAPÍTULO IV. PROTOCOLO TCP/IP.

En los inicios de las redes de comunicación para computadoras, el departamento de defensa de los estados unidos se vio en la necesidad de establecer mecanismos normalizados para interconectar equipo de cómputo de diferentes fabricantes, para permitir así la creación de una red de cobertura nacional. El trabajo fue financiado por DARPA (Defence Advanced Research Proyect Agency) y la red en la que se ocuparía fue llamada ARPANET (actualmente INTERNET), su nombre fue el conjunto de servicios TCP/IP.

La conectividad en una red se realiza mediante un protocolo del conjunto de protocolos que conforman a TCP/IP debe este poder realizar el envío de acuerdo con la dirección de Internet que especifica a cada nodo de la red. La conexión que se realiza entre dos aplicaciones se conoce como conectividad esto es que, para que se realice la conectividad, la información debe de pasar por todos los niveles que hay entre dos aplicaciones.

DARPA comenzó a trabajar con una tecnología de red de redes a mediados de los años setenta, su arquitectura y protocolos tomaron su forma actual entre 1977 y 1979. En ese tiempo, DARPA era conocida como la principal agencia en proporcionar fondos para la investigación de redes de paquetes conmutados y fue pionera de muchas ideas sobre la conmutación de paquetes con su bien conocida ARPANET. ARPANET utilizaba interconexión convencional de línea rentada punto a punto, pero DARPA también ofreció fondos para la explotación de conmutación de paquetes a través de redes de radio y mediante canales de comunicación por satélite.

La disponibilidad de DARPA en cuanto a fondos para la investigación, atrajo la atención y la imaginación de muchos grupos de investigación, en especial de los investigadores que ya tenían experiencia previa utilizando conmutación de paquetes en ARPANET.

La Internet global se inició alrededor de 1980 cuando DARPA comenzó a convertir las máquinas conectadas a sus redes de investigación a sus redes de investigación en máquinas con el nuevo protocolo TCP/IP. ARPANET, una vez en su lugar, se convirtió rápidamente en la columna vertebral del nuevo Internet, y fue utilizada para realizar muchos de los primeros experimentos con el TCP/IP. La transmisión hacia la tecnología Internet se completó en 1983, cuando la Oficina del Secretario de Defensa ordenó que todas las computadoras conectadas a redes de largo alcance finalizara el TCP/IP.

A siete años de su concepción, Internet había crecido hasta abarcar cientos de redes individuales localizadas en los Estados Unidos y en Europa. Conectaban casi 20, 000 computadoras en universidades, así como a centros de investigación privados y gubernamentales.

4.1. SERVICIOS DE INTERNET.

Para entender los detalles técnicos de TCP/IP es necesario entender los servicios que proporciona. Los protocolos como el TCP y IP proporcionan las reglas para la comunicación. Contienen los detalles referentes a los formatos de los mensajes, describen cómo responder una computadora cuando llega un mensaje y específica de qué manera una computadora maneja un error u otras condiciones anormales.

4.1.1. NIVEL DE APLICACIÓN .

En una red de redes TCP/IP aparece como un grupo de programas de aplicación que utiliza la red para llevar a cabo tareas útiles de comunicación. Se utiliza el termino interoperabilidad para referirnos a la habilidad que tienen los diversos sistemas de computación para cooperar en la resolución de problemas computacionales. Los programas de aplicación de Internet muestran un alto grado de interoperabilidad.

Los servicios de aplicación de Internet más populares y difundidos son:

Correo electrónico (Protocolo SMTP).- el correo electrónico permite que un usuario componga memorándums y los envíe a otros usuarios o grupos. Así como también permite que un usuario lea los memorándums que ha recibido. El correo electrónico ha sido tan exitoso que muchos usuarios de Internet dependen de él para su correspondencia normal de negocios. Aunque existen muchos sistemas de correo electrónico, al utilizar el TCP/IP se logra que la entrega sea más confiable debido a que no se basa en computadoras intermedias para distribuir los mensajes de correo. Un sistema de entrega de correo TCP/IP opera al hacer que la máquina del transmisor contacte directamente la máquina del receptor.

Transferencia de archivos (Protocolo ETP).- Aunque los usuarios algunas veces transfieren archivos por medio del correo electrónico, el correo está diseñado para mensajes cortos de texto. Los protocolos TCP/IP incluyen un programa de aplicación para transferencia de archivos, el cual permite que los usuarios envíen o reciban archivos arbitrariamente grandes de programas,

de datos o de texto. Al utilizar el programa de transferencia de archivos, se puede copiar de una máquina a otra una gran base de datos que contenga imágenes, un programa escrito en un lenguaje de programación, o un directorio de idiomas. El sistema tiene una manera de verificar que los usuarios cuenten con autorización o, incluso, de impedir el acceso.

Acceso remoto (Protocolo TELNET).- El acceso remoto permite que un usuario que esté frente a una computadora se conecte a una máquina remota y establezca una sesión interactiva. El acceso remoto hace aparecer una ventana en la pantalla del usuario, la cual se conecta directamente con la máquina remota al enviar cada golpe de tecla desde el teclado del usuario a una máquina remota y muestra en la ventana del usuario cada carácter que la computadora remota genere. Cuando termina la sesión de acceso remoto, la aplicación regresa al usuario a su sistema local.

4.1.2. NIVEL DE RED.

Un programador que crea un programa de aplicación que utiliza protocolos TCP/IP tiene una visión totalmente diferente de una red de redes, con respecto a la visión que tiene un usuario que únicamente ejecuta aplicaciones como el correo electrónico. En el nivel de red, una red de redes proporciona dos grandes tipos de servicios que todos los programas de aplicación utilizan.

Servicios sin conexión de entrega de paquetes.- Este servicio forma la base de todos los otros servicios de la red de redes. La entrega sin conexión es una abstracción del servicio de la mayoría de las redes de conmutación de

paquetes ofrecen. Simplemente significa que una red de redes TCP/IP rutea mensajes pequeños de una máquina a otra, basándose en la información de dirección que contiene cada mensaje. Debido a que el servicio sin conexión rutea cada paquete por separado, no garantiza una entrega confiable y en orden.

Servicio de transporte de flujo confiable.- La mayor parte de las aplicaciones necesitan mucho más que sólo la entrega de paquetes, debido a que requieren que el software de comunicaciones se recupere de manera automática de los errores de transmisión, paquetes perdidos o fallas de conmutadores intermedios a lo largo del camino entre el transmisor y el receptor. El servicio de transporte confiable resuelve dichos problemas. Permite que una aplicación en una computadora establezca una "conexión" con una aplicación en otra computadora, para después enviar un gran volumen de datos a través de la conexión como si ésta fuera permanente y directa del hardware.

4.1.3. CARACTERÍSTICAS DE TCP/IP.

Independencia de la tecnología de red.- Como TCP/IP está basado en una tecnología convencional de conmutación de paquetes, es independiente de cualquier marca de hardware en particular. La Internet global incluye una variedad de tecnologías de red que van de redes diseñadas para operar dentro de un solo edificio a las diseñadas para abarcar grandes distancias. Los protocolos TCP/IP definen la unidad de transmisión de datos llamada datagrama, y especifican cómo transmitir los datagramas en una red en particular.

Interconexión universal.- Una red de redes TCP/IP permite que se comunique cualquier par de computadoras conectadas a ella. Cada computadora tiene asignada una dirección reconocida de manera universal dentro de la red de redes. Cada datagrama lleva en su interior las direcciones de su fuente y su destino para tomar decisiones de ruteo.

Acuses de recibo punto a punto.- Los protocolos TCP/IP de una red de redes proporciona acuses de recibo entre la fuente y el último destino en vez de proporcionarlos entre máquinas sucesivas a lo largo del camino, aun cuando las dos máquinas no estén conectadas a la misma red física.

Estándares de protocolo de aplicación.- Además de los servicios básicos de nivel de transporte, los protocolos TCP/IP incluyen estándares para muchas aplicaciones comunes, incluyendo correo electrónico, transferencia de archivos y acceso remoto.

4.2. ARQUITECTURA TCP/IP.

El objetivo primordial de obtener un esquema que esconde los detalles del hardware subyacente de red a la vez que proporciona servicios universales de comunicación. El resultado principal es una abstracción de alto nivel que proporciona la estructura para todas las decisiones en cuanto a diseño.

4.2.1 INTERCONEXIÓN DEL NIVEL DE APLICACIÓN

Las primeras interconexiones heterogéneas de red proporcionaban la uniformidad por medio de programas de nivel de aplicación, en tales sistemas, un programa de nivel de aplicación que corre en cada máquina de la red “entiende” los detalles sobre las conexiones de red para esa máquina e interactúa con los programas de aplicación a través de dichas conexiones.

Utilizar programas de aplicación para ocultar los detalles de la red puede parecer natural al principio, pero tal enfoque da como resultado una comunicación limitada e incomoda. Agregar funcionalidad al sistema implicaría diseñar un nuevo programa de aplicación para cada máquina. Agregar nuevo hardware de red implicaría modificar o crear nuevos programas para cada posible aplicación. En una máquina, cada programa de aplicación debe “entender” las conexiones de red para esa máquina, dando como resultado la duplicación del código.

Los usuarios que tienen experiencia con el trabajo con redes entienden que una vez que la interconexión crezca a cientos o miles de redes, nadie podría diseñar todos los programas necesarios de aplicación. Además, el éxito del esquema de comunicación un paso a la vez requiere que todos los programas de aplicación que se ejecutan a lo largo del camino funcionen correctamente. Cuando falla un programa intermedio, tanto el origen como el destino se encuentran imposibilitados para detectar o resolver el problema.

4.2.2. INTERCONEXIÓN DEL NIVEL DE RED.

Una interconexión de red proporciona un mecanismo que entrega en tiempo real los paquetes, desde su fuente original hasta su destino final. Conmutar pequeñas unidades de datos en vez de archivos o grandes mensajes tiene muchas ventajas. Primero, el esquema se proyecta directamente hacia el hardware subyacente de red, haciéndolo extremadamente eficiente. Segundo, la interconexión a nivel de red separa de los programas de aplicación las actividades de comunicación de datos, permitiendo que computadoras intermedias manejen el tráfico de red sin “entender” las aplicaciones que lo utilizan. Tercero, utilizar conexiones de red mantiene flexible a todo el sistema, haciendo posible la construcción de instalaciones de comunicación con propósitos generales. Cuarto, el esquema permite que los administradores de red agreguen nuevas tecnologías de red al modificar o agregar una pieza sencilla de software nuevo a nivel de red, mientras los programas de aplicación permanecen sin cambios.

4.2.3. PROPIEDADES DE INTERNET.

Conocer el servicio universal es importante, ya que puede haber muchas ejecuciones de servicio universales. En el diseño, queremos ocultar al usuario la arquitectura subyacente de la red de redes. Esto es, no se quiere obligar a que los usuarios o los programas de aplicación entiendan los detalles de las interconexiones del hardware para utilizar la red de redes. Tampoco se quiere imponer una topología de interconexión de red. En particular, agregar una nueva red a la red de redes no debe implicar la añadidura de conexiones físicas directas entre la nueva red y las redes ya existentes. Se quiere ser capaz de

enviar datos a través de redes intermedias aunque no estén conectadas en forma directa a las máquinas de origen o destino.

4.2.4. ARQUITECTURA DE INTERNET.

Físicamente. Dos redes sólo pueden conectarse por medio de una computadora en medio de las dos. Sin embargo, una conexión no proporciona la interconexión que tenemos en mente, debido a que dicha conexión no garantiza que la computadora cooperará con otras máquinas que se desean comunicar. Para obtener una red de redes viable, necesitamos computadoras que estén dispuestas a intercambiar paquetes de una red a otra. Las computadoras que interconectan dos redes y transfieren paquetes de una a otra, se conocen como compuertas de red de redes o ruteadores de red de redes.

En la figura 4.1. en la figura, el ruteador R conecta las red 1 y 2. Para que R actúe como ruteador, debe capturar y transferir los paquetes de la red1 que estén dirigidos a las máquinas de la red 2. De manera similar, R debe capturar y transferir los paquetes de la red 2 que estén dirigidos a las máquinas de la red 1.

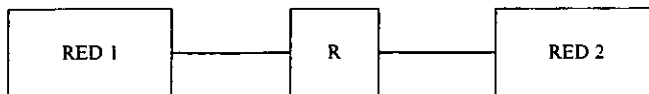


FIGURA 4.1. DOS REDES FÍSICAS INTERCONECTADAS POR R (UN RUTEADOR).

En la figura 4.1, las formas que representan nubes se utilizan para denotar redes físicas, ya que el hardware específico no es importante. Cada red puede ser una LAN o una WAN, y cada una puede tener pocos o muchos anfitriones conectados.

4.3. DIRECCIONES INTERNET.

En este punto se analizarán las direcciones de una de redes. Un ingrediente esencial que le ayuda al software TCP/IP a ocultar los detalles de las redes físicas y hace que la red de redes parezca una sola entidad uniforme. Esto se realiza mediante el protocolo IP que también es el encargado directo de realizar la conectividad dentro de una red homogénea.

IDENTIFICADORES UNIVERSALES.

Un sistema de comunicaciones es universal si permite que cualquier computadora anfitrión se comunique con cualquier otro anfitrión. Para lograr esto, hay que establecer un método aceptado globalmente para identificar a otras computadoras que estén conectadas a la red si las dos computadoras se encuentran en una misma red homogénea la conexión se llama conectividad.

A menudo, los identificadores de anfitrión se clasifican como nombres, direcciones o rutas. Shock (1978) sugiere que un nombre identifica lo que un objeto es una dirección identifica donde está y una ruta indica cómo llegar hasta ahí. Aunque estas definiciones son intuitivas, pueden ser confusas. Los nombres, direcciones y rutas se refieren a representaciones sucesivas de bajo nivel de identificadores de anfitrión. En general, las personas prefieren nombres

pronunciables para identificar máquinas, mientras que el software trabaja de manera más eficiente con representaciones compactas de los identificadores que nosotros conocemos como direcciones. Este término también se pudo haber llamado identificadores universales de anfitrión TCP/IP.

TIPOS PRIMARIOS DE DIRECCIONES IP.

En una red de redes como en una gran red igual a cualquier otra red física. La diferencia es que la red de redes tiene una estructura virtual, imaginada por sus diseñadores, e implantada totalmente en software. Por lo tanto, los diseñadores son libres de elegir el formato y tamaño de los paquetes, las direcciones, las técnicas de entrega, y así en adelante, nada es direccionado por el hardware. Para las direcciones, los diseñadores del TCP/IP eligen un esquema análogo al direccionamiento en las redes físicas, en el que cada anfitrión en la red de redes tiene asignada una dirección de número entero de 32 bits, llamada su dirección de red de redes o dirección IP. La parte inteligente del direccionamiento en una red de redes es que los números enteros son seleccionados con cuidado para hacer eficiente el ruteo. De manera específica, una dirección IP codifica la identificación de la red a la que se conecta al anfitrión en una red de redes TCP/IP tiene asignada una dirección de número entero de 32 bits que se utiliza en todas las comunicaciones con dicho anfitrión.

Los detalles de una dirección IP nos ayudan a entender mejor las ideas abstractas. En el caso más sencillo, cada anfitrión conectado a la red de redes tiene asignado un identificador universal de 32 bits como su dirección dentro de la red, los bits de dirección IP de todos los anfitriones en una red comparten un prefijo común.

Conceptualmente, cada dirección es un par (netid, hostid), en donde netid identifica una red y hostid un anfitrión dentro de la red. Cada dirección IP debe tener una de las primeras tres formas mostradas en la figura 4.2.

Definida una dirección IP, se puede determinar su tipo según los tres bits de orden, de los que son necesarios sólo dos bits para distinguir entre los tres tipos primarios. Las direcciones tipo A, que se utilizan para las pocas redes que tiene más de 2^{16} de anfitriones (por ejemplo, 65, 536), asignan 7 bits al campo netid al campo netid y 24 bits al campo hostid. Las direcciones tipo B, que se utilizan para redes de tamaño mediano que tiene entre 2^8 (por ejemplo, 256) y 2^{16} anfitriones, asignan 14 bits al campo netid y 16 bits al hostid. Por último, las direcciones tipo C, que tienen menos de 2^8 anfitriones, asignan 21 bits al campo netid y solo 8 bits al hostid.

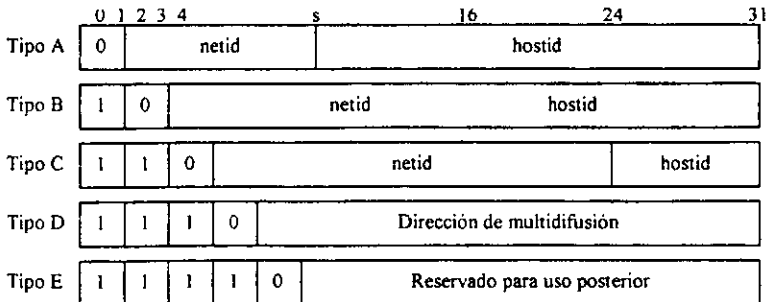


FIGURA 4.2 LAS CINCO FORMAS DE DIRECCIONES DE INTERNET (IP)

NOTACIÓN DECIMAL CON PUNTOS.

Las direcciones IP se pueden escribir, como un conjunto de cuatro enteros decimales separados por puntos, en donde cada entero proporciona el valor de un octeto de la dirección IP. Por lo tanto, la dirección de 32 de una red de redes es:

1000000 00001010 00000010 00011110

se escribe:

128.10.2.30

Se utiliza la notación decimal cuando se expresan direcciones IP. La mayor parte del software TCP/IP que muestran una dirección IP o que requiere que una persona la introduzca, utiliza la notación decimal con puntos.

4.4. PROTOCOLO ARP.

El protocolo ARP (Address Resolution Protocol) es el encargado de realizar el mapeo de direcciones IP a direcciones físicas. En este protocolo la conectividad es muy importante ya que este protocolo se trabaja en el nivel de Internet la cual se conecta con la capa inferior (interfaz de red) llamándose este proceso conectividad.

Se ha descrito el esquema de direcciones TCP/IP, en el que cada anfitrión tiene asignada una dirección de 32 bits así mismo se ha dicho que una red de

redes se comporta como una red virtual que utilizan solo direcciones asignadas cuando envía y recibe paquetes también se han revisado muchas tecnologías de redes físicas y hemos notado que dos máquinas en una red física se pueden comunicar solamente si conocen sus direcciones físicas de red, lo que no se ha mencionado es como un anfitrión o un ruteador transforma una dirección IP en la dirección física correcta cuando necesita enviar un paquete a través de una red física.

TIPOS DE DIRECCIONES FÍSICAS.

Existen dos tipos básicos de direcciones físicas, ejemplificados por Ethernet que tienen direcciones físicas grandes y fijas, así como por proNET que tienen direcciones físicas cortas y de fácil configuración. La asociación de direcciones es difícil para las redes de tipo Ethernet, pero resulta sencilla para las redes proNET.

ENCAPSULACIÓN E IDENTIFICACIÓN DE ARP.

Cuando los mensajes ARP viajan de una máquina a otra, se deben transportar en tramas físicas. En la figura 4.3, se muestra como se transporta el mensaje ARP, en la porción de datos de una trama.

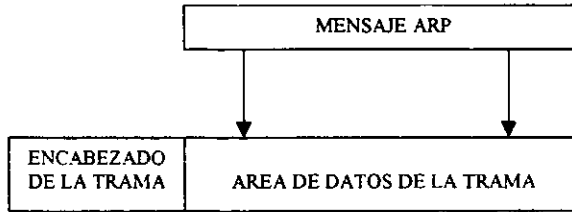


FIGURA 4.3 MENSAJE ARP ENCAPSULADO EN UNA TRAMA DE RED FÍSICA.

Para identificar que la trama transporta un mensaje ARP, el transmisor asigna un valor especial al campo de tipo en el encabezado de la trama y coloca el mensaje ARP en el campo de datos de la misma, cuando llega una trama a una computadora, el software de red utiliza el campo de tipo de trama para determinar su contenido. En la mayor parte de las tecnologías, se utiliza un solo valor para el tipo de todas las tramas que transporta un mensaje ARP. El software de red en el receptor debe examinar el mensaje ARP para distinguir entre solicitudes y respuestas.

4.5. PROTOCOLO ICMP.

El protocolo Internet de control de mensajes (ICMP), utiliza IP como si fuera un protocolo de capa superior, realizado por todos los anfitriones IP, envía mensajes de error y de control.

En el sistema sin conexión que se ha descrito hasta ahora, cada ruteador opera de manera automática, ruteando o entregando los datagramas que llegan sin coordinarse con el transmisor original. El sistema trabaja bien si todas las

máquinas funcionan de manera correcta y si están de acuerdo respecto a las rutas.

Por desgracia, ningún sistema funciona bien todo el tiempo. Además de las fallas en las líneas de comunicación y en los procesadores, el IP tiene falla en la entrega de datagramas cuando las máquinas de destino están desconectadas temporal o permanentemente de la red, cuando el contador de tiempo de vida expira, o cuando los ruteadores intermedios se consignan tanto que no pueden procesar el tráfico entrante. La más importante diferencia entre tener una sola red implantada con hardware dedicada y tener una red de redes implantada con software es que, en el primer caso, el diseñador puede añadir hardware especial para informar a los anfitriones conectados cuando surge un problema. En una red de redes que no tiene un mecanismo de hardware como el anterior, un transmisor no puede indicar si ocurrió una falla en la entrega original por un mal funcionamiento local o remoto. La depuración se vuelve muy difícil. El protocolo IP, por si mismo, no contiene nada para ayudar al transmisor a comprobar la conectividad ni para ayudarlo a aprender sobre dichas fallas.

Para permitir que los ruteadores en una red de redes reporten los errores o proporcionen información sobre circunstancias inesperadas, los diseñadores agregaron a los protocolos TCP/IP un mecanismo de mensajes de propósito especial. El mecanismo, conocido como protocolo de mensajes de Control Internet (ICMP), se considera como parte obligatoria de IP y se debe incluir en todas las implantaciones IP.

CORRECCIÓN DE ERRORES.

Técnicamente, el ICMP es un mecanismo de reporte de errores. Proporciona una forma para que ruteadores que encuentren un error lo reporten en la fuente original. Aunque la especificación del protocolo subraya los usos deseables del ICMP y sugiere acciones posibles para responder a los reportes de error, el ICMP no especifica del todo la acción que debe tomarse para cada posible error. Cuando un datagrama causa un error, el ICMP sólo puede reportar la condición del error de la fuente original del datagrama: la fuente debe relacionar el error con un programa de aplicación individual o debe tomar alguna otra acción para corregir el problema.

La mayor parte de los errores provienen de la parte original, pero otros no. Sin embargo, debido a que el ICMP reporta los problemas a la fuente original, no se puede utilizar para informar los problemas de los ruteadores intermedios. Por ejemplo, suponga que un datagrama sigue en camino a través de una secuencia de ruteadores, R1, R2...Rk si Rk tiene información de ruteo incorrecta, y, por un error, rutea el datagrama hacia el ruteador Re, éste no podrá utilizar el ICMP para reportar el error de Rk, sino para comunicarse sólo con la fuente original.

Un datagrama sólo contiene campos que especifican la fuente original y el último destino: no contiene un registro completo de su viaje a través de la red de redes (a excepción de casos inusuales en los que se utiliza la opción de registro de ruta). Además, como los ruteadores pueden establecer y cambiar sus propias tablas de ruteo, no existe un conocimiento global de las rutas. Por lo tanto, cuando un datagrama llega a un ruteador, es posible conocer el camino

que siguió para llegar hasta ahí. Sin embargo, si detecta un problema, no puede saber que grupo de máquinas intermedias procesaron el datagrama, así que no puede informarles del problema. En vez de descartar discretamente el datagrama.

4.6. PROTOCOLO UDP.

En el grupo de protocolos TCP/IP, el protocolo de datagrama de usuario o UDP proporciona el mecanismo primario que utilizan los programas de aplicación para enviar datagramas a otros programas de aplicación. El UDP proporciona puertos de protocolo utilizados para distinguir entre muchos programas que se ejecutan en la misma máquina. Esto es, además de los datos, cada mensaje UDP contiene tanto el número de puerto de destino como el número de puerto de origen, haciendo posible que el software UDP en el destino entregue el mensaje al receptor correcto y que ése envíe una respuesta.

El UDP utiliza el Protocolo Internet subyacente para transportar un mensaje de una máquina a otra y proporciona la misma semántica de entrega de datagrama, sin conexión y no confiable que el IP. No emplea acuses de recibo para asegurarse de que llegan mensajes, no ordena mensajes entrantes, ni proporciona retroalimentación para controlar la velocidad a la que fluye la información entre las máquinas. Por lo tanto, los mensajes UDP se pueden perder, duplicar o llegar sin orden.

Además, los paquetes pueden llegar más rápido de lo que el receptor los puede procesar. El protocolo de datagramas de usuario (UDP) proporciona un servicio de entrega sin conexión y no confiable, utilizando el IP para

transportar mensajes entre máquinas. Emplea el IP para llevar mensajes, pero agrega la capacidad para distinguir entre varios destinos dentro de una computadora anfitrión.

Un programa de aplicación que utiliza el UDP acepta toda la responsabilidad por el manejo de problemas de confiabilidad, incluyendo a la pérdida, duplicación y retraso de los mensajes, la entrega fuera de orden y la pérdida de conectividad. Por desgracia los programadores de aplicaciones a menudo olvidan estos problemas cuando diseñan software. Además, como los programadores a menudo prueban el software de red utilizando redes de área local, altamente confiables y de baja demora, el procesamiento de pruebas puede no evidenciar las fallas potenciales. Por lo tanto, muchos programadores de aplicación que confían en el UDP trabajan bien en un ambiente local, pero fallan dramáticamente cuando se utilizan en una red de redes TCP/IP más grande.

ENCAPSULACIÓN DE UDP Y CONECTIVIDAD DE PROTOCOLOS.

El UDP es un protocolo de transporte, el UDP reside sobre la capa del Protocolo Internet. Conceptualmente, los programas de aplicación accesan el UDP, que utiliza el IP para enviar y recibir datagramas como se muestran en la figura 4.4.

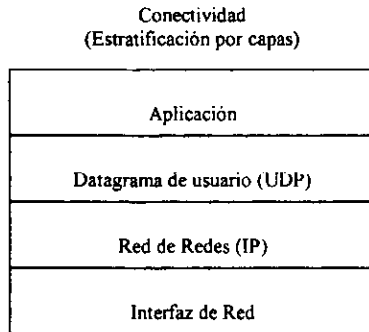


FIGURA 4.4. ESTRATIFICACIÓN CONCEPTUAL POR CAPAS DE UDP ENTRE PROGRAMAS DE APLICACIÓN E IP.

Estratificar por capas el UDP por encima del IP significa que un mensaje UDP completo, incluye el encabezado UDP y los datos, se encapsula en un datagrama IP mientras viaja a través de una red de redes, tal como se muestra en la figura 4.5.

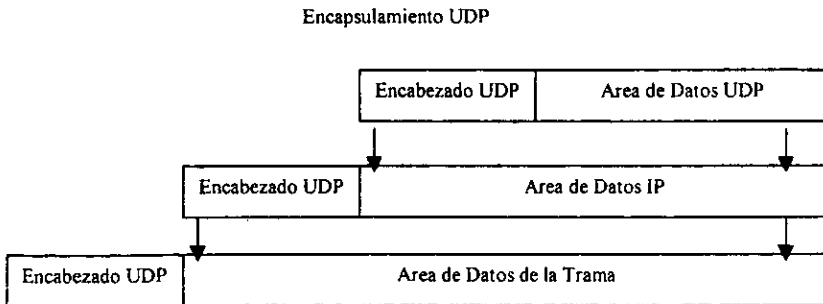


FIGURA 4.5 DATAGRAMA UDP ENCAPSULADO EN UN DATAGRAMA IP PARA SU TRANSMISIÓN A TRAVÉS DE UNA RED DE REDES.

La capa IP sólo es responsable de transferir datos entre un par de anfitriones dentro de una red de redes, mientras que la capa UDP solamente es responsable de diferenciar entre varias fuentes o destinos dentro de un anfitrión.

4.7. PROTOCOLO TCP.

El protocolo de control de transmisión TCP (Transmission Control Protocol), se trata de un protocolo del nivel de transporte orientado a conexión, que ofrece un servicio seguro de transporte de grupos de octetos. La conexión se realiza en modo full dúplex, por lo tanto, soporta una comunicación simultánea en los dos sentidos. El protocolo utiliza como UDP, el mecanismo de puerto.

En el nivel más bajo, las redes de comunicación por computadora proporcionan una entrega de paquetes no confiable. Los paquetes se pueden perder o destruir cuando los errores de transmisión interfieren con los datos, cuando falla el hardware o cuando las redes se sobrecargan demasiado. Las redes que rutean dinámicamente los paquetes pueden entregarlos en desorden, con retraso o duplicado. Además, las tecnologías subyacentes de red pueden dictar un tamaño óptimo de paquete o formular otras obligaciones necesarias para lograr velocidades eficientes de transmisión. En el nivel más alto, los programas de aplicación a menudo necesitan enviar grandes volúmenes de datos de una computadora a otra. Utilizar un sistema de entrega sin conexión y no confiable para la transferencia de gran volumen se vuelve tedioso, molesto y requiere que los programadores incorporen, en cada programa de aplicación, la detección y solución de errores. Debido a que es difícil diseñar, entender o

modificar el software que proporciona confiabilidad, muy pocos programadores de aplicación tienen los antecedentes técnicos necesarios.

4.7.1. CARACTERÍSTICAS.

La interfaz entre los programas de aplicación y el servicio TCP/IP de entrega confiable se puede caracterizar por cinco funciones.

Orientación de flujo. Cuando dos programas de aplicación (procesos de usuario) transfieren en grandes volúmenes de datos, pensamos en los datos como flujo de bits, divididos en octetos de 8 bits, que informalmente se conocen como bytes. El servicio de entrega de flujo en la máquina de destino pasa al receptor exactamente la misma secuencia de octetos que le pasa el transmisor en la máquina de origen.

Conexión del circuito virtual. La transferencia de flujo es análoga a realizar una llamada telefónica. Antes de poder empezar la transferencia, los programas de aplicación, transmisor y receptor interactúan con sus respectivos sistemas operativos, informándose de la necesidad de realizar una transferencia de flujo.

Transferencia con memoria intermedia. Los programas de aplicación envían un flujo de datos a través del circuito virtual pasando repetidamente octetos de datos al software de protocolo. Cuando transfieren datos, cada aplicación utiliza piezas del tamaño que encuentre adecuado, que pueda ser tan pequeña como un octeto. En el extremo receptor, el software de protocolo entrega octetos del flujo de datos en el mismo orden en que se enviaron,

poniéndolos a disposición del programa de aplicación receptor tan pronto como se reciben y verifican.

Flujo estructurado. Importante entender que el servicio de flujo TCP/IP no está obligado a formar flujo estructurado de datos.

Conexión full dúplex. Las conexiones proporcionadas por el servicio de flujo TCP/IP permiten la transferencia concurrentemente en ambas direcciones. Dichas conexiones se conocen como Full Dúplex. Desde el punto de vista de un proceso de aplicación, una conexión Full Dúplex consiste en dos flujos independientes que se mueven en direcciones opuestas, sin ninguna interacción aparente.

4.7.2. TELNET.

El conjunto de protocolos TCP/IP incluye un protocolo de terminal remota sencillo, llamada TELNET. TELNET permite al usuario de una localidad establecer una conexión TCP con un servidor de acceso a otro. TELNET transfiere después las pulsaciones de teclado directamente desde el teclado del usuario a la computadora remota como si hubiesen sido hechos en un teclado unido a la máquina remota, TELNET también transporta la salida de la máquina remota de regreso a la pantalla del usuario. El servicio se llama *transparent* (transparente) por que da la impresión de que el teclado y monitor del usuario están conectados de manera directa a la máquina remota.

Un usuario se convierte a TELNET, un programa de aplicación en la máquina del usuario se convierte en el cliente. El cliente establece una

conexión TCP con el servidor por medio de la cual se comunicarán. Una vez establecida la conexión con el cliente acepta los pulsos de teclado del usuario y los manda al servidor, al tiempo que acepta caracteres de manera concurrente que el servidor regresa y despliega en la pantalla del usuario. El servidor debe aceptar una conexión TCP del cliente y después transmitir los datos entre la conexión TCP y el sistema operativo local.

Utilizamos el término pseudo terminal para describir el punto de entrada del sistema operativo que permite que un programa que se está corriendo como servidor TELNET, transfiera caracteres al sistema operativo, como si vinieran de un teclado. Es imposible construir un servidor TELNET a menos que el sistema operativo proporcione dicha característica. Si el sistema soporta la abstracción de una pseudo terminal, el servidor TELNET podrá implantarse con programas de aplicación. Cada servidor esclavo conecta una corriente TCP de un cliente a una pseudo terminal en particular.

El arreglo del servidor TELNET para que sea un programa de nivel de aplicación tiene sus ventajas y sus desventajas. La ventaja más obvia es que hace la modificación y el control más fácil que si el código estuviera esclavo en el sistema operativo. La desventaja evidente es su ineficiencia. Cada pulso de teclado viaja del teclado del usuario a través del sistema operativo hacia el programa cliente, el programa cliente regresa a través del sistema operativo y a través de la red de redes hacia la máquina servidor.

4.7.3. FTP.

FTP es el mayor protocolo de TCP/IP para la transferencia de archivos, se da entre las aplicaciones TCP/IP utilizadas con mayor frecuencia, y cuenta con mucho tráfico en red. Existían protocolos de transferencia de archivos estándar para ARPANET antes de que comenzara a funcionar TCP/IP. Estas versiones tempranas de software de transferencia de archivos evolucionaron hasta llegar al estándar actual, conocido como file transfer protocol (FTP protocolo de transferencia de archivos).

CARACTERÍSTICAS.

Dado un protocolo de transferencia confiable de extremo a extremo como el TCP, la transferencia de archivos podría ser trivial sin embargo, como se ha señalado anteriormente, los detalles de autorización el nombre y la representación entre máquinas heterogéneas hace que el protocolo sea complejo, además el FTP, ofrece muchas facilidades que van más allá de la función de transferencia misma.

Acceso interactivo. Aunque el FTP está diseñado para usarse mediante programas, la mayor parte de las implantaciones proporcionan una interfaz interactiva que permite a las personas interactuar fácilmente con los servicios remotos.

Especificación de formato (representación). el FTP permite al cliente especificar el tipo de formato de datos almacenados (ASCII o EBCDIC)

Control de atenuación. El FTP permite que los clientes se autoricen así mismos con el envío de un nombre de conexión y una clave de acceso al servidor antes de pedir la transferencia de archivo.

MODELO DE PROCESO FTP.

La mayor parte de las implantaciones FTP de servidores permiten el acceso concurrente de varios clientes. Los clientes se valen del TCP para conectarse a un servidor. Un proceso sencillo de servidor maestro espera las conexiones y crea un proceso esclavo para manejar cada conexión. Sin embargo, a diferencia de casi todos los servidores, el proceso esclavo no ejecuta todos los cálculos necesarios. Por el contrario, el esclavo capta y maneja la conexión de control de cliente pero utiliza un proceso (o procesos) adicional para manejar una conexión de transferencia de datos separada. La conexión de control transporta comandos que indican al servidor que archivo transferir. La conexión de transferencia de datos, que también usa el TCP como protocolo de transporte, transporta todas las transferencias de datos.

El proceso de control de cliente se conecta al proceso de servidor mediante una conexión TCP. En general los procesos de conexión y la conexión de control permanecen activos mientras el usuario continúa con la sesión FTP. Sin embargo el FTP establece una nueva conexión de transferencia de datos para cada transferencia de archivos.

4.8. PROTOCOLO SMTP.

El protocolo de transferencia estándar se conoce como SMTP, Simple Mail Transfer Protocol (Protocolo de Transferencia de correo simple). El SMTP es más sencillo que el Mail Transfer Protocol, MTP original. El protocolo SMTP se enfoca específicamente en cómo se transfiere el sistema de entrega de correo subyacente los mensajes a través de un enlace de una máquina a otra. No especifica de qué manera acepta el sistema de correo los mensajes de correo de un usuario o cómo presenta al usuario la interfaz de usuario el correo entrante. El SMTP tampoco especifica en qué forma se almacena el correo o con qué frecuencia el sistema de correo trata de enviar mensajes.

El SMTP es sorprendentemente sencillo. La comunicación entre un cliente y un servidor consiste en texto ASCII que es posible leer. Aún cuando el SMTP define rígidamente el formato de los comandos, los usuarios pueden leer fácilmente, el cliente establece una conexión de flujo confiable con el servidor y espera que el servidor envíe un mensaje 220 READY FOR MAIL. Al recibir el mensaje 220, el cliente envía un comando HELLO. El extremo de una línea marca el fin de un comando. El servidor responde identificándose. Una vez que la comunicación se ha establecido, el emisor puede enviar uno o más mensajes de correo, terminar la conexión o solicitar al servidor que intercambie las funciones de emisor y receptor para que los mensajes puedan fluir en la dirección opuesta. El receptor debe enviar un acuse de recibo por cada mensaje.

4.9. CONECTIVIDAD EN TCP/IP.

La conectividad en el protocolo TCP/IP no es otra cosa que la estratificación por capas de protocolos o sea que los principios generales de la conectividad por capas, se muestran en las capas del software de protocolo de Internet, y esto es, que los datagramas fluyen sobre las capas, a través del software de protocolo.

4.9.1. LA CONECTIVIDAD ENTRE CAPAS DEL PROTOCOLO.

Se hace una analogía en los módulos del software de protocolo, como una pila vertical constituida por capas, como se muestra en la figura 4.6. cada capa tiene la responsabilidad de manejar una parte del problema.

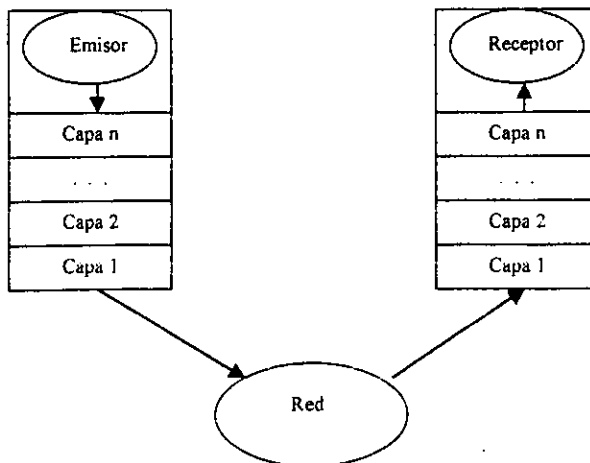


FIGURA 4.6. ORGANIZACIÓN CONCEPTUAL DEL SOFTWARE DE PROTOCOLO EN CAPAS.

Conceptualmente, enviar un mensaje desde un programa de aplicación en una máquina hacia un programa de aplicación en otra, significa transferir el mensaje a través de la red y, luego, transferir el mensaje hacia arriba, a través de las capas sucesivas del software de protocolo en la máquina receptora ese proceso es al que se le conoce como conectividad dentro de una red.

El software de protocolo es mucho más complejo de lo que se muestra en el modelo simplificado de la figura 4.8. cada capa toma decisiones acerca de lo correcto del mensaje y selecciona una acción apropiada con base en el tipo de mensaje o la dirección de destino.

Para entender la diferencia entre la organización conceptual del software de protocolo y los detalles de implantación, consideremos la comparación que se muestra en la figura 4.7. El diagrama conceptual en la figura 4.7a, muestra una capa de Internet entre una capa de protocolo de alto nivel y una capa de interfaz de la red. El diagrama de la figura 4.7b, muestra el hecho de que el software IP puede comunicarse con varios módulos de protocolo de alto nivel y con varias interfaces de red.

Aun cuando un diagrama conceptual de la conectividad por capas no muestra todos los detalles, sirve como ayuda para explicar los conceptos, generales. En la figura 4.8, muestra las capas de software de protocolo utilizadas por un mensaje que atraviesa tres redes. El diagrama muestra sólo la interfaz de la red y las capas de Protocolo Internet en los ruteadores debido a que sólo estas capas son necesarias para recibir, rutear y enviar los datagramas. Se entiende que cualquier máquina conectada hacia dos redes debe tener dos

módulos de interfaz de red, aunque el diagrama de conectividad muestra sólo una capa de interfaz de red en cada máquina.

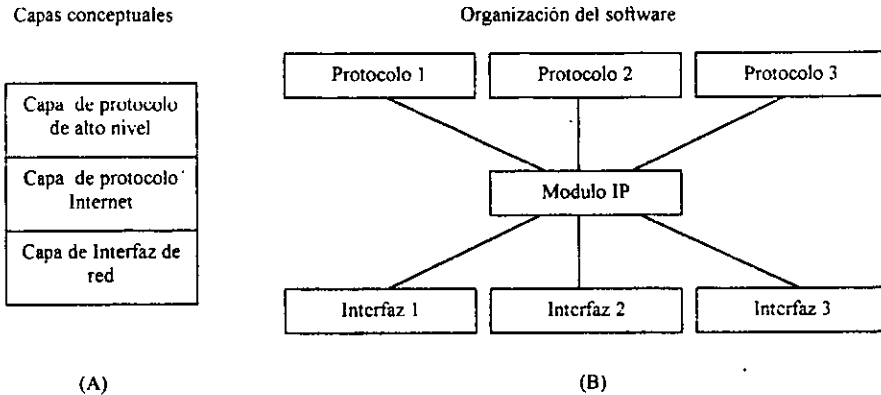


FIGURA 4.7 UNA COMPARACIÓN DE (A) CONECTIVIDAD DE PROTOCOLOS Y (B) UNA VISIÓN DE LA ORGANIZACIÓN DEL SOFTWARE QUE MUESTRA VARIAS INTERFACES DE RED ENTRE IP Y VARIOS PROTOCOLOS.

Como se muestra en la figura 4.8, un emisor en la máquina original transmite un mensaje que la capa de IP coloca en un datagrama de regreso, nuevamente (hacia una red diferente). Sólo cuando se alcanza la máquina en el destino final IP extrae el mensaje y lo pasa hacia arriba, hacia las capas superiores del software de protocolo.

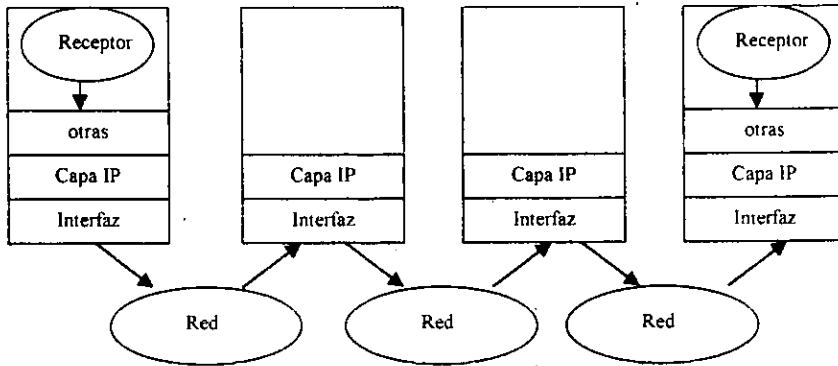


FIGURA 4.8. EL MODELO DE CONECTIVIDAD POR CAPAS DE TCP/IP DE INTERNET

El segundo modelo mayor de conectividad proviene de las investigaciones que se realizan respecto al conjunto de protocolos de TCP/IP. Con un poco de esfuerzo, el modelo ISO puede ampliarse y describe el esquema de conectividad del TCP/IP, pero los presupuestos subyacentes son lo suficientemente distintos para distinguirlos como dos diferentes.

El software TCP/IP está organizado en cuatro capas conceptuales que se construyen sobre una quinta capa de hardware.

Capa de aplicación. En el nivel más alto, los usuarios llaman a una aplicación que accesa servicios disponibles a través de la red de redes TCP/IP. Una aplicación interactúa con uno de los protocolos de nivel de transporte para enviar o recibir datos. Cada programa de aplicación selecciona el tipo de transporte necesario, el cual puede ser una secuencia de mensajes individuales

o un flujo continuo de octetos. El programa de aplicación pasa los datos en ña forma requerida hacia el nivel de transporte para su entrega.

Capa de transporte. La capa de transporte proporciona la comunicación entre un programa de aplicación y otro. Este tipo de comunicación se conoce frecuentemente como comunicación punto a punto. La capa de transporte confiable, asegurando que los datos lleguen sin errores y en secuencia. Para hacer esto, el software de protocolo de transporte tiene el lado de recepción enviando acuses de recibo de retorno y la parte de envío retransmitiendo los paquetes perdidos. El software de transporte divide el flujo de datos que se está enviando en pequeños fragmentos (por lo general conocidos como paquete) y pasa cada paquete, con una dirección de destino, hacia la siguiente capa de transmisión.

Capa Internet. La capa Internet maneja la comunicación de una máquina a otra. Esta acepta una solicitud para enviar un paquete desde la capa de transporte, junto con una identificación de la máquina, hacia la que se debe enviar el paquete. Encapsulado el paquete en un datagrama IP, llena el encabezado del datagrama, utiliza un algoritmo de ruteo para determinar si puede entregar el datagrama directamente o si debe enviarlo a un ruteador y pasar el datagrama hacia la interfaz de red apropiada para su transmisión. La capa Internet también maneja la entrada de datagramas, verifica su validez y utiliza un algoritmo de ruteo para decidir si el datagrama debe procesar de manera local, el software de la capa de red de redes borra el encabezado del datagrama y selecciona, de entre varios protocolos de transporte, un protocolo con el que manejará el paquete. Por último, la capa Internet envía los mensajes

ICMP de error y control necesarios y maneja todos los mensajes ICMP entrantes.

Capa de interfaz de red. El software TCP/IP de nivel inferior consta de una capa de interfaz de red responsable de aceptar los datagramas IP y transmitirlos hacia una red específica. Una interfaz de red puede consistir en un dispositivo controlador (por ejemplo, cuando la red es una red de área local a la que las máquinas están conectadas directamente) o un complejo subsistema que utiliza protocolo de enlace de datos (por ejemplo, cuando la red consiste de conmutadores de paquetes que comunican con anfitriones utilizando HDLC).

4.9.2. CONECTIVIDAD DE PROTOCOLOS.

Independientemente del esquema de conectividad que se utiliza o de las funciones de las capas, la operación de los protocolos estratificados por capas se basa en una idea fundamental, la idea, conocida como principio de conectividad puede resumirse de la siguiente forma:

Los protocolos estratificados por capas están diseñados de modo que una capa n en el receptor de destino, reciba exactamente el mismo objeto enviado por la correspondiente capa n de la fuente.

La conectividad permite que el diseñador de protocolos enfoque su atención hacia la capa a la vez sin preocuparse acerca del desempeño de las capas inferiores. Cuando se constituye una aplicación para transferencia de archivos, el diseñador piensa sólo en dos copias del programa de aplicación que se correrá en dos máquinas y se concentrará en los mensajes que se necesitan

intercambiar para la transferencia de archivos. El diseñador asume que la aplicación en el anfitrión receptor es exactamente la misma que el anfitrión emisor.

CAPÍTULO V. ANALISIS COMPARATIVO ENTRE OSI, SNA Y TCP/IP.

Objetivo:

Realizar un estudio comparativo de las arquitecturas de OSI, TCP/IP y SNA.

CAPÍTULO V. ANALISIS COMPARATIVO ENTRE OSI, SNA Y TCP/IP.

Es fácil entender que, en las capas superiores, el principio de conectividad se aplica a través de la transferencia punto a punto y que en las capas inferiores se aplica en una sola transferencia de máquina. No es tan fácil ver cómo el principio de conectividad se aplica a la conectividad Internet. Los anfitriones conectados a una red de redes deben considerarse como una gran red virtual, con los datagramas IP que hacen las veces de tramas de red. Desde este punto de vista, los datagramas viajan desde una fuente original hacia un destino final y el principio de la conectividad garantiza que el destino final reciba exactamente el datagrama que envió la fuente. Debemos concluir que, a pesar de que la mayor parte de los datagramas permanecen intactos cuando pasan a través de una red de redes, el principio de conectividad por capas sólo se aplica a los datagramas que realizan transferencias de una sola máquina. Para ser precisos, no debemos considerar que las capas de Internet proporcionan un servicio punto a punto.

A continuación, el presente capítulo se enfocan a dar algunas diferencias entre la conectividad del modelo de referencia OSI; SNA y TCP/IP a partir de las capas que los componen, iniciando así con la Arquitectura de red de sistemas y el Protocolo Internet.

5.1. ANÁLISIS COMPARATIVO ENTRE SNA Y TCP/IP.

Como hemos mencionado en capítulos anteriores, las ventajas de la conectividad en redes, llámese OSI, SNA, o TCP/IP, son muy grandes; pero sólo se manejan dentro de una red de área local. El siguiente capítulo se enfocará al análisis comparativo entre las arquitecturas y/o protocolos que se estudiaron en los capítulos 2, 3 y 4 tomando en cuenta las siguientes observaciones fundamentales sobre el diseño de sistemas de comunicación que hasta hoy en día se toman en cuenta, por tanto diremos que:

Ningún hardware de red por si mismo puede satisfacer todos los requerimientos.

Los usuarios buscan la interconexión universal.

La primera observación es técnica. Las redes de área local, que proporcionan la mayor velocidad de comunicación, están limitadas en cuanto a su alcance geográfico; las redes de área amplia abarcan grandes distancias pero no pueden proporcionar conexiones de alta velocidad. Ninguna tecnología de red por si misma satisface todas las necesidades, así que nos vemos forzados a considerar muchas tecnologías subyacentes de hardware.

La segunda observación es evidente, se tiene la necesidad de poder comunicarnos entre dos puntos cualquiera que éstos sean. En particular, queremos un sistema de comunicación que no esté limitado por las fronteras de las redes físicas.

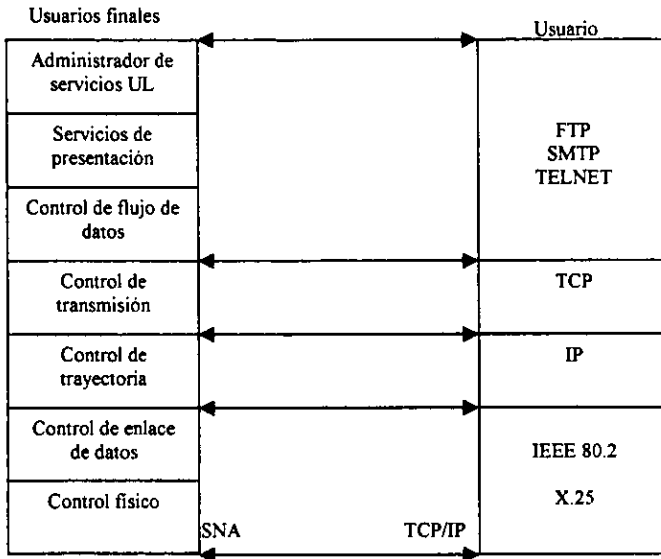


FIGURA 5.1 CORRESPONDENCIA DE CAPAS EN SNA Y TCP/IP.

Las ventajas de TCP/IP en comparación con SNA son muy grandes ya que SNA sólo es compatible con IBM y no se pudiera compartir recursos fuera de esta red y no se cumple con la función primordial de minimizar costos y tiempo para el concepto de las comunicaciones. Para ello se citarán algunas virtudes del protocolo de Internet.

Independencia de la tecnología de red.- Como TCP/IP está basado en una tecnología convencional de conmutación de paquetes, es independiente de cualquier marca de hardware en particular.

Interconexión universal.- Una red de redes TCP/IP permite que se comunique cualquier par de computadoras conectadas a ella. Cada

computadora tiene asignada una dirección reconocida de manera universal dentro de la red de redes.

Estándares de protocolo de aplicación.- Además de los servicios básicos de nivel de transporte, los protocolos TCP/IP incluyen estándares para muchas aplicaciones comunes, incluyendo correo electrónico, transferencia de archivos y acceso remoto.

La meta es construir una interconexión de redes, unificada y cooperativa que incorpore un servicio universal de comunicación. Dentro de la red, las computadoras utilizarán funciones subyacentes de comunicación sin importar la tecnología, el nuevo software, incorporado entre los mecanismos de comunicación de tecnología independiente y los programas de aplicación, ocultarán los detalles de bajo nivel y hará que el grupo de redes parezca ser una sola gran red. Un esquema de interconexión como el que se describe se conoce como red de redes o Internet.

5.2. ANÁLISIS COMPARATIVO ENTRE SNA Y OSI.

Aquí se pretende hacer un análisis comparativo entre ambas arquitecturas, la SNA y la OSI, que semejanzas tiene ambas capas o niveles entre si y también las semejanzas en cuanto a su funcionamiento. En seguida se muestra la figura 5.2 en donde se puede apreciar gráficamente qué nivel de SNA le corresponde a que capa de la arquitectura de OSI en cuanto a su funcionamiento.

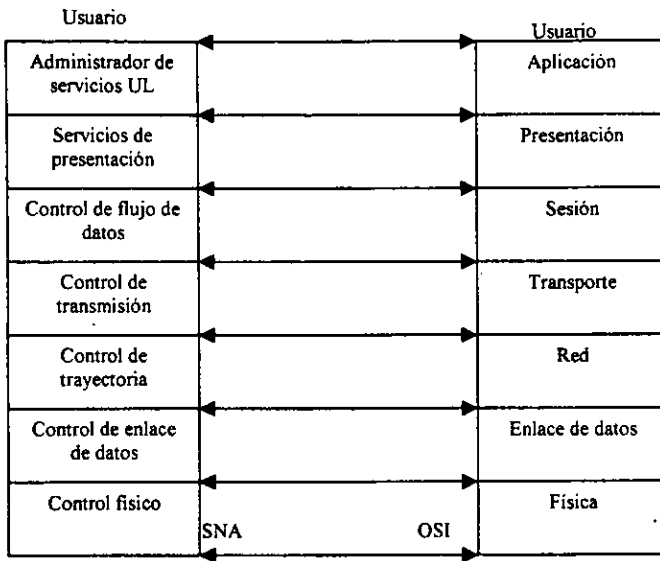


FIGURA 5.2. COMPARACIÓN ENTRE SNA Y OSI.

ADMINISTRADOR DE SERVICIOS UL.

El administrador de servicios de la UL, participa al establecer y dar de baja la sesión, y administra los servicios de la aplicación. Una parte de sus funciones se pueden comparar con la capa de aplicación del modelo OSI.

SERVICIOS DE PRESENTACIÓN.

El nivel de servicios de presentación, ofrece transformación de datos, efectúa la codificación y compresión de datos, y da formato al despliegue; todo esto comparable con la capa de presentación del modelo OSI.

CONTROL DE FLUJO DE DATOS.

Los niveles de control de flujo de datos y de control de transmisión, efectúan algunas funciones en forma conjunta y proporcionan algunos de los servicios de los niveles de protocolos de sesión y de transporte del modelo OSI.

CONTROL DE TRAYECTORIA.

El nivel de control de trayectoria ofrece funciones de encadenamiento y control de congestión (flujo) asociadas con la capa de red del modelo OSI.

CONTROL DE ENLACE DE DATOS.

El nivel de control de enlace de datos (SDLC), es el responsable de la transmisión de unidades de datos sin errores sobre las conexiones entre los nodos, esto comparable con la capa de enlace de datos del modelo OSI.

Existen dos diferentes básicas entre la arquitectura SNA y la OSI al establecer sesiones del usuario final:

Primero.- Que el PCSS esta involucrado de manera activa en SNA.

Segunda.- Que SNA requiere que una UL sea primaria y la otra secundaria.

5.3. ANÁLISIS COMPARATIVO ENTRE TCP/IP Y OSI.

La comparación de TCP/IP con el modelo OSI, es muy frecuente trayendo consigo como se relacionan y en que niveles y funciones son comunes. Se puede observar que el modelo OSI tiene más capas que TCP/IP, pero si se examina la funcionalidad de las capas, se encuentra que las cuatro capas inferiores son compatibles.

Antes de profundizar en el estudio de la relación existente entre OSI y TCP/IP, se debe poner en claro el uso de las siglas "OSI", que a menudo se utilizan para hacer referencia al modelo de referencia Open System Interconexión. También se utilizan para designar una conjunto de protocolos más detallados que se utilizarán como lineamientos para configurar una red OSI real. Cuando se utilizan las siglas "OSI" para referirnos al modelo de referencia se modificaran en la forma adecuada. La figura 5.3 constituye un intento por presentar la relación que existe entre los estratos de TCP/IP, el modelo de referencia OSI y los estándares componentes reales para guiar el desarrollo de sistemas reales.

El lado izquierdo de la figura 5.3 es una presentación de 7 nombres de estratos o niveles del modelo OSI. En el lado derecho de la figura 5.3 hay algunos nombres de estratos de los cuatro niveles de TCP/IP, y en los recuadros están los nombres de los niveles.

El conjunto de protocolos TCP/IP ha sido igualado con los niveles adecuados en el modelo OSI, pero se debe de tener presente que es más sencillo trazar estas figuras que hacer equivalentes en realidad estas componentes. En

general, los estándares de OSI son mucho más vastos, tanto en número como en funcionalidad, que los estándares de TCP/IP. Uno de los desafíos para los usuarios de las redes TCP/IP en los próximos años será la necesidad de emigrar a estándares de OSI.

El objetivo de TCP/IP y OSI es proporcionar un conjunto de protocolos de comunicaciones que sean independientes del fabricante. El motivo del departamento de la Defensa de Estados Unidos para desarrollar TCP/IP a fines de la década de 1970 fue ensanchar la base de hardware y software de la cual tenían que elegir para alentar ofertas competitivas, en vez de encerrarse en una red de propietario como es el caso de la red SNA (Arquitectura de sistema de Red) de IBM.

Sin embargo, con el desarrollo de estándares internacionales, ha quedado claro que en la década de 1990 mucho mayor número de fabricantes soportarán estándares internacionales diferentes de TCP/IP como enfoque principal en el uso de redes. Asimismo, estándares internacionales cuentan con el apoyo de la mayoría de los gobiernos de Europa Occidental, así como también con el respaldo de organizaciones creadoras de estándares. Estos factores, a la par con la mayor funcionalidad y el conjunto de protocolos más numerosos de los estándares internacionales, ha llevado a organizaciones gubernamentales de los Estados Unidos, entre ellas el Departamento de la defensa, a declarar que también cambiarán a OSI en la década siguiente.

La base instalada en redes TCP/IP era mucho mayor de la de las redes con el estándar OSI. Todo esto significa que la migración de redes basadas en TCP/IP a redes OSI tomará varios años, y en algunas aplicaciones puede hacer

cabida para ambas. No obstante, una consecuencia de la necesidad de la migración ha sido un vasto número de obras literarias que abordan el problema del ajuste de TCP/IP a OSI.

TCP/IP (Protocolo de Control de Transmisión/Protocolo Internet), al igual que OSI se desarrolló con una arquitectura en niveles. Se diseñó así para poder intercambiar las partes de cada nivel según el tipo de conexión que se utilizará. Como se concibieron varias tecnologías distintas, las partes tenían que estar estructuradas de forma que sólo fuera necesario cambiar una pieza para utilizarlo en un medio diferente. El modelo OSI se diseñó varios años después que TCP/IP.

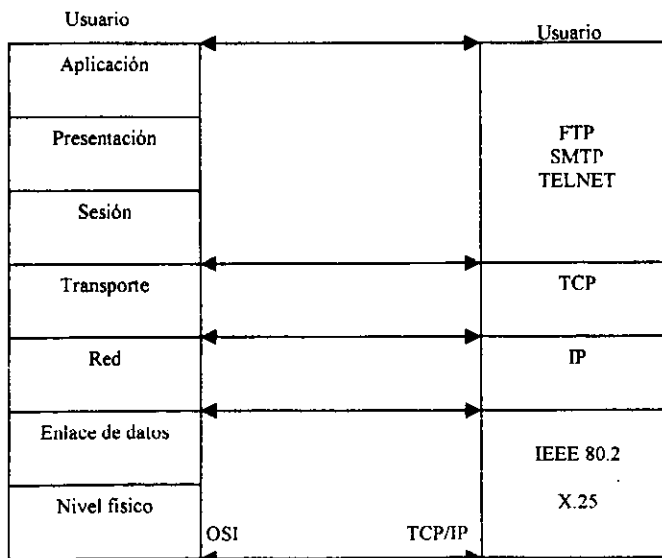


FIGURA 5.3 MODELO TCP/IP Y EL MODELO OSI.

En la figura 5.3 se muestra los niveles o capas del modelo TCP/IP, así también la comparación con el modelo OSI.

Hasta la capa 2, los modelos son compatibles, OSI en las capas 1 2 define diferentes medios donde los sistemas pueden ser usados y TCP/IP fue diseñado para ser independiente del medio, así que en principio, TCP/IP deberá correr en cualquier sistema estándar OSI. En general y observando cuidadosamente los detalles de la configuración, ésta también es utilizada en la práctica y nos permite operar ambos protocolos en los mismos medios.

Cuando consideramos las capas 3 y 4 de Internet, transporte en TCP/IP y la capa de red y transporte de OSI, esta última cuenta con un número de diferentes opciones que pueden ser utilizadas en estas capas. Sin embargo, hay un conjunto de opciones en OSI que producen una funcionalidad casi idéntica a TCP/IP, comparable pero no compatible.

Las mayores diferencias ocurren en la capa de aplicación de TCP/IP. A éste nivel, el sistema OSI separa este nivel en tres capas agregando las capas de sesión y presentación. Esta es quizás la diferencia más significativa entre ambos grupos de protocolos.

Las capas de presentación de OSI tienen que ver con el problema que se mencionó anteriormente, el de llevar e interpretar el significado completo de la información entre computadoras con diferentes arquitecturas.

En OSI el poder de estas funciones es mucho mayor que el tradicional de TCP/IP. Con OSI es mucho más sencillo lograr compatibilidad y la

interoperabilidad entre diferentes sistemas, sin que afecten significativamente su desempeño.

CONCLUSIONES.

Al término del presente trabajo se pudo establecer la diferencia que existe entre interconexión y conectividad en redes digitales, ya que la primera se da en medios heterogéneos y la segunda en medio homogéneos.

También se demostró que el modelo de referencia OSI tiene futuro todavía, y la arquitectura SNA tiende a desaparecer por ser únicamente para redes privadas de IBM.

Cabe mencionar que la arquitectura de una red esta organizada de tal forma que hace posible la comunicación entre diferentes usuarios conectados dentro de la misma red, sin importar la distancia entre estos. Aquí entran en función los protocolos para establecer la comunicación.

En base a la información obtenida sobre TCP/IP se puede concluir que es un protocolo que puede hacer posible que se puedan interconectar todo tipo de redes sin importar su tecnología de fabricación, agregando a esto diremos que TCP/IP opera en redes de gran cobertura así como también en redes muy pequeñas.

Se pudo observar que solo se podían hacer los comparativos entre OSI, SNA y TCP/IP, solo entre arquitectura, ya que SNA es una arquitectura, OSI es un estándar y TCP/IP un protocolo.

BIBLIOGRAFÍA

Mischa Schwartz

Redes de telecomunicaciones

Ed. Addison Wesley

1994.

Thomas W. Madron

Redes de área local

Ed. Noriega editores

1993.

Cheryl, C. Currid

Craig, A. D. Gillet

Domine Novell Netware

Ed. Macrobit Editores, S.A. de C.V

1991.

Benitez, Santana J.L./Nuñez, Rodriguez R.

Principales Sistemas operativos y conectividad

Ed. Compucosmos

1991.

Douglas E. Comer

Redes globales de información con Internet y TCP/IP

Tercera edición

Ed. Prentice-Hall Hispanoamericana, S.A.

1996.

Parker, Tim

Aprendiendo TCP/IP en 14 días

Ed. Prentice-Hall hispanoamericana, S.A.

1995.

González, S. Nestor

Comunicaciones y redes de procesamientos de datos

Ed. Mc. Graw-Hill

1992.

Hermann, J. Helgert

Integrated services digital networks

Ed. Addison Wesley

1991.

Beltraño, M. José Antaño

Redes locales de computadoras

Ed. Mc. Graw-Hill

1991.

Tanenbaum, Andrew S.

Redes de ordenadores

Segunda edición

Ed. Prentice-Hall Hispanoamericana, S.A.

1993.