UNIVERSIDAD NACIONAL
AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
ACATLÁN

ORIGEN Y CARACTERÍSTICAS DEL PROTOCOLO TCP/IP

TESINA

QUE PARA OBTENER EL TÍTULO DE
LICENCIADO EN
MATEMATICAS APLICADAS Y COMPUTACION

P R E S E N T A :

JOSE LUIS MARTINEZ SUAREZ

ASESOR:
M. EN C. SARA CAMACHO CANCINO.

AGOSTO, 2007

ÍNDICE

ÍNDICE DE IMAGENES

Figuras del Capitulo I.

Figuras del Capitulo II.

Figuras del Capitulo III.

INTRODUCCIÓN

Los protocolos de comunicación actualmente son de gran utilidad para realizar muchas tareas rutinarias tales como enviar, recibir y estar comunicados en tiempo real entre máquinas a nivel mundial con igual o diferente plataforma (Windows, Windows NT, Unix, Novell, etc.), por tal razón, es importante entender los medios que están involucrados para lograr estas tareas. En la actualidad la mayoría de usuarios utilizan estos protocolos.

El trabajo está estructurado en tres capítulos:

Capítulo I Introducción a los Protocolos: En este capítulo se deberán entender los conceptos básicos relacionados con los protocolos.

Capítulo II Protocolo TCP/IP: Este protocolo es la base de Internet; entender cómo funciona nos da la pauta para comprender su poderío.

Capítulo III Aplicaciones y Futuro del Protocolo TPC/IP: Se deberá comprender dónde se usa y cuáles son las tendencias del protocolo a fin lograr los objetivos de las tareas diarias.

La intención del estudio es proporcionar una herramienta de consulta rápida, permitiendo comprender la importancia de los protocolos; que generalmente muchos usuarios están en contacto con ellos de una forma rutinaria sin tener una mínima idea de cómo funcionan. Estando dirigido a personas con conocimientos básicos en al ámbito de sistemas, que desde mi punto de vista deben de entender las características y funcionamiento de los protocolos, razón por la cual está elaborado en un lenguaje accesible.

CAPÍTULO I

1. INTRODUCCIÓN A LOS PROTOCOLOS

Un protocolo es un conjunto de reglas y procedimientos establecidos entre dos dispositivos para permitir la comunicación entre ambos, quienes pueden trabajar en conjunto y en jerarquías para este fin, a continuación se describirá su desarrollo histórico, para posteriormente describir su funcionamiento y características.

1.1 ORIGEN

En los años 60´s, prevalecían redes que comunicaban solo a equipos de una sola marca o asociados, como los desarrollados por IBM con arquitectura SNA. Surgiendo paralelamente redes experimentales que conectaban máquinas heterogéneas, siendo de interés superior a las de redes homogéneas. Al surgir la necesidad de interconectar equipos incompatibles, surge el modelo OSI (Internacional Standardización Organization) para sistemas abiertos, debido a los enormes gastos en la capacitación y la migración de aplicaciones, por tal causa surge de un subcomité creado en 1977, para desarrollar un estándar de comunicación entre sistemas heterogéneos.

Dicho modelo simplemente establece las normas de interacción entre los sistemas conectados; no se pronuncia sobre la estructura interna del sistema de comunicación de cada máquina, ni de la relación con su sistema operativo (Uyless (1995) Redes de Computadoras Protocolos, Normas e Interfaces (2da. ed). México: Alfa Omega). Véase (tabla 1.1).

AÑO	RED	PROPOSITO	ALCANCE
1969	ARPANET (Advanced Research Projects Agency)	Conectar computadoras distantes de forma flexible y dinámica.	A principios de los 80 ya se conectaban unas 100 computadoras y servía como lenguaje de comunicación a la familia de protocolos TCP/IP
	Red independiente CSNET (Computer Science Nerwork) y la MILNET (red militar del departamento de defensa)	Utilizaron los protocolos TCP/IP para interconectar sus equipos.	
1983	Interconectaron las tres redes ARPANET, CSNET y MILNET naciendo la red de redes: INTERNET	La esencia de la operación fueron los protocolos TCP/IP	Permite comunicarse con computadoras de diferentes entornos con UNIX, MS-DOS o MacOS.
1986	NSFnet (National Science Foundation)	Para facilitar el acceso de toda la comunidad científica americana a cinco grandes centros de supercomputarización.	Se convirtió en la espina dorsal de Internet.
1992	Creación de la Internet Society (ISOC).	Integra todas las organizaciones y empresas implicadas en construir la red. Su objetivo será consensual las acciones de extensión de Internet.	Su objetivo será consensuar las acciones de extensión de Internet.
1994			El número de "hosts" conectados era de tres millones y se habían llegado a integrar 25.000 redes de 146 países.
Actualmente	Internet		Es la red más grande, más poderosa e indispensable en todos los rublos en el que interfieren los seres humanos.

Tabla 1.1

1.2 FUNCIÓN

Entendemos por protocolo al conjunto de reglas y procedimientos en toda comunicación, aplicada en el entorno dos o más equipos conectados en red, a estas reglas y procedimientos técnicos que dictan su comunicación e interacción se denominan protocolos.

Los protocolos de red involucran estos tres puntos:

1 La existencia de muchos protocolos. Éstos facilitan la comunicación básica, teniendo como propósito diferentes y distintas tareas, además de contar con sus propias ventajas y limitaciones.

2 El hecho de que algunos protocolos sólo trabajen en ciertos niveles. Por ejemplo, un protocolo que trabaje a nivel físico asegura que los paquetes de datos pasen a la tarjeta de red NIC (Netwok Interface Card) y salgan al cable de la red.

3 Los protocolos también pueden trabajar juntos en una jerarquía. Al igual que una red incorpora funciones a cada uno de los niveles, distintos protocolos trabajan juntos a distintos niveles en la jerarquía de protocolos. Por ejemplo, el nivel de aplicación del protocolo TCP/IP que corresponde con el nivel de presentación del modelo OSI. Vistos conjuntamente, los protocolos describen la jerarquía de funciones y prestaciones

El proceso técnico en que los datos son transmitidos a través de la red se puede dividir en dos pasos; discretos y sistemáticos. En cada uno se realizan ciertas acciones que no se llevan acabo en el otro, incluyendo sus propias reglas, procedimiento y protocolos.

Estos pasos se llevan a cabo en un orden apropiado y es lo mismo en cada uno de los equipos de la red. En el equipo origen, estos pasos se llevan a cabo de arriba hacia abajo y en el destino, de forma contraria.

A mediados de los 80´s, la mayoría de las redes eran de tipo LAN (Local Área Network), que servían a un solo departamento o compañía y rara vez se conectaba a entornos más grandes, a medida que la tecnología y la comunicación de datos avanzaba; estás redes se hicieron cada vez más grandes que se comunicaban entre si (dándoles por nombre encaminables) ya que los datos son enviados de una a otra, a lo largo de varios caminos disponibles. Surgiendo de esta manera los protocolos encaminables.

Debido a que estos protocolos se pueden utilizar para unir varias LAN y crear entornos de red de área extensa que en la actualidad han tomado gran importancia. Por ejemplo los protocolos IP, IPX; los cuales se verán con mayor detalle más adelante.

En una red, interfieren varios protocolos. Al hacerlo, se asegura que los datos sean preparados correctamente, se transfieran al destino correspondiente y se reciban de forma apropiada. El trabajo de los distintos protocolos debe de estar bien coordinado de modo que no se produzcan conflictos o se realicen tareas incompletas. A los resultados de esta coordinación se les conoce como trabajo en multiniveles.

1.3 PROTOCOLOS

1.3.1. PROTOCOLOS BÁSICOS DE NETWARE

Novell proporciona un conjunto de protocolos desarrollados específicamente para NetWare. Los cinco protocolos principales utilizados por este son:

1 Protocolo de acceso al medio.

2 IPX/SPX (Protocolo de Intercambio de paquetes entre redes /intercambio de paquetes en secuencia).

3 Protocolo de información de encaminamiento (RIP).

4 Protocolo de notificación de servicios (SAP).

5 Protocolo básico de NetWare (NCP).

Debido a que estos protocolos se definieron antes de la finalización del modelo OSI, no se ajustan exactamente a este. Actualmente, no existe una correlación directa entre los límites de los niveles de las dos arquitecturas. Estos protocolos siguen un patrón de recubrimiento. Concretamente, los protocolos de nivel superior (NCP, SAP y RIP) están recubiertos por IPX/SPX. Luego, una cabecera y un final del protocolo de acceso al medio recubre a este, tal y como lo muestra la (figura 1.2).

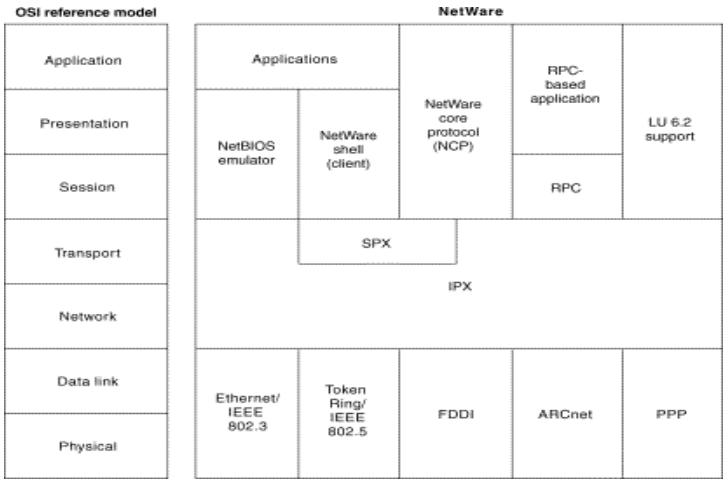

Figura 1.2

1.3.1.1 PROTOCOLO DE ACCESO AL MEDIO

Estos protocolos definen el direccionamiento que permite diferenciar a los nodos de una red NetWare. Dicho direccionamiento está implementado en la NIC, los cuales son los responsables de colocar la cabecera al paquete que incluye el código del origen y del destino. Una vez transmitido el paquete, se verifica que la dirección origen coincida con la dirección destino del paquete, o si el paquete es un mensaje de difusión, la NIC copia el paquete y lo envía a la jerarquía de protocolos.

Además del direccionamiento, proporciona un control de errores a nivel de bit como una comprobación de redundancia cíclica CRC (Cyclic Redundancy Check). La cual utiliza un cálculo complejo para generar un número basado en los datos transmitidos. El dispositivo que realiza el envío hace un cálculo antes de la transmisión y lo incluye en el paquete enviado al destino. A su ves el dispositivo destino vuelve a hacer este cálculo después de la transmisión. Si ambos obtienen el mismo resultado, se excluye error alguno en la transmisión. A este procedimiento se le conoce como ***comprobación de redundancia***, porque cada transmisión incluye no sólo los datos, sino que además incluye valores de comprobación extras (redundantes).

1.3.1.2 IPX/SPX

IPX (Internetwork Packet Exchange) define los esquemas de direccionamiento utilizados en una red e intercambio de paquetes en secuencia y SPX (Sequenced Packet Exchange), proporciona la seguridad y fiabilidad al protocolo IPX. Este protocolo esta basado en datagramas, no orientado a la conexión y no fiable, equivalente a IP y no requiere confirmación por cada paquete enviado.

Cualquier control de confirmación de conexión tiene que ser favorecido por los protocolos superiores a IPX. SPX entrega los servicios orientados a la conexión y fiables a nivel de transporte. En la (figura 1.3), se ve claramente dicha conexión.

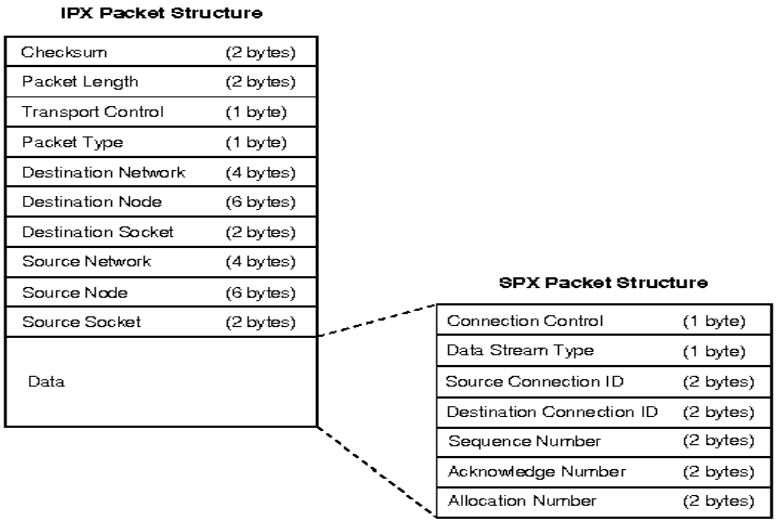

Figura 1.3

IPX define dos tipos de direccionamiento:

1 ***De red:*** La dirección de un segmento de red, identificado por el número de red asignado durante la instalación.

2 ***Direccionamiento de nodo:*** La dirección de un proceso en un nodo que esta identificado por un número de socket.

Dicho protocolos sólo se utilizan en redes con servidores Novell NetWare y suelen instalarse con otro conjunto de protocolos como TCP/IP. Incluso NetWare está empezando a utilizar TCP/IP como un estándar.

1.3.1.3 PROTOCOLO DE INFORMACIÓN DE ENCAMINAMIENTO (RIP)

RIP (Routing Information Protocol), al igual que IPX, facilita el intercambio de información de encaminamiento en una red NetWare y fue desarrollado desde XNS. Sin embargo, en RIP se ha añadido al paquete un campo de dato extra para mejorar el criterio de decisión para seleccionar la ruta más rápida hasta un destino, véase la (figura 1.4).

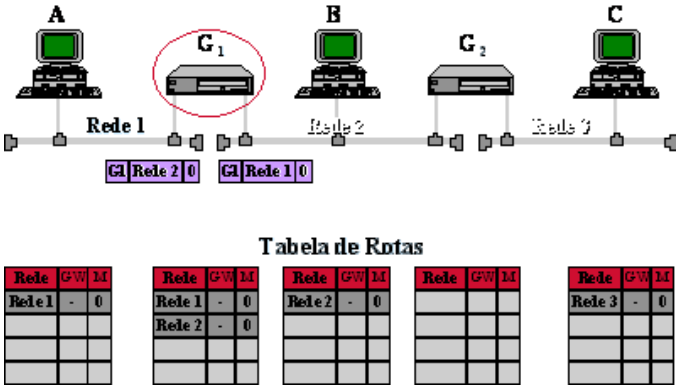

Figura 1.4

El hecho de realizar una difusión de un paquete RIP permite que ocurran ciertas cosas:

1. Las estaciones de trabajo pueden localizar el camino más rápido a un número de red.
2. Solicitar información de encaminamiento a otros routers para actualizar sus propias tablas internas.
3. Responder a peticiones de encaminamiento de otras estaciones de trabajo o de otros routers.

4. Asegurarse de que otros routers conozcan y detecten un cambio en la configuración de la red.

1.3.1.4 PROTOCOLO DE NOTIFICACIÓN DE SERVICIO (SAP)

El Protocolo de notificación de servicios SAP (System, Anwendungen and Produkte) permite a aquellos nodos que proporcionan servicios (incluyen a los servidores de archivos, servidores de impresión) informar de sus servicios y direcciones. Los clientes de la red son capaces de obtener la dirección de la red de los servidores a los que pueden acceder. Con SAP, la incorporación y eliminación de servicios en la red se vuelve dinámica. Por omisión, un servidor SAP informa de su presencia cada 60 segundos. Un paquete SAP contiene:

1 ***Información operativa:*** Indica la operación que está realizando el paquete.

2 ***Tipo de servicio:*** Especifica el tipo de servicio ofrecido por el servidor.

3 ***Nombre del servidor:*** Muestra el nombre del servidor que difunde los servicios.

4 ***Dirección de red:*** Da el número de red del servidor que difunde los servicios.

5 ***Dirección de nodo:*** Muestra el número de nodo del servidor que difunde los servicios.

6 ***Dirección de socket:*** Indica el número de socket del servidor que difunde los servicios.

7 ***Total de saltos hasta el servidor:*** Apunta el número de saltos que hay hasta el servidor que difunde los servicios.

8 ***Campo de operación:*** Especifica el tipo de petición.

9 ***Información adicional:*** Uno o más conjuntos de campos que pueden seguir al campo de operación con más información sobre uno o más servidores.

1.3.1.5 NCP (NETWARE CORE PROTOCOL)

El Protocolo básico de NetWare NCP (Netware Core Protocol) define el control de la conexión y la codificación de la petición de servicio que hace posible que puedan

interactuar los clientes y los servidores. Este protocolo proporciona los servicios de transporte y de sesión. Tal protocolo también proporciona seguridad durante la transmisión de datos tal y como se ve en la (figura 1.5).

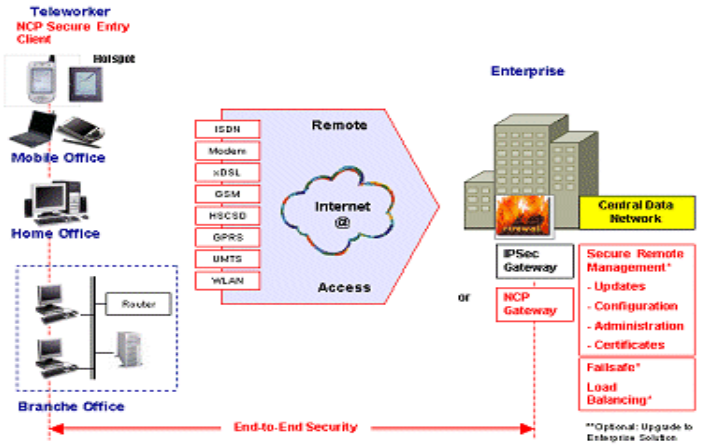

Figura 1.5

Características:

1 Una familia de protocolos de control de red (NCP) establecen y configuran los distintos protocolos de nivel de red.

2 NCP se utiliza para asignar una dirección IP a los equipos de la red.

3 También distribuye la conexión de la capa de red y libera la dirección IP.

4 Elige y configura los paquetes enviados por uno o más protocolos de la red.

5 La configuración de los protocolos de cada capa de red es manejada y separada por los protocolos de control de red (NCP) durante la fase de red.

1.3.2 SISTEMA BÁSICO DE ENTRADA / SALIDA (NetBIOS)

La mayoría de los servicios y aplicaciones que se ejecutan en el sistema operativo Windows utilizan la interfaz NetBIOS . Se desarrolló sobre LAN y se ha convertido en una interfaz estándar para que las aplicaciones puedan acceder a los protocolos de red en el nivel de transporte con comunicaciones orientadas y no orientadas a la conexión. Existen interfaces

NetBIOS para NetBEUI, NWLink y TCP/IP. Las interfaces NetBIOS necesitan una dirección IP y un nombre para identificar de forma única a un equipo, obsérvese la (figura 1.6).

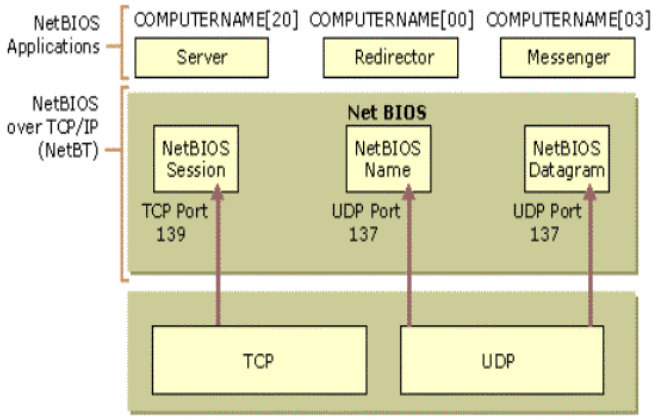

Figura 1.6

Las cuatro funciones más importantes de NetBIOS son:

1 ***La resolución de nombres:*** Cada estación de trabajo tiene uno o más nombres. NetBIOS mantiene una tabla con los nombres y algunos sinónimos. El primer nombre en la tabla es el nombre único de la NIC.

2 ***El servicio de datagramas:*** Esta función permite enviar un mensaje a un nombre, a un grupo de nombres, o a todos los usuarios de la red. Sin embargo, debido a que no utiliza conexiones punto a punto, no se garantiza que el mensaje llegue a su destino.

3 ***Servicio de sesión:*** Este servicio abre una conexión punto a punto entre dos estaciones de trabajo de una red. Una estación inicia una llamada a otra y abre la conexión. Debido a que ambas estaciones son iguales, pueden enviar y recibir datos concurrentemente.

4 ***Estado de la sesión NIC:*** Esta función ofrece información sobre la NIC local, otras NIC y las sesiones activas disponibles a cualquier aplicación que utilice NetBIOS, ver (figura 1.7).

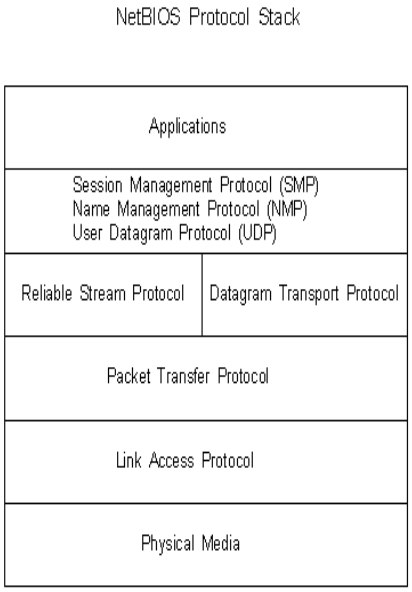

Figura 1.7

NetBIOS proporciona a un programa las herramientas para establecer una sesión de red con otro, y debido a que muchos de éstos lo soportan, es muy popular.

1.3.3 NetBEUI

NetBEUI es el acrónimo de Interfaz de usuario ampliada NetBIOS. Originalmente, estaba casi unido con NetBIOS y se les consideraba como un protocolo.

NetBEUI es un protocolo pequeño, rápido y eficiente a nivel de transporte proporcionado con todos los productos de red de Microsoft. Está disponible desde mediados de los ochenta y se suministró con el primer producto de red de Microsoft: MS-NET.

Entre las ventajas de NetBEUI se incluyen su pequeño tamaño (importante para los equipos que ejecuten MS-DOS), su velocidad de transferencia de datos en el medio y su compatibilidad con todas las redes Microsoft. El principal inconveniente de NetBEUI es que no soporta el encaminamiento. También está limitado a redes Microsoft. NetBEUI es una buena solución económica para una red de trabajo en grupo donde todas las estaciones utilizan sistemas operativos Microsoft. Obsérvese la (figura 1.8).

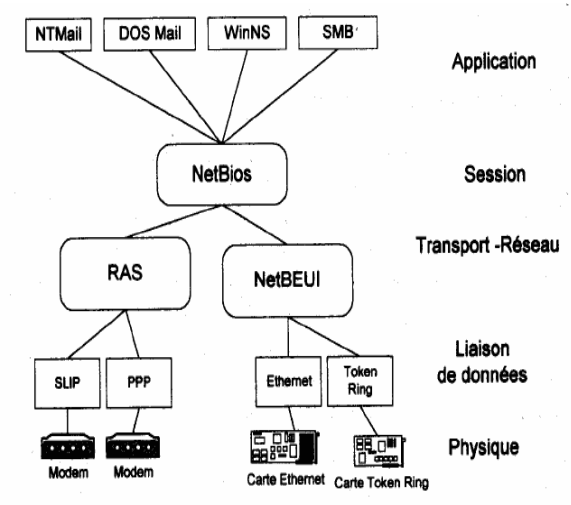

Figura 1.8

1.3.4 COMUNICACIÓN AVANZADA ENTRE PROGRAMAS (APPC)

La comunicación avanzada entre programas, es un protocolo de transporte que IBM desarrollo como parte de su arquitectura de sistemas en red (SNA). Se diseñó para permitir que los programas de aplicación que se estuviesen ejecutando en distintos equipos se puedan comunicar e interconectar datos directamente.

1.3.4.1 APPLE TALK

Apple Talk no es más que una pila de protocolos que están incorporados en las computadoras Mac, y que cumplen con las normas OSI, siendo independientes de los medios físicos con los que puede funcionar.

Apple Talk es la jerarquía de protocolos de computadoras Apple para permitir que los equipos Apple Macintosh compartan archivos e impresoras en un entorno de red (Uyless (1995) Redes de Computadoras Protocolos, Normas e Interfaces (2a. ed.) México: Alfa Omega).

En 1984 se introdujo esta jerarquía como una tecnología LAN auto configurable. Se diseño con una interfase de red transparente, es decir en la interacción entre clientes y servidores se requiere poca interacción por parte del usuario. Existen dos versiones:

1. ***Apple Talk Fase 1:*** Se desarrolló por los 80's estrictamente para el uso de workgroups en áreas locales. Por consiguiente tiene dos limitaciones:

El segmento de red puede contener no más de 32 nodos activos.
Soporta sólo las redes de corta extensión.

2 ***AppleTalk Fase 2***: Se diseñó para el uso en inter-redes más grandes y elimina las limitaciones de AppleTalk Fase 1. La fase 2 permite la combinación de múltiples estaciones en un único segmento de red y soporta ambos tipos: redes de corta extensión y las redes extendidas, observe la (figura 1.9).

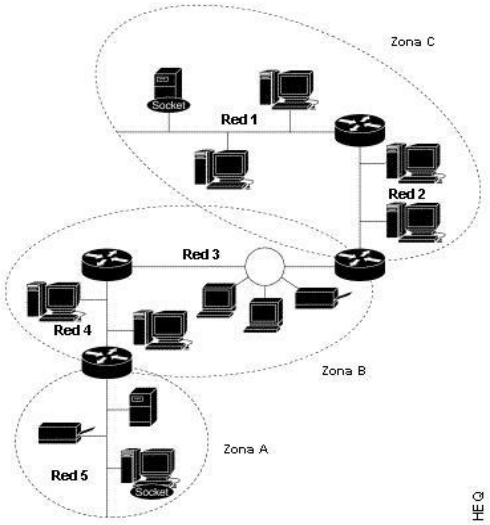

Figura 1.9

Las redes Apple Talk son colocadas jerárquicamente. Son cuatro los componentes que forman la base de una red Apple Talk.

1. ***Sockets:*** Es una única localización direccionable en un nodo que son utilizados para el envío y recepción de datagramas.
2. ***Nodos***: Dispositivo que está conectado a la red, cada uno corresponde a una sola red y a una zona específica.
3. ***Redes:*** *Consiste* en un solo cable lógico y múltiples nodos conectados.
4. ***Zonas***: Es un grupo lógico de nodos o de redes.

1.3.5 DECnet

Es una red distribuida de la DECnet (Digital Equipment Corporation) y consta de seis capas:

1 La capa física.
2 Capa de control de enlace de datos.
3 Capa de transporte.
4 La capa de servicios de la red, corresponde a las cuatro capas inferiores del modelo OSI.
5 La quinta capa la de aplicación, es una mezcla de la capaz de presentación y aplicación del modelo OSI.
6 No cuenta con una capa de sesión separada.

Como se muestra en la (figura 1.10).

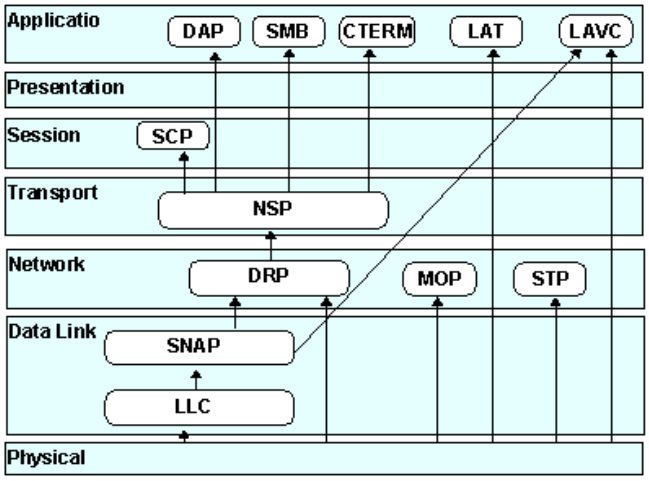

Figura 1.10

DECnet define un marco general tanto para la red de comunicaciones de datos como para el procesamiento distribuido de datos. Su objetivo es permitir la interconexión generalizada de diferentes computadoras y redes punto a punto, multipunto o conmutadas de manera que el usuario comparta programas, archivos de datos y dispositivos de terminal remota; puede soportar la norma del protocolo internacional X.25 y cuenta con capacidades para conmutación de paquetes. Ofrece un emulador mediante el cual se pueden interconectar

microcomputadoras IBM. También se maneja para comunicación digital de datos (PMCDD).

Define redes de comunicación sobre LAN Ethernet, redes de área metropolitana con Interfaz de datos distribuida de fibra (FDDI MAN) y WAN que utilicen características de transmisión de datos privados o públicos. DECnet también puede utilizar protocolos TCP y OSI, así como sus propios protocolos.

1.4 LO MÁS IMPORTANTE

Existen diversos protocolos involucrados en la transmisión y control de datos entre diferentes plataformas como es el caso de Netware y Windows, todos tienen el mismo objetivo: permitir la comunicación entre diferentes equipos.

La funcionalidad y orden apropiado en la ejecución y transmisión de datos tienen un propósito, algunos permiten que interactúen los clientes y los servidores, otros definen el esquema de direccionamiento de datos, tenemos aquellos que incorporan y eliminan servicios en la red como pueden ser servidores de impresión, de archivos, etc. Se tiene en cuenta aquellos que permiten que un programa sea posible ejecutarse en distintas maquinas interconectadas punto a punto o multipunto.

Cada protocolo tiene una función especifica por lo que se determina que uno depende de otro para concluir el objetivo de transmitir información, obtener servicios y aun mas el de ejecutar un programa al mismo tiempo que otro usuario.

A medida que el tiempo ha ido avanzando la necesidad de comunicación entre ususarios es de mayor importancia, por esto los administradores de redes han acordado tener un conjunto de tecnologías y normas comunes para permitir la interconexión entre las aplicaciones de usuarios (no solo la conexión entre redes). De ahí que las actividades como la transferencia e archivos, y el correo electrónico deberían estandarizarse. El protocolo de control de transmisión/protocolo de Internet (TCP/IP) se desarrollo con ese objetivo, Este protocolo esta formado por diferentes elementos, además proporciona procedimientos de comunicación permitiendo el acceso a Internet y sus recursos.

CAPÍTULO II

1. PROTOCOLO TCP/IP

El protocolo TCP/IP nos permite enlazar máquinas que utilizan diferentes sistemas operativos y plataformas, por tal razón de su estudio para conocer los protocolos, arquitectura y funcionalidad que lo hacen ser en la actualidad él más rentable en el área de comunicaciones.

2.1 ORIGEN

Lo que hace interesante a este protocolo es su adopción casi universal, así como el crecimiento de Internet. A mediados de los 70´s ARPA comenzó a trabajar con una tecnología de red de redes y tomo forma entre 1977 y 1979. Por su gran contribución a la investigación al caso y por sus ideas sobre la comunicación de paquetes con su bien conocida ARPANET, obligo a ARPA a estudiar la interconexión de redes y alentó al enlace de estas.

En 1980 se inicio Internet global ARPA, comenzando a convertir máquinas conectadas a sus redes con el protocolo TCP/IP. Así ARPANET se convirtió en la columna vertebral del Internet, y fue utilizada para los primeros experimentos con el TCP/IP, en 1983 se completó Internet, cuando la Oficina del Secretario de Defensa ordenó que todas las máquinas conectadas a redes de largo alcance utilizaran TCP/IP. Se divide ARPANET para investigaciones futuras y la otra militar, conocida como red militar (MILNET). En 1986 se incrementan los esfuerzos para enlazar redes de área amplia, llamada NSFNET, se une a ARPANET y todas las redes con fondos de NSF utilizan protocolos TCP/IP (tabla 2.1).

PERIODO	ALCANCE
1960 a 1970.	El TCP/IP fue originado con los experimentos de intercambio de paquetes dirigido por el U.S. Department of Defense Advanced Research Projects Agency (DARPA).
1970	Las computadoras de la Advanced Research Agency Network (ARPANET) comienzan a utilizar el NCP (Network Control Protocol).
1972	La primera especificación Telnet. “Ad hoc Telnet Protocol” se define como una RFC, la 318.

PERIODO	ALCANCE
1973	RFC 454. Se introduce el FTP (File Transport Protocol)
1974	El TCP (Transmission Control Program) se especifica detalladamente.
1981	El estándar IP se publica en la RFC 791
1982	La 'Defense Communications Agency' (DCA) y ARPA establecen a la 'Transmision Control Protcolo (TCP) y al Internet Protocol (IP) como la colección de protocolos TCP/IP.
1983	ARPANET cambia de NCP a TCP/IP
1984	Se define el concepto de DNS (Domain Name System)
1986	Nace NSFNET para enlazar redes de área amplia.
1989	El físico Tim Berners-Lee CERN (Centro Europeo para la Investigación Nuclear) desarrolla Se desarrolló una superficie tipo hipertexto y un protocolo de comunicación (HTTP: HyperText Transfer Protocol)
1989	World Wibe Web se desarrolló por el informático británico Timothy Berners-Lee para el Consejo Europeo de Investigación Nuclear (CERN, siglas en francés

Tabla 2.1

2.2 ARQUITECTURA

El protocolo TCP (Transmission Control Protocol) /IP (Internet Protocol), es comúnmente utilizado en todas las computadoras conectadas a Internet para lograr la comunicación entre ellas, con una instancia de tiempo diferente, con hardware y software incompatibles, lo cual es una de las grandes ventajas del TCP/IP, dado que permite que la comunicación entre estas variantes sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de hardware. La arquitectura de TCP/IP consta de cuatro niveles o capas (figura 2.2) en las que se agrupan los protocolos. Cada una es responsable de sus diferentes facetas en la comunicación. De esta forma, se define la familia de protocolos TCP/IP como una combinación de cuatro capas.

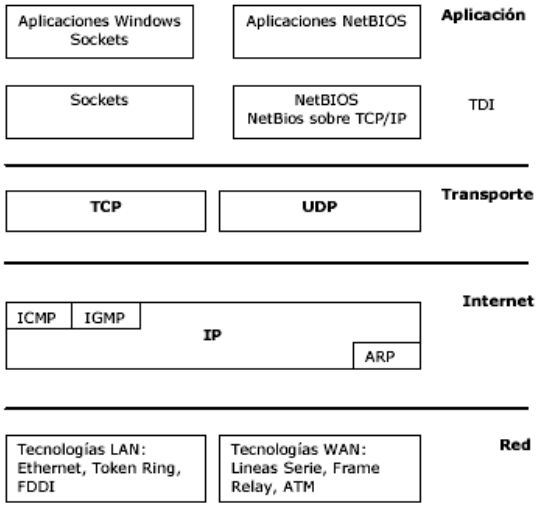

Figura 2.2

En dicho esquema, la capa superior accede únicamente a los servicios prestados por la capa de nivel inferior a ella. Es así como se independiza una capa del resto de las capas inferiores, lo que permite tener un esquema modular.

A continuación se describe cada una de estas capas:

CAPA DE RED

También denominada capa de datos o capa de acceso a red (network interface layer), permite al sistema operativo de enviar, recibir y mover paquetes de información a través de la red o redes a la que se encuentra conectado, así como encaminarlos por las diferentes rutas que deben recorrer para llegar a su destino. En esta capa encontramos los protocolos de más bajo nivel, destacando el IP, el protocolo ICMP y el IGMP, cuya funcionalidad es la de proporcionar apoyo al IP para manejar mensajes especiales de la red, como los de error y transmisión múltiple.

CAPA DE INTERNET

Aquí se encapsulan los paquetes en datagramas Internet y ejecuta todos los algoritmos de enrutamiento (routing) de paquetes. Los 4 protocolos de esta capa son: IP (Internet

Protocol), ARP (Address Resolution Protocol), ICMP (Internet Control Message Protocol) e IGMP (Internet Group Management Protocol).

1. ***IP:*** Es el responsable del envío y enrutamiento de paquetes entre máquinas y redes.
2. ***ARP:*** Obtiene las direcciones de hardware de las máquinas situadas en la misma red física.
3. ***ICMP:*** Manda los mensajes e informa de errores en el envió de paquetes.
4. ***IGMP:*** Se utiliza para la comunicación entre routers.

La dirección obtenida por el ARP, es única. La cual es implementada vía hardware por el fabricante de la tarjeta de red, y lo selecciona de un rango de direcciones único asignado por él, garantizando la unicidad de dicha tarjeta.

1. Se ocupa de la transmisión de los bits sin estructura sobre el medio físico.
2. Describe la interfaz en el ámbito eléctrico, electromagnético o luminoso, tanto en lo mecánico como en lo funcional.
3. Equipo Terminal: adaptador o tarjeta y puerto.
4. Equipo intermedio: Repetidor, amplificador, concentrador de terminales, MODEM, codec, CSU, DSU, transductor.
5. El protocolo IP gestiona el envío de datagramas a través de la red hasta su destino.

Esta capa realiza el análisis de cada datagrama que recibe, si la dirección del receptor coincide con la dirección física del dispositivo, el datagrama puede pasar hacia arriba por las capas, de lo contrario se ignora.

CAPA DE TRANSPORTE

La capa de transporte, proporciona el nivel de "sesión" en la comunicación. Los dos protocolos posibles de transportes son TCP y UDP (User Datagram Protocol). Se puede utilizar uno u otro protocolo dependiendo del método preferido de envío de datos. TCP da

un tipo de conectividad "orientada a conexión". Típicamente se utiliza para transferir largas cantidades de datos de una sola vez, también se utiliza en aplicaciones que requieren un "reconocimiento" o validación de los datos recibidos. El UDP proporciona conexión de comunicación y no garantiza la entrega de paquetes. Las aplicaciones que utilicen UDP normalmente envían pequeñas cantidades de datos de una sola vez. La aplicación que lo utilice, es la responsable en este caso de la integridad de los paquetes y establece sus propios mecanismos para la repetición de mensajes, seguimientos, etc., no existiendo garantía de entrega ni de orden de entrega en la máquina destino.

Las principales tareas de esta capa son:

1. Proporciona la comunicación entre un programa de aplicación y otro (conocida como comunicación punto a punto).
2. Regula el flujo de información.
3. Entrega un transporte confiable, sin errores y en secuencia.
4. Divide el flujo de datos en pequeños paquetes y los pasa con una dirección de destino hacia la siguiente capa de transmisión.

También acepta datos desde varios programas y los envía a la capa siguiente, para lograrlo añade información adicional a cada paquete, incluyendo códigos que identifican el programa de envió e indica también que programa de aplicación debe recibir, así como una suma de verificación. La máquina receptora utiliza esta suma para verificar que el paquete haya llegado intacto y utiliza el código de destino para identificar el programa de aplicación al que se debe entregar.

CAPA DE APLICACIÓN

Esta se encarga de manejar los detalles particulares relativos a las diferentes aplicaciones que utilizará el usuario (WWW, TELNET, FTP). Permitiendo una independencia entre las diferentes capas y obliga a que la comunicación entre las computadoras se realice mediante capas del mismo nivel (figura 2.3).

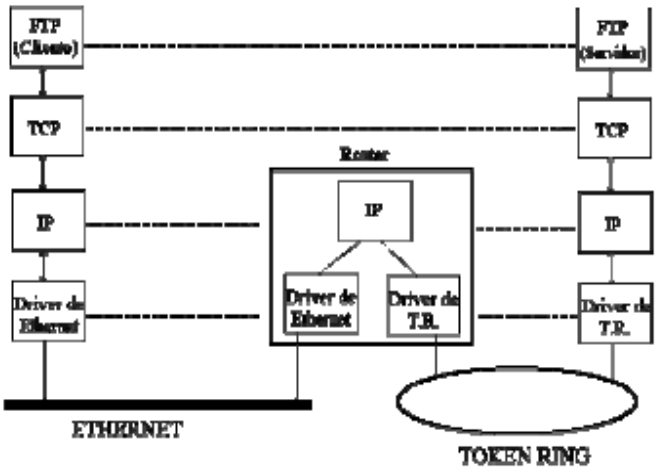

Figura 2.3

La comunicación en Internet se produce mediante el intercambio de paquetes de información (datagramas), estos viajan por las computadoras que están conectadas hasta alcanzar su objetivo o son descartados por algún motivo.

De esta forma, podemos diferenciar dos tipos de funciones por los cuales se transmiten los paquetes de información:

1. Computadora emisor/receptor (end-system o end-host): Aquí se engloba la computadora origen o destinatario de la comunicación.
2. Computadora intermedia (intermediate-system, router o gateway): Son todas las computadoras por las que van pasando los datagramas hasta la computadora destino de la comunicación o hasta el origen.

El protocolo IP dispone de un sistema de numeración que permite diferenciar todas y cada una de las computadoras conectadas. Estas direcciones han de cumplir dos requisitos básicos (figura 2.4).

1. Deben ser únicas: No puede haber dos computadoras con la misma dirección.
2. Las direcciones son números de 32 bits (4 bytes). Estas direcciones se representan mediante cuatro números decimales separados por un punto.

CLASE	RANGO		
A	0.0.0.0	Hasta	127.255.255.255
B	128.0.0.0	Hasta	191.255.255.255
C	192.0.0.0	Hasta	223.255.255.255
D	224.0.0.0	Hasta	239.255.255.255
E	240.0.0.0	Hasta	247.255.255.255

Figura 2.4

Una vez definido el direccionamiento de redes y computadoras en Internet, mencionaremos los servicios de DNS (Domain Name Server). Debido a que es más fácil recordar un nombre que una dirección numérica (158.109.0.4), se crearon los servidores de nombres DNS, que son las máquinas encargadas de transformar un nombre en su dirección correspondiente.

Las direcciones IP están constituidas por 4 números enteros, cada uno de ellos de un byte y separados por un punto (ejemplo: 144.132.3.145) dando un total de 32 bits, al mismo tiempo se dividen 2 partes, una identifica una red y la segunda a un equipo dentro de la red, siendo los bits que se encuentran mas a la izquierda o mas significativos los que indican la clase de red. Los formatos de las direcciones IP soportan cinco clases de red.

- **Las redes de clase A**, proporciona solamente siete bits al campo de dirección para identificar la red física y 24 para identificar la estación de trabajo, lo que permite tener un máximo de 128 redes. Por esto las redes de clase A están destinadas principalmente para su utilización por pocas infraestructuras grandes. Una dirección con el primer bit establecido en cero (0) es una dirección clase A. Las direcciones estarán comprendidas entre 0.0.0.0 y 127.255.255.255, la máscara de subred será 255.0.0.0.

- **Las redes de clase B**, donde los dos bits más altos están definidos por uno, cero (1, 0), están constituidas por 14 bits para el campo de dirección de red y 16 bits para el campo de dirección de host, pero permite tener un máximo de 16.384 redes. Esta clase de direcciones permite tener un buen equilibrio entre espacio de direcciones de

red y estaciones de trabajo. Las direcciones están comprendidas entre 128.0.0.0 y 191.255.255.255, la mascara de subred será 255.255.0.0.

- **Las redes e clase C,** alojan 21 bits para el campo de dirección de red. Sin embargo, sólo proporcionan 8 bits para el campo de dirección de host o estación de trabajo. Esto permite tener un máximo de 2.097.152 redes pero cada una de las cuales puede tener 256 estaciones de trabajo (restando a esta las direcciones reservadas con los últimos valores que sean ceros o unos). Por lo tanto, el número de host por red puede ser un factor de limitación. Las direcciones estarán comprendidas entre 192.0.0.0 y 223.255.255.255, la mascara de subred será 255.255.255.0.

- **Las direcciones de clase D,** están reservadas para grupos de difusión, es usada para implementar una forma de arreglos múltiples en el cual una dirección se refiere a una colección de host en Internet, de las cuales todas reciben el datagrama IP, teniendo direcciones especificas de multidestino. Las direcciones estarán comprendidas entre 224.0.0.0 y 239.255.255.255, además que, los cuatro bits más altos están definidos por 1,1,1 y 0.

- **Las direcciones de clase E,** también son definidas por IP, pero se encuentran reservadas para una utilización futura. En este tipo de clase los cuatro bits superiores están definidos por 1 y el quinto bit es siempre 0.

2.3 CARACTERÍSTICAS

Ya dentro de un sistema TCP/IP los datos transmitidos se dividen en pequeños paquetes, la tarea de IP es llevar los datos a granel (los paquetes) de un sitio a otro, esto es posible gracias a los ruteadores que son utilizados para este fin. Mientras TCP se encarga del flujo y asegura que los datos estén correctos. Las líneas de comunicación son compartidas entre varios usuarios. Cualquier tipo de paquete puede transmitirse al mismo tiempo, se ordenará y combinará cuando llegue a su destino.

Los paquetes no siempre deben enviarse directamente entre dos computadoras, estos paquetes pasan de computadora a computadora hasta llegar a su destino. Claro está, es el secreto de cómo se pueden enviar datos y mensajes entre dos computadoras aunque no estén

conectadas directamente entre sí. Es sorprendente que en cuestión de segundos se puedan enviar archivos de buen tamaño de una máquina a otra, aunque estén separadas por miles de kilómetros y pese a que los datos tienen que pasar por múltiples computadoras. Una de las razones de la rapidez es que, cuando algo anda mal, sólo es necesario volver a transmitir un paquete, no todo el mensaje. Los paquetes no necesitan seguir la misma trayectoria y así llevarlo de un lugar a otro y usar la conexión más idónea que esté disponible en ese instante. No todos los paquetes de los mensajes tienen que viajar, necesariamente, por la misma ruta, ni necesariamente tienen que llegar todos al mismo tiempo.

Su flexibilidad los hace muy confiables ya que al perderse el enlace, el sistema usa otro. Cuando se envía un mensaje, el TCP origen divide los datos en paquetes, los ordena en secuencia, agrega cierta información para control de errores y después los lanza hacia fuera, y los distribuye. Por su parte TCP destino recibe los paquetes, verifica si hay errores y los vuelve a combinar para convertirlos en los datos originales. De existir un error en algún punto, TCP destino envía un mensaje solicitando que se vuelvan a enviar determinados paquetes.

2.4 TIPOS DE PROTOCOLOS TCP/IP

2.4.1 FTP

El protocolo FTP (File Transfer Protocol) permite captar desde su computadora archivos procedentes de cualquier usuario o servidor del mundo. La oferta de los servidores de FTP es muy variada, permitiéndo la transferencia de archivos (documentos, textos, imágenes, sonidos, programas, etc.) entre dos computadoras.

Si bien la transferencia de archivos entre dos computadoras es el mismo proceso en todos los casos, podemos clasificar esta operación en dos tipos, dependiendo de que sea necesario o no, autorización para entrar en la computadora remota.

CARACTERISTICAS DEL FTP

El FTP nos ofrece otras facilidades que van más allá de la función de transferencia.

1. ***Acceso interactivo*:** Diseñado para usarse mediante programas, la mayor parte de las implementaciones proporcionan una interfase interactiva que permite a las personas interactuar con servidores remotos.
2. ***Especificación de formato:*** Permite al cliente especificar el tipo y formato de datos almacenado. Se puede especificar si un archivo contiene enteros de textos y binarios o conjuntos de caracteres ASCII.
3. ***Control de autenticación:*** Se requiere que los clientes se autoricen introduciendo un nombre de conexión y un password de acceso al servidor; de lo contrario se rechaza el acceso al cliente.

MODELO DE PROCESO FTP

La mayor parte de las implementaciones FTP permiten el acceso concurrente de varios clientes y estos se valen del TCP para conectarse al servidor. El servidor espera las conexiones y crea un proceso clave para manejar cada conexión, el esclavo acepta y maneja la conexión de control, utilizando un proceso adicional para manejar una conexión de transferencia de datos separada.

1. La conexión de control transporta comandos que indican al servidor qué archivo transferir.
2. La conexión de transferencia de datos, que también usa TCP como protocolo de transporte, transporta las transferencias de datos.

Las conexiones, procesos y transferencias de datos que los emplean pueden crearse de manera dinámica cuando se necesitan, pero la conexión de control continúa a través de una sesión. Una vez que la conexión de control desaparece la sesión se termina y el software en ambos extremos termina todos los procesos de transferencia de datos.

EL FTP DESDE PUNTO DE VISTA DEL USUARIO

Los usuarios lo ven como un sistema interactivo. El cliente ejecuta repetidamente las siguientes operaciones: leer una línea de entrada, analizar ésta para extraer un comando y sus argumentos, así como ejecutar el comando con los argumentos especificados:

Para iniciar el FTP bajo sistema operativo, se invoca poniendo **c:\> ftp**, una vez hecho esto, procedemos a usar los comandos de este protocolo, si se desconocen, podremos obtener un listado con sólo teclear help en el indicador.

ftp> help

EJEMPLO:

Las características de autorización lo hace más seguro, se prohíbe el acceso a cualquier archivo hasta que no se obtenga una conexión y una clave de acceso para la computadora en la que opera el servidor. Muchas de las localidades del TCP/IP permiten al FTP anónimo, es decir que el cliente no necesita una cuenta o clave de acceso, sino especificar un nombre de conexión anónimo y una clave invitada. Permitiendo su conexión pero restringe su acceso a los archivos públicos disponibles.

Por ejemplo si un usuario desea copiar un archivo basta con solo ejecutar lo siguiente como lo muestra la (figura 2.5).

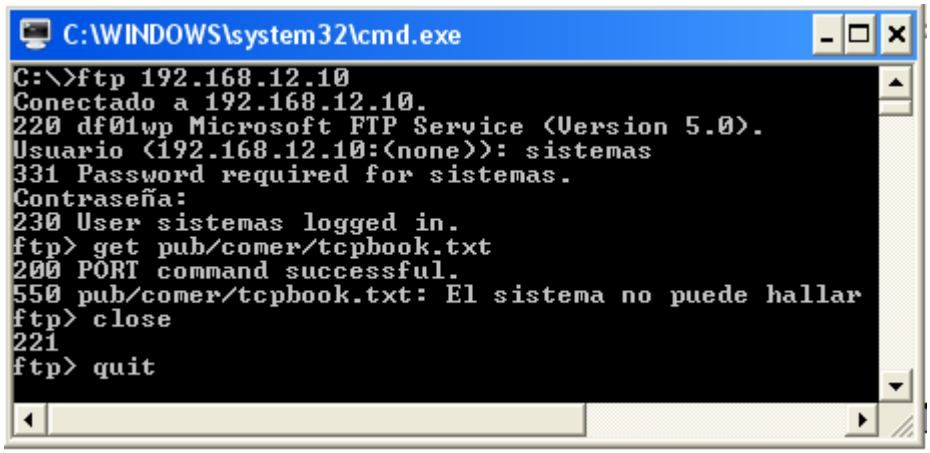

Figura 2.5

2.4.2 SMTP

El protocolo SMTP (Simple Mail Transfer Protocol), o protocolo simple de transferencia de correo electrónico basado en texto utilizado para el intercambio de mensajes entre computadoras y/o distintos dispositivos (PDA´s, Celulares, etc). SMTP esta basado en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores.

HISTORIA

En 1982 se diseña el primer sistema para intercambiar correos electrónicos para ARPANET, definido como RFC 821 (Request for comments) y RFC 822. Donde RFC 821 define el protocolo y la segunda el formato del mensaje. Con el tiempo se ha convertido en uno de los protocolos más usados en Internet. Para adaptarse a las nuevas necesidades surgidas del crecimiento y popularidad se han hecho varias ampliaciones a este protocolo, como poder enviar texto con formato o archivos adjuntos.

Las respuestas que da el servidor pueden ser de varias clases:

- 2XX, para una respuesta afirmativa
- 3XX, para una respuesta temporal afirmativa
- 4XX, para una respuesta de error, pero se espera a que se repita la instrucción
- 5XX, para una respuesta de error.

Una vez que el servidor recibe el mensaje finalizado con un punto puede bien almacenarlo si es para un destinatario que pertenece a su dominio, o bien retransmitirlo a otro servidor para que finalmente llegue a un servidor del dominio del receptor.

FORMATO DEL MENSAJE

El mensaje está compuesto por dos partes:

1. ***Cabecera:*** Las tres primeras líneas son la cabecera. En ellas se usan unas palabras clave para definir los campos del mensaje. Estos campos ayudan a los clientes de correo a organizarlos y mostrarlos. Los más típicos son subject (asunto), from

(emisor) y to (receptor). Estos dos últimos campos no hay que confundirlos con MAIL FROM y RCPT TO, que pertenecen al protocolo.

2. ***Cuerpo del mensaje:*** es el mensaje propiamente dicho. En el SMTP básico está compuesto únicamente por texto, y finalizado con una línea en la que el único carácter es un punto.

A continuación se presenta una (tabla 2.6) de los comandos básicos del protocolo SMTP:

COMANDO	DESCRIPCIÓN
HELO [servidor]	Es el comando para abrir paso al diálogo SMTP.
HELP [comandos]	Pide información sobre los comandos que soporta el servidor, si se especifica un parámetro el servidor nos enviará información referente al comando escrito.
EXPN [lista de correo]	Este comando sirve para pedir listas de correo del servidor
DATA	Este comando especifica al servidor SMTP que a partir de la siguiente línea se empezará a escribir el mensaje (cabecera y contenido). Para indicar que el mensaje se ha completado de escribir se escribirá una línea con solamente un ".", a partir de ahí el servidor enviará el mensaje
MAIL FROM [mail]	Comienza una nueva transacción de envío de mensaje. Especifica la lista de máquinas por las que ha pasado, y el buzón de correo
NOOP	Al ejecutar este comando el servidor debe responder con un OK. Sirve para comprobar que la conexión con el servidor sigue activa o que el servicio que ofrece sigue disponible.
QUIT	Cierra la conexión con el servidor.
AUTH [Método]	Sirve para autentificarse ante el servidor, empleando el método indicado, para cifrar el usuario y la contraseña. (RFC 2554)
RSET	Aborta el envío actual y que reinicia la comunicación desde que se creó la conexión.
SEND FROM	Los códigos de respuesta se enviaran a una Terminal
TURN	El emisor cede el turno al receptor para que actúe como emisor
VRFY [nombre]	Pide Confirmación de que [nombre] es un usuario del MTA receptor

Tabla 2.6

CÓDIGOS DE RESPUESTA

Cada vez que trabajamos con un servidor SMTP, éste devolvera unos números de tres dígitos, llamados "status-code" (tabla 2.7), esto indica el estado del servidor.

CÓDIGO	DESCRIPCIÓN
2??	El comando se envió correctamente.
211	El sistema tiene disponible la ayuda
214	Mensaje de información de ayuda
220	El servicio está disponible
251	El usuario no es local, entonces se remite el mensaje al servidor
3??	Se aceptó el comando pero se espera que el cliente introduzca mas datos
354	Comenzar la introducción del correo, acabando con CR/LF
4??	El comando ha sido rechazado, pero el cliente debería intentarlo de nuevo
421	El servicio de correo no está disponible
452	No se produjo la acción por que el disco no tiene espacio de almacenamiento suficiente
5??	Se rechazó el comando
500	Error en la sintaxis, no se pudo reconocer el comando
501	Error en la sintaxis de los parámetros del comando
502	El comando no esté implementado
504	El parámetro del comando no esté implementado
550	La acción no se realizó porque no se ha encontrado el buzón
551	El usuario no es local, intente enviarlo mediante <servidor>
554	Se produjo un fallo en la transacción

Tabla 2.7

Normatividad de los Códigos de Estado:

1. El primer dígito nos da el nivel de error.
2. El segundo, y tercer dígito nos concreta los detalles.

CONTENIDO DEL MENSAJE (RFC 822)

Está formado por cabeceras, una línea en blanco y el cuerpo. Hay un conjunto de cabeceras predefinidas. Ejemplos:

1. ***From:*** Dice quien escribió el mensaje.
2. ***Sender:*** Quien envió realmente el mensaje.
3. ***Reply - To*:** A quien se debe responder.

La sintaxis es: Nombre valor, este valor debe ocupar varias líneas basta con empezar con un espacio a partir de la segunda y Las definidas por el usuario deben iniciar con x.

2.4.3 TELNET

Este protocolo permite al usuario de una localidad establecer una conexión TCP con un servidor de acceso a otro, transfiere las pulsaciones del teclado directamente desde el teclado del usuario a la computadora remota como si se hubiesen hecho directamente desde la remota. También transporta la salida de la maquina remota de regreso a la pantalla del usuario. Llamado a este servicio transparente, porque da la impresión de que el teclado y el monitor del usuario están conectados de manera directa a la remota. Esta conexión remota se da por medio de un software cliente TELNET en el cual solo basta especificar el nombre de dominio o la dirección IP.

Telnet ofrece tres servicios básicos:

1. El primero define una NVT (Network Virtual Terminal) que proporciona una interfaz estándar para los sistemas remotos. Esto elimina la necesidad para las computadoras "servidor" y "usuario" de guardar información de las características de la otra terminal y de las convenciones para manejarlo. Ambos mapean las características del dispositivo local para que a través de la red parezca un NVT y ambos pueden asumir un mapeado similar en el otro extremo.

2. El segundo incluye un mecanismo que permite al cliente y al servidor negociar opciones, entre esas opciones se podría incluir el cambio del juego de caracteres, el modo de eco, etc.

   La estrategia básica para el uso de opciones es hacer que una parte o ambas inicien la petición de activar alguna opción. El otro lado pueda entonces aceptar o rechazarla. Si es aceptada, tiene efecto inmediato; de lo contrario, el aspecto asociado de la conexión queda tal y como se especifica para un NVT. Una parte siempre puede rehusar activar una opción y nunca debe rehusar desactivar alguna opción ya que ambos lados deben estar preparados para soportar un NVT.

3. Y tercero, trata con una simetría de la sintaxis de negociación puede potencialmente llevar a bucles infinitos de reconocimiento cada parte viendo las órdenes que llegan no como reconocimientos sino como nuevas peticiones para reconocer. Para evitar esto, prevalecen las siguientes normas:

Las partes sólo pueden solicitar un cambio del estado de una opción; una parte no puede enviar una "petición" simplemente para anunciar en qué modo está.
Si una parte recibe lo que parece una petición para entrar en algún modo en el que ya está, la petición no debería reconocerse. No responder esto es esencial para evitar bucles infinitos en la negociación. Es necesario enviar una respuesta para las peticiones de cambio de modo incluso si no se ha cambiado el modo.

Siempre que una parte envíe una orden de opción a la otra, ya que un proceso de servidor maestro espera nuevas conexiones y crea un nuevo esclavo para manejar cada conexión, se utiliza el término pseudos terminal para describir el punto de entrada que permite que un programa, transfiera caracteres al sistema operativo como si viniera del teclado.

Para comprender mejor obsérvese la (figura 2.8).

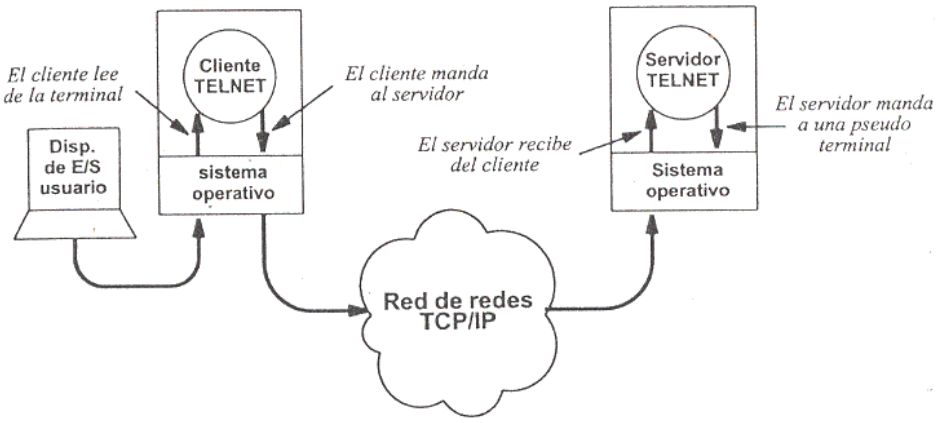

Figura 2.8

Cuando se invoca Telnet, una aplicación de la maquina del usuario se convierte en el cliente. El cliente establece una conexión TCP con el servidor por medio del cual se comunicaran.

Para hacer posible que TELNET interactué con los diferentes sistemas operativos y que permita al usuario interrumpir un proceso u otra acción, es necesario que TELNET se adapte a la heterogeneidad y esto es posible gracias al NVT el cual manda una secuencia de datos y comandos a través de Internet como se muestra en la (figura 2.9).

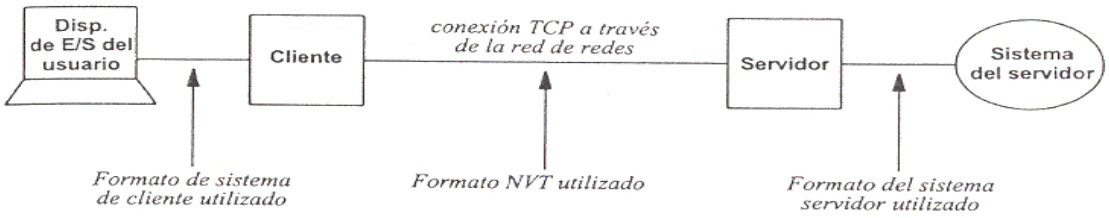

Figura 2.9

Aunque una conexión a través de la red es intrínsecamente bidireccional (full-dúplex), se debe ver al NVT como un dispositivo unidireccional (half-dúplex) operando en modo lineal. A no ser que se negocien opciones indicando lo contrario, se aplican las siguientes condiciones por defecto a la transmisión de datos por la conexión TELNET:

1. Los datos se deben acumular en la computadora donde se generan hasta tener una línea completa de datos o hasta que alguna señal definida localmente indique que debemos transmitir los datos. Esta señal se puede generar por un proceso o por un usuario. Todo ello mientras que el espacio de almacenamiento local lo permita.

2. Cuando un proceso ha terminado de enviar datos y no tiene más datos que procesar, el proceso debe transmitir la orden Go Ahead (Continuar).

ESTRUCTURA DE ORDENES TELNET

Todas las órdenes consisten, en una secuencia de dos bytes: el carácter de escape IAC (Interpretar como Orden) seguido por el código de orden. Las órdenes que negocian estas opciones consisten en secuencias de tres bytes, siendo el tercero el código para la opción referenciada. Se ha elegido este formato para hacer que se use racionalmente el espacio de datos -- mediante negociaciones, a partir del NVT básico, por supuesto -- las colisiones de byts de datos con órdenes se minimicen, requiriendo esas colisiones la inconveniencia e ineficiencia de "escapar" a los byts de datos. Estas son las órdenes TELNET definidas. Téngase en cuenta que estos códigos o secuencias sólo tienen el significado que se indica si van inmediatamente precedidos por un IAC como se muestra en la (tabla 2.10).

NOMBRE	CÓDIGO	SIGNIFICADO
SE	240	Fin de los parámetros de subnegociación.
NOP	241	No-operación.
DMARK	242	La parte del flujo de datos de un Synch. Siempre se debe acompañar de una notificación urgente de TCP.
IP	244	Señal de interrupción de proceso
AO	245	Aborto de Salida
AYT	246	Señal de esta ahí
EC	247	Señal de borrar carácter
EL	248	Señal de borrar línea
SB	250	Indica que lo que sigue es una sub - negociación de la opción indicada.
WILL	251	Autorización de realizar una opción especificada
DO	253	Aprobación para permitir una opción especifica
IAC	255	Se interpreta al siguiente octeto como comando

Tabla 2.10

En TELNET, las opciones son negociables esto permite reconfigurar la conexión para el cliente y el servidor, ofreciendo la transmisión de datos de 8 bits, el rango de opciones es amplio: Algunos extienden las capacidades de manera significativa mientras que otros tratan con detalles menores.

En la (figura 2.11), se listan algunas de las opciones de este protocolo que se implantan con mayor frecuencia.

Nombre	Código	RFC	Significado
Transmisión binaria	0	856	Se cambia la transmisión a modo binario de 8 bits
Eco	1	857	Se permite que uno de los lados haga eco para los datos que recibe
Supresión de GA	3	858	Se suprime (ya no se manda) la señal de continuar después de los datos
Estado	5	859	Petición del estado de la opción TELNET de una localidad remota
Marca de tiempo	6	860	Petición de que se inserte una marca de tiempo en la corriente de retorno para sincronizar dos extremos de una conexión
Tipo de terminal	24	884	Intercambio de información sobre la elaboración y modelo de una terminal que se está usando (permite que los programas se ajusten a la salida como las secuencias de posicionamiento del cursor para la terminal del usuario)
Fin de registro	25	885	Termina los datos mandados con código EOR
Modo de línea	34	1116	Utiliza la edición local y envía líneas completas en lugar de caracteres individuales

Figura 2.11

2.4.4 RPC (Remote Procedure Call)

El protocolo RPC (Remote Procedure Call), permite a un programa ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambas ya que éstas se encuentran encapsuladas dentro del RPC.

RPC es muy utilizada dentro del paradigma cliente-servidor. Siendo el cliente quien inicia el proceso solicitando al servidor que ejecute cierto procedimiento o función y enviando éste de vuelta el resultado de dicha operación al cliente. Hay distintos tipos de RPC, muchos de ellos estandarizados como pueden ser el RPC de Sun (RFC 1057), DCE (Distributed Computing Environment), DCOM de Microsoft. La mayoría utilizan un

lenguaje de descripción de interfaz (IDL) que define los métodos exportados por el servidor, obsérvese la estructura de RPC, (figura 2.12).

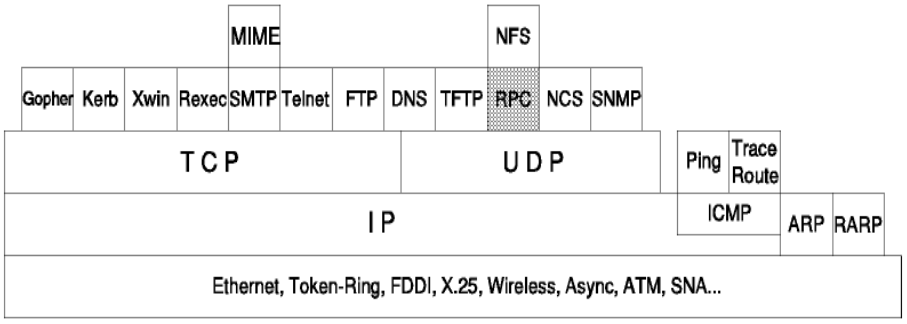

Figura 2.12

El RPC permite que los programas llamen a subrutinas que se ejecutan en un sistema remoto. El cliente envía un mensaje de llamada al proceso servidor y espera un mensaje de respuesta. La llamada incluye los parámetros del procedimiento y la respuesta los resultados.

Podemos conceptualizar y simplificar a RPC de la siguiente manera:

1. El proceso manda un mensaje de llamada y espera por la respuesta.
2. Del lado del servidor un proceso permanece dormido a la espera de mensajes de llamada. Cuando llega una llamada, el proceso servidor extrae los parámetros del procedimiento, calcula los resultados y los devuelve en un mensaje de respuesta.

Este es sólo un posible modelo, ya que el protocolo RPC no impone restricciones específicas en el modelo de concurrencia. En el modelo anterior, el proceso llamador se bloquea hasta que se recibe un mensaje de respuesta y puede continuar su ejecución mientras espera una respuesta, o el servidor puede despachar una tarea separada para cada llamada que reciba de modo que quede libre para recibir otros mensajes.

Las llamadas a procedimientos remotos difieren de las llamadas a procedimientos locales en los siguientes aspectos, como lo muestra la (figura 2.13).

1. Uso de variables globales ya que el servidor no tiene acceso al espacio de memoria del llamador.
2. El rendimiento puede verse afectado por los tiempos de transmisión.
3. Puede ser necesaria la autentificación del usuario.
4. Se debe conocer la dirección del servidor.

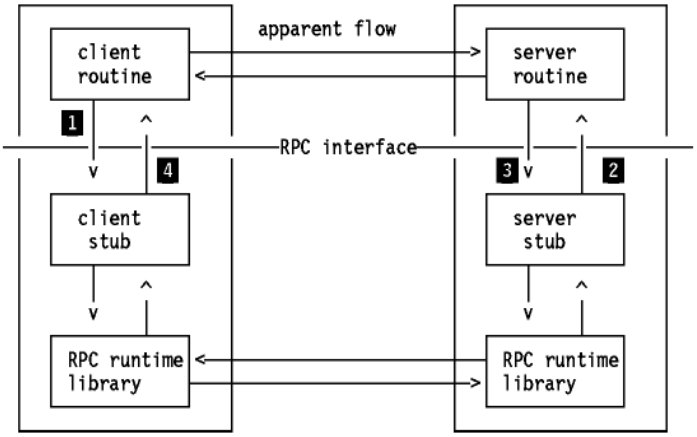

Figura 2.13

Este protocolo se puede implementar sobre cualquier protocolo de transporte. En el caso de TCP/IP, puede usar tanto TCP como UDP como capa de transporte. El tipo de transporte es un parámetro del comando RPCGEN. En caso de que se use UDP, este no proporciona fiabilidad, por lo que dependerá del programa llamador que la garantice. Cabe señalar que incluso con TCP, el programa llamador sigue necesitando una rutina para el tiempo límite con el fin de tratar situaciones excepcionales, como por ejemplo la caída del servidor.

MENSAJE DE LLAMADA DE RPC

El mensaje de llamada de RPC consta de varios campos:

1. ***Números de programa y de procedimiento***.

   Cada llamada contiene tres campos (enteros sin signo):

   - Número del programa remoto.

- Número de versión del programa remoto.
- Número del procedimiento remoto.

Que identifican unívocamente al procedimiento a ejecutar. El número de programa remoto identifica un grupo funcional de procedimientos, por ejemplo, un sistema de archivos, que incluiría procedimientos individuales como "leer" y "escribir". Estos procedimientos individuales se identifican con un número de procedimiento único dentro del programa remoto. A medida que el programa remoto evoluciona, a cada versión se le asigna un número.

Cada programa remoto está conectado a un puerto. El número de este puerto se puede elegir libremente, exceptuando los puertos reservados para "servicios bien conocidos". Es evidente que el llamador tendrá que conocer el número de puerto usado por el programa remoto.

2. ***Campos de autentificación:*** Existen dos campos, credenciales y verificador, para la autentificación del llamador al servicio. Depende del servidor el usar esta información para la autentificación del usuario. Además, cada implementación es libre de elegir entre los varios protocolos de autentificación que están soportados. Algunos de ellos son:

    - Autentificación nula.
    - Autentificación UNIX***:*** Los llamadores de un procedimiento remoto se pueden identificar de igual modo que en el sistema UNIX.
    - Autentificación DES: Además del identificador de usuario, al servidor se le envía un campo correspondiente a un sello de tiempo. Este sello de tiempo es la hora actual, cifrada con una llave conocida sólo para el servidor y el llamador (basado en el concepto de llave secreta y llave pública de DES).

3. ***Parámetros de los procedimientos***.

    Los datos (parámetros) pasados al procedimiento remoto.

PORTMAP (Mapeador de Puertos)

El programa llamador tiene que conocer el número de puerto exacto usado por un programa RCP para ser capaz de enviarle un mensaje. Portmap es una aplicación del servidor el cual mapea el número de programa y la versión del puerto usado por el programa. Debido a que tiene asignado el número de puerto reservado, todo lo que tiene que hacer el llamador es preguntarle al servicio el host remoto por el puerto usado por el programa servidor. Sólo tiene conocimiento de los programas de su host. Cada programa RCP debe registrarse con el Portmap local cuando éste arranca. También debe anular su registro cuando finaliza su ejecución. Normalmente, la aplicación llamadora contacta el Portmap en el host de destino para obtener el número de puerto correcto de un programa remoto determinado, y luego envía el mensaje de llamada a ese puerto. Existe una variante consistente en que el llamador manda también los parámetros del procedimiento al Portmap y este a su vez se encarga de invocarlo (figura 2.14).

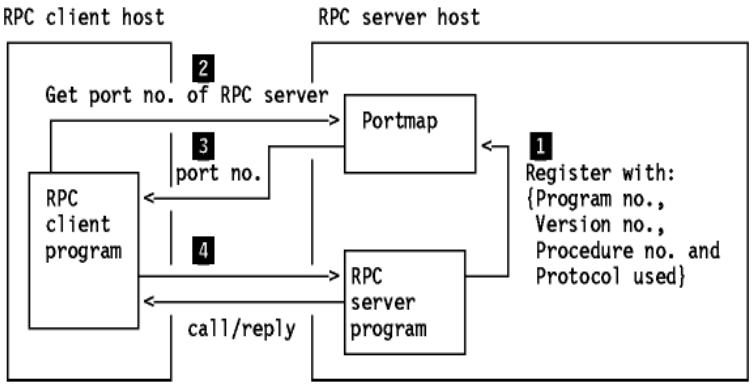

Figura 2.14

RPCGEN

RPCGEN es una herramienta que genera código en C para el protocolo RPC. Su entrada es un fichero escrito en un lenguaje similar a C, conocido como lenguaje RPC. Asumiendo que se usa un fichero de entrada llamado proto.x, RPCGEN produce los siguientes archivos de salida:

1. Un fichero cabecera llamado proto.h que contiene definiciones comunes de constantes y macros.
2. El código fuente del "stub" del cliente, protoc.c
3. El código fuente del "stub" del servidor, protos.c
4. El fichero fuente de rutinas XDR, protox.c

Hoy en día se está utilizando el XML como lenguaje para definir el IDL y el HTTP como protocolo de red. Dando lugar a lo que se conoce como servicios WEB.

2.4.5 SNMP

SNMP (*Simple Network Management Protocol*) es el protocolo definido por los comités técnicos de Internet para ser utilizado como una herramienta de gestión de los distintos dispositivos en cualquier red. Su funcionamiento es sencillo, aunque su implementación es tremendamente compleja. SNMP utiliza la capa de transporte de TCP/IP mediante el envío de datagramas UPD, sin embargo, el hecho de usar UDP hace que el protocolo no sea fiable. SNMP está basado en un conglomerado de agentes. Cada agente es un elemento de la red que ofrece unas determinadas variables al exterior, para ser leídas o modificadas. Asimismo, pueden enviar "alertas" a otros agentes para avisar de eventos que tengan lugar. Generalmente llamado "gestor" al agente encargado de recibir estos eventos.

Cada agente SNMP ofrece información dentro de una MIB (Base de Información de Gestión), la MIB está descrita en ASN.1 para facilitar un transporte transparente por la capa de red. Así, los fabricantes de routers han extendido las MIBs estándar incluyendo información específica de sus equipos.

Con SNMP se puede monitorear el estado de un enlace punto a punto para detectar cuando está congestionado y tomar así medidas oportunas, se puede hacer que una impresora alerte al administrador cuando se ha quedado sin papel, o que un servidor envíe una alerta cuando la carga de su sistema incrementa significativamente. SNMP también permite la modificación remota de la configuración de dispositivos, de forma que se podría modificar las direcciones IP de un ordenador a través de su agente SNMP.

SNMP se sitúa en el tope de la capa de transporte de la pila OSI, o por encima de la capa UDP de la pila de protocolos TCP/IP, como podemos ver en la (figura 2.15).

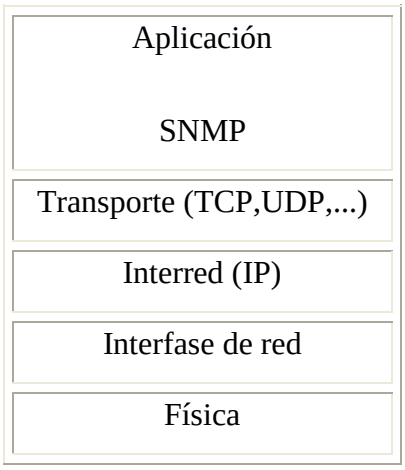

Figura 2.15

NECESIDAD DE ADMINISTRAR REDES

Los problemas que se presentan en la interconexión de redes son principalmente dos:

1. **Dispositivos diferentes:** La interconexión de redes permite diferentes tipos de dispositivos y estos son de distintos vendedores, todos ellos soportando el protocolo TCP/IP. Debido a esto, la administración de redes se presenta como un problema. Sin embargo, usar una tecnología de interconexión abierta permitió que existieran las redes formadas por dispositivos de distintos fabricantes, por lo que para administrar estas redes, habrá que usar una tecnología de administración de redes abierta.
2. **Administraciones diferentes:** Como se permite la interconexión entre redes de distinto propósito y distinto tamaño, hay que tener en cuenta que también están administradas, gestionadas y financiadas de distinta forma.

EVOLUCIÓN HISTÓRICA DEL PROTOCOLO SIMPLE DE GESTIÓN DE RED (SNMP)

El protocolo Snmpv1 fue diseñado a mediados de los 80's por Case, McCloghrie, Rose, and Waldbusser, como una solución a los problemas de comunicación entre diferentes tipos de red. En un principio, su principal meta era el lograr una solución temporal hasta la llegada de protocolos de gestión de red con mejores diseños y más completos. Pero esos administradores de red no llegaron y SNMPv1 se convirtió en la única opción para la gestión de red.

El manejo de este protocolo era simple, se basaba en el intercambio de información de red a través de mensajes (PDU's). Además de ser un protocolo fácilmente extensible a toda la red, debido a esto su uso se estandarizó entre usuarios y empresas que no querían demasiadas complicaciones en la gestión de sus sistemas informáticos dentro de una red. No obstante este protocolo no era perfecto, además no estaba pensado para poder gestionar la inmensa cantidad de redes que cada día iban apareciendo. Para subsanar sus carencias surgió la versión 2 (SNMP v2). Las mayores innovaciones respecto a la primera versión son:

1. Introducción de mecanismos de seguridad, totalmente ausentes en la versión 1. Estos mecanismos protegen la privacidad de los datos, confieren autentificación a los usuarios y controlan el acceso.
2. Mayor detalle en la definición de las variables.
3. Se añaden estructuras de la tabla de datos para facilitar el manejo de los datos. El hecho de poder usar tablas hace aumentar el número de objetos capaces de gestionar, con lo que el aumento de redes dejó de ser un problema.

Realmente esta versión 2 no fue más que un parche, es más hubo innovaciones como los mecanismos de seguridad que se quedaron en pura teoría, no se llegaron a implementar. Por estas razones, este año se ha producido la estandarización de la versión 3. Con dos ventajas principales sobre sus predecesores:

1. Añade algunas características de seguridad como privacidad, autentificación y autorización a la versión 2 del protocolo.

2. Uso de Lenguajes Orientados a Objetos (Java, C++) para la construcción de los elementos propios del protocolo (objetos). Estas técnicas confieren consistencia y llevan implícita la seguridad, por lo que ayudan a los mecanismos de seguridad.

Simple SNMP (Network Management Protocol), o protocolo simple de gestión de redes, es aquel que permite la gestión remota de dispositivos de red, tales como switches, routers y servidores. Su función está basada en los llamados MIBs (Management Information Base), que son bases de datos que definen, almacenan información y parámetros del sistema. SNMP puede hacer consultas e incluso actualizaciones a ésta base de datos, lo que permite la administración y monitoreo remoto de dispositivos de red. Existen programas que periódicamente obtienen datos por SNMP de algún parámetro en especial, esto permite hacer gráficas de uso del sistema.

SNMP es un protocolo de gestión de red, esto es, un conjunto de estructuras y primitivas que permiten tener datos concretos del tráfico que se produce en la red, así como quien lo produce.

2.4.6 NFS

NFS (Netowrk File System), que originalmente fue desarrollado por Sun Microsystem Incorporated, proporciona un acceso de archivos compartidos en línea que es transparente e integrado, muchas de las localidades TCP utilizan NFS para interconectar los archivos de sus computadoras. El NFS es casi invisible, los nombres de los archivos nos muestran si son locales o remotos.

IMPLANTACION NFS

En la (figura 2.16) se muestra cómo NFS está infiltrado en un sistema operativo. Cuando se ejecuta un programa se llama al sistema operativo para que abra un archivo, almacene o recupere datos en archivos. El acceso al archivo acepta la petición y la transmite de manera automática al software del sistema del archivo local o al cliente NFS. Cuando recibe una petición, el software de cliente utiliza el protocolo NFS para ponerse en contacto con el

servidor apropiado de una máquina remota. Al contestar el servidor remoto, el software del cliente devuelve los resultados el programa de aplicación.

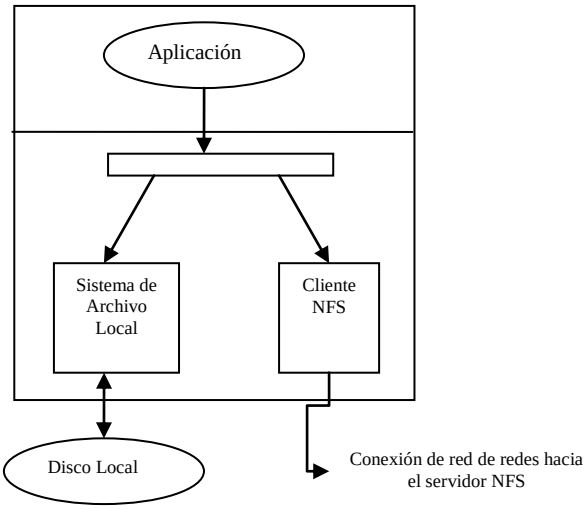

Figura. 2.16

Cuando un programa de aplicación solicita una operación de archivo, el sistema operativo debe transportar la petición al sistema de archivos local o al software de cliente NFS.

LLAMADA DE PROCEDIMIENTO REMOTO

En lugar de definir el protocolo NFS de cero, es en sí un mecanismo general de llamada de procedimiento remoto (remote procedure call o RPC) y una representación de datos externa (external data representación o XDR) de propósito general. Por ejemplo un programador puede dividir un programa de un lado como cliente y del otro como servidor y que utilicen la llamada RPC como mecanismo de comunicación.

El mecanismo RPC oculta todos los detalles de los protocolos, haciendo que los programadores escriban programas distribuidos.

XDR, es una herramienta relacionada, permite a los programadores transmitir datos entre máquinas heterogéneas. Como no todas las computadoras representan enteros binarios de

32 bits en el mismo formato, XDR resuelve el problema definiendo una representación independiente de la máquina. En un extremo del canal de comunicación, un programa invoca procedimientos XDR para hacer la conversión de la representación de hardware local.

La ventaja principal de XDR es que automatiza buena parte de la tarea de conversión de datos, proporcionando un compilador XDR con los enunciados de declaraciones del programa para el que deben transformar los datos.

2.4.7 X-WINDOW

El sistema X-Window (Window, sin la 's' final) fue desarrollado a mediados de los años 80´s en el MIT para dotar de una interfaz gráfica a los sistemas UNIX. Este protocolo permite la interacción gráfica en red entre un usuario y una o más computadoras haciendo transparente la red para éste. Generalmente se refiere a la versión 11 de este protocolo, X11, el que está en uso. X-Window está construido con una arquitectura cliente-servidor.

El servidor de X-Window, ejecutado sobre la máquina servidora, se encarga de generar las instrucciones gráficas. El cliente de X-Window, ejecutado sobre las máquinas conectadas a la máquina servidor, es el encargado de convertir las instrucciones gráficas que recibe del servidor en las instrucciones que precisa el sistema operativo para mostrar las ventanas y su contenido. Gracias a esta arquitectura se consigue aislar el servidor X-Window de los diferentes sistemas operativos que se conecten como clientes. Los clientes X-Window si son dependientes del sistema operativo.

X-Window se encarga de visualizar la información gráfica y es totalmente independiente del sistema operativo. El sistema X-Window distribuye el procesamiento de aplicaciones especificando enlaces cliente-servidor. El servidor provee servicios para acceder a la pantalla, teclado y mouse, mientras que los clientes son las aplicaciones que utilizan estos recursos para interacción con el usuario. De este modo mientras el servidor se ejecuta de manera local, las aplicaciones pueden ejecutarse remotamente desde otras máquinas, proporcionando así el concepto de transparencia de red.

Dado que X-Window es un protocolo que permite ejecutar programas propios del entorno de ventanas en cualquier computadora de la red, y presentar su salida en cualquier otra computadora, si la computadora tiene un servidor X-Window (lo cual sucede en la mayoría de las máquinas UNIX, y también en los X-Terminal y en las computadoras con Windows que ejecuten un determinado programa), al conectarse uno con otra computadora, se puede hacer que se presente información en la computadora en el que uno esta trabajando. Para ello, hay que hacer dos cosas:

1. En la computadora local, se autoriza a la máquina remota a que presente cosas en nuestra terminal, que lea el teclado y el ratón en ciertos momentos. Eso se hace con la orden xhost:
2. En el otro ordenador, indicarle en que computadora de la red tiene que enviar las órdenes de presentación de la información. Puede ser cualquier Terminal de la red.
3. En cualquier caso, lo que se está haciendo es indicarle mediante una variable de entorno al sistema remoto la computadora y pantalla en la cual tiene que presentar la información.

2.5 FUNCIONAMIENTO DEL PROTOCOLO TCP/IP

IP

IP no esta orientado a conexión a diferencia del protocolo X.25, está basado en la idea de datagramas (figura 2.17), los cuales son transportados transparentemente, pero no siempre con seguridad, desde el host fuente hasta el host destino, recorriendo varias redes mientras viaja.

El protocolo IP trabaja de la siguiente manera; la capa de transporte toma los mensajes y los divide en datagramas (Drew Heywood (2001) Redes con Microsoft TCP/IP (3ra. ed.) Pearson Education). Este se transmite a través de la red, posiblemente fragmentándose en unidades más pequeñas, durante su recorrido normal. Al final, cuando todas las piezas llegan a la máquina destinataria, la capa de transporte los reensambla para así reconstruir el mensaje

original. Un datagrama IP consta de una parte de cabecera y una parte de texto. La cabecera tiene una parte fija de 20 octetos y una parte opcional de longitud variable. El campo Versión indica a qué versión del protocolo pertenece cada uno de los datagramas. Mediante la inclusión de la versión en cada datagrama, no se excluye la posibilidad de modificar los protocolos mientras la red se encuentre en operación.

El campo opciones se utiliza para fines de seguridad, encaminamiento fuente, informe de errores, depuración, sellado de tiempo, así como otro tipo de información. Esto, básicamente, proporciona un escape para permitir que las versiones subsiguientes de los protocolos incluyan información que actualmente no está presente en el diseño original. También, para permitir que los experimentadores trabajen con nuevas ideas y para evitar la asignación de bits de cabecera a información que muy rara vez se necesita.

Debido a que la longitud de la cabecera no es constante, un campo de la cabecera, IHL, permite que se indique la longitud que tiene la cabecera en palabras de 32 bits. El valor mínimo es de 5. Tamaño 4 bit.

El campo tipo de servicio le permite al hostal indicarle a la subred el tipo de servicio que desea. Es posible tener varias combinaciones con respecto a la seguridad y la velocidad.

Para voz digitalizada, por ejemplo, es más importante la entrega rápida que corregir errores de transmisión. En tanto que, para la transferencia de archivos, resulta más importante tener la transmisión fiable de entrega rápida. También, es posible tener algunas otras combinaciones, desde un tráfico rutinario, hasta una anulación instantánea. Tamaño 8 bits.

La longitud total incluye todo lo que se encuentra en el datagrama, tanto la cabecera como los datos. La máxima longitud es de 65 536 octetos (bytes). El campo Identificación se necesita para permitir que el hostal destinatario determine a qué datagrama pertenece el fragmento recién llegado. Todos los fragmentos de éste contienen el mismo valor de identificación. Tamaño 16 bits.

Enseguida viene un bit que no se utiliza, y después dos campos de 1 bit. Las letras DF quieren decir no fragmentar. Esta es una orden para que las pasarelas no fragmenten el datagrama, porque el extremo destinatario es incapaz de poner las partes juntas nuevamente.

Por ejemplo, supóngase que se tiene un datagrama que se carga en un micro pequeño para su ejecución; podría marcarse con DF porque la ROM de micro espera el programa completo en un datagrama. Si el datagrama no puede pasarse a través de una red, se deberá encaminar sobre otra red, o bien, desecharse.

Las letras MF significan más fragmentos. Todos los fragmentos, con excepción del último, deberán tener ese bit puesto. Se utiliza como una verificación doble contra el campo de Longitud total, con objeto de tener seguridad de que no faltan fragmentos y que el datagrama entero se reensamble por completo.

El desplazamiento de fragmento indica el lugar del datagrama actual al cual pertenece este fragmento. En un datagrama, todos los fragmentos, con excepción del último, deberán ser un múltiplo de 8 octetos, que es la unidad elemental de fragmentación. Dado que se proporcionan 13 bits, hay un máximo de 8192 fragmentos por datagrama, dando así una longitud máxima de datagrama de 65 536 octetos, que coinciden con el campo Longitud total. Tamaño 16 bits.

El campo Tiempo de vida es un contador que se utiliza para limitar el tiempo de vida de los paquetes. Cuando se llega a cero, el paquete se destruye. La unidad de tiempo es el segundo, permitiéndose un tiempo de vida máximo de 255 segundos. Tamaño 8 bits. Cuando la capa de red ha terminado de ensamblar un datagrama completo, necesitará saber qué hacer con él. El campo Protocolo indica, a qué proceso de transporte pertenece el datagrama. El TCP es efectivamente una posibilidad, pero en realidad hay muchas más.

El número utilizado en este campo sirve para indicar a qué protocolo pertenece el datagrama que se encuentra a continuación de la cabecera IP, de manera que pueda ser tratado correctamente cuando llegue a su destino. Tamaño 8 bits.

El código de redundancia de la cabecera es necesario para verificar que los datos contenidos en la cabecera IP son correctos. Por razones de eficiencia este campo no puede utilizarse para comprobar los datos incluidos a continuación, sino que estos datos de usuario se comprobarán posteriormente a partir del código de redundancia de la cabecera siguiente, y que corresponde al nivel de transporte. Este campo debe calcularse de nuevo cuando cambia alguna opción de la cabecera, como puede ser el tiempo de vida. Tamaño: 16 bits.

La dirección de origen contiene la dirección del host que envía el paquete. Tamaño: 32 bits.

La dirección de destino: Esta dirección es la del host que recibirá la información. Los routers o gateways intermedios deben conocerla para dirigir correctamente el paquete. Tamaño: 32 bits.

Figura 2.17

TCP

Una entidad de transporte TCP (figura 2.18), acepta mensajes de longitud arbitrariamente grandes procedentes de los procesos de usuario, los separa en pedazos y transmite cada pedazo como si fuera un datagrama separado. La capa de red, no garantiza que los datagramas se entreguen apropiadamente, por lo que TCP deberá utilizar temporizadores y retransmitirlos si es necesario. Los datagramas que consiguen llegar, pueden hacerlo en desorden; y dependerá de TCP el hecho de reensamblarlos en mensajes, con la secuencia correcta.

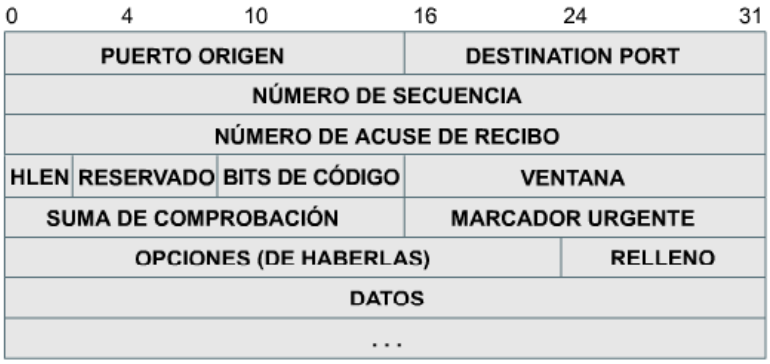

Figura 2.18

Cada octeto de datos transmitido por TCP tiene su propio número de secuencia privado. El espacio de números de secuencia tiene una extensión de 32 bits, para asegurar que los duplicados antiguos hayan desaparecido, en el momento en que los números de secuencia den la vuelta, sin embargo TCP, sí se ocupa en forma explícita del problema de los duplicados retardados cuando intenta establecer una conexión, utilizando el protocolo de ida-vuelta-ida para este propósito.

La primera cosa que llama la atención es que la cabecera mínima de TCP sea de 20 octetos. Enseguida se analizará minuciosamente campo por campo, los campos puerto fuente y puerto destino identifican los puntos terminales de la conexión, cada host deberá decidir por sí mismo cómo asignar sus puertos.

Los campos número de secuencia y asentimiento en superposición efectúan sus funciones usuales. Estos tienen una longitud de 32 bits, debido a que cada octeto de datos está numerado en TCP.

La longitud de la cabecera TCP indica el número de palabra de 32 bits que están contenidas en la cabecera de TCP (Drew Heywood (2001) Redes con Microsoft TCP/IP (3ra. ed.) Pearson Education). Esta información es necesaria porque el campo opciones tiene una longitud variable, y por lo tanto la cabecera también. Después aparecen seis banderas de 1 bit. Si el puntero acelerado se está utilizando, entonces URG se coloca a 1. El puntero acelerado se emplea para indicar un desplazamiento en octetos a partir del número de secuencia actual en

el que se encuentran datos acelerados. Esta facilidad se brinda en lugar de los mensajes de interrupción.

ESTABLECIMIENTO DE CONEXIÓN

El bit SYN se utiliza para el establecimiento de conexiones. La solicitud de conexión tiene SYN=1 y ACK=0, para indicar que el campo de asentimiento en superposición no se está utilizando. La respuesta a la solicitud de conexión si lleva un asentimiento, por lo que tiene SYN=1 y ACK=1. En esencia, el bit SYN se utiliza para denotar las TPDU CONNECTION REQUEST Y CONNECTION CONFIRM, con el bit ACK utilizado para distinguir entre estas dos posibilidades. Véase (figura 2.19).

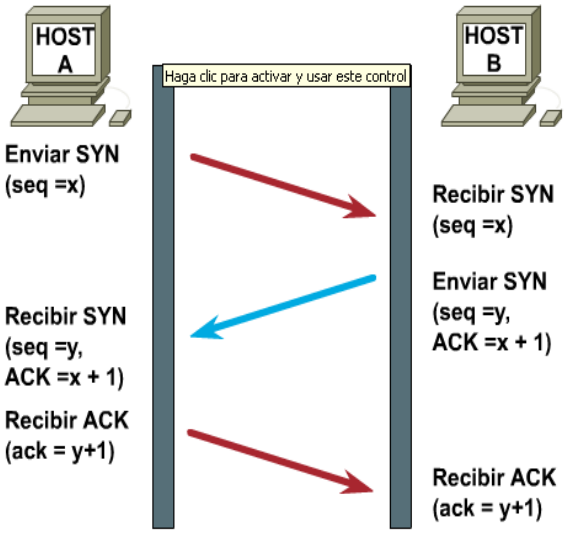

Figura 2.19

El bit FIN se utiliza para liberar la conexión; especifica que el emisor ya no tiene más datos. Después de cerrar una conexión, un proceso puede seguir recibiendo datos indefinidamente. El bit RST se utiliza para reiniciar una conexión que se ha vuelto confusa debido a SYN

duplicados y retardados, o a caída de los hostales. El bit EOM indica el Fin del Mensaje. Obsérvese (figura 2.20).

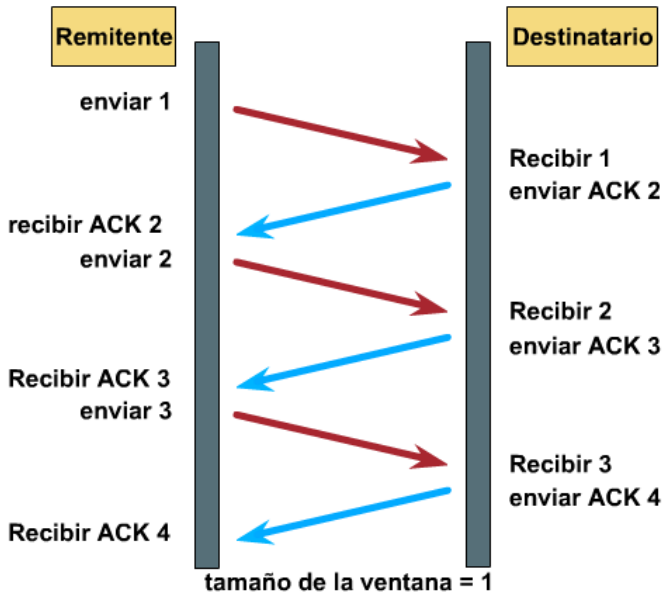

Figura 2.20

El control de flujo en TCP se trata mediante el uso de una ventana deslizante de tamaño variable. Es necesario tener un campo de 16 bits, porque la ventana indica el número de octetos que se pueden transmitir más allá del octeto asentido por el campo ventana y no cuántas TPDU.

El código de redundancia también se brinda como un factor de seguridad extrema. El algoritmo de código de redundancia consiste en sumar simplemente todos los datos, considerados como palabras de 16 bits, y después tomar el complemento a 1 de la suma. El campo de Opciones se utiliza para diferentes cosas, por ejemplo para comunicar tamaño de tampones durante el procedimiento de establecimiento.

2.6 SIMILITUDES Y DIFERENCIAS DEL MODELO OSI Y TCP/IP

Antes de introducirnos a este punto, es de gran importancia detenernos y retomar brevemente el estudio del modelo OSI, para así contar con un marco de referencia para comprender las similitudes y diferencias con el modelo TCP/IP.

MODELO OSI

Al ir incrementando la cantidad y tamaño de las redes que a su vez utilizaban implementaciones de hardware y software diferentes, por lo que eran incompatibles y se volvió muy difícil para las redes que utilizaban especificaciones distintas poder comunicarse entre sí. La ISO (Organización Internacional para la Normalización) realizó varias investigaciones acerca de los esquemas de red y reconoció que era necesario crear un modelo de red que pudiera ayudar a los diseñadores de red a implementar redes que pudieran comunicarse y trabajar en conjunto (interoperabilidad) y por lo tanto, elaboraron el modelo de referencia OSI en 1984.

En el modelo de referencia OSI, hay siete capas numeradas y presentan las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas, de manera que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje.

Las siete capas del modelo de referencia OSI se muestran en la (figura 2.21):

Figura 2.21

Cada capa individual del modelo OSI tiene un conjunto de funciones que debe realizar para que los paquetes de datos puedan viajar en la red desde el origen hasta el destino. A continuación, se presenta una breve descripción de cada capa del modelo de referencia OSI.

Capa 7: La capa de aplicación es la más cercana al usuario; suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa OSI, sino solamente a aplicaciones que se encuentran fuera del modelo OSI. También establece la disponibilidad de los potenciales socios de comunicación, sincroniza y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

Capa 6: La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común.

Capa 5: La capa de sesión establece, administra y finaliza las sesiones entre dos hosts que se están comunicando. Proporciona sus servicios a la capa de presentación, sincroniza el diálogo entre las capas de presentación de los dos hosts y administra su intercambio de datos. Además de regular la sesión, la capa de sesión ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.

Capa 4: La capa de transporte se preocupa de la transmisión origen-destino uniendo procesos de un host a otro host e integra el control de flujo y control de errores, de forma que los datos lleguen correctamente de un extremo a otro.
Específicamente, la confiabilidad del transporte entre dos hosts es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales. Al proporcionar un servicio confiable.

Capa 3: La capa de red encamina los paquetes entre el erigen y destino, los mensajes se fragmentan en paquetes y son enviados de forma independiente. Su misión es unificar redes heterogenias: todos los host tienen un identificador similar a este nivel (direcciones IP).

Capa 2: La capa de enlace de datos proporciona un tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico (comparado con el lógico) , la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo.

Capa 1: La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares se definen a través de las especificaciones de la capa física.

Las diferentes capas del modelo OSI poseen diferentes agrupaciones para los datos. Cada capa tiene un PDU (unidad de datos de protocolo). Las PDU de las capas inferiores se utilizan comúnmente y se deben memorizar: la capa de transporte usa segmentos; los segmentos se encapsulan en paquetes; los paquetes se fraccionan y encapsulan en tramas; y las tramas se transforman en una corriente de bits en los medios físicos véase (figura 2.22).

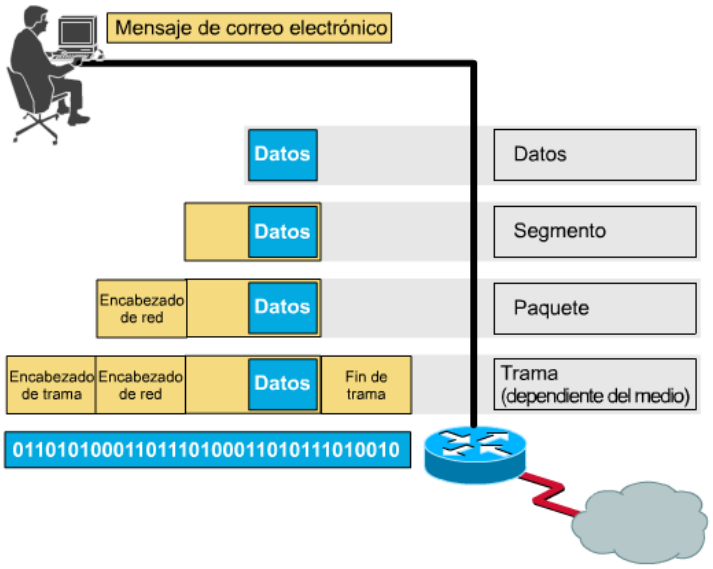

Figura 2.22

Para que los paquetes de datos puedan viajar desde el origen hasta su destino, cada capa del modelo OSI en el origen debe comunicarse con su capa igual en el destino. Esta forma de comunicación se conoce como comunicaciones de par-a-par. Durante este proceso, cada protocolo de capa intercambia información, conocida como PDU, entre capas iguales.

Los paquetes de datos de una red parten de un origen a un destino. Cada capa depende de la función de servicio de la capa OSI que se encuentra debajo de ella. Para brindar este servicio, la capa inferior utiliza el encapsulamiento para colocar la PDU de la capa superior en su campo de datos, luego agrega cualquier encabezado e información final que la capa necesite para ejecutar su función. A medida que los datos se desplazan hacia abajo a través de las capas del modelo OSI, se agregan encabezados e información final adicional. Después de que las Capas 7, 6 y 5 han agregado la información, la Capa 4 agrega más información. Este agrupamiento de datos, la PDU de la Capa 4, se denomina segmento, ver (figura 2.23).

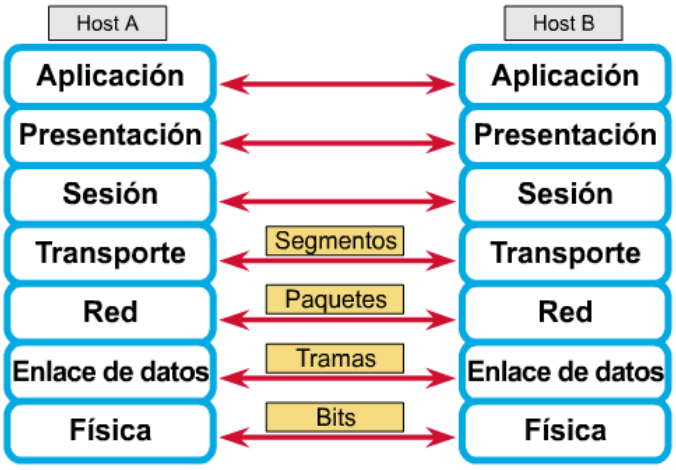

Figura 2.23

Este encabezado contiene la información necesaria para completar la transferencia, la capa de enlace de datos suministra un servicio a la capa de red. Encapsula la información de la capa de red en una trama (la PDU de la Capa 2), el encabezado de la trama contiene información (por ej., direcciones físicas) que es necesaria para completar las funciones de enlace de datos. La capa de enlace de datos suministra un servicio a la capa de red encapsulando la información de la capa de red en una trama.
La capa física codifica los datos de la trama de enlace de datos en un patrón de unos y ceros (bits) para su transmisión a través del medio (generalmente un cable) en la Capa 1.

El modelo OSI, patrocinado por la Comunidad Europea y, más tarde, por el gobierno de los Estados Unidos, no llegó a tener la implantación esperada. Entre otros motivos, porque el modelo TCP/IP ya había sido aceptado entre investigadores por las bases que sustentan Internet y el modelo OSI, fue tan ambicioso y complejo que termino arrinconado.

Sin embargo, la idea de la división por capas del modelo OSI es realmente valiosa. Esta misma idea se aplica a todas las redes actuales, incluyendo Internet.

Una vez ya visto el modelo OSI, ahora si podemos analizar las numerosas similitudes y diferencias con TCP/IP.

Los puntos similares son:

1. Los dos protocolos están diseñados para proporcionar un servicio de transporte seguro, orientado a conexión y de extremo a extremo, sobre una red insegura, que puede perder, dañar, almacenar y duplicar paquetes.
2. Los dos deben enfrentarse a los peores problemas como sería el caso de una subred que pudiera almacenar una secuencia válida de paquetes y más tarde volviera a entregarlos.
3. También son semejantes por el hecho de que los dos tienen una fase de establecimiento de conexión, una fase de transferencia de datos y después una fase de liberación de la conexión. Los conceptos generales del establecimiento, uso y liberación de conexiones también son similares.
4. Utilizan la comunicación ida-vuelta-ida para eliminar las dificultades potenciales ocasionadas por paquetes antiguos que aparecieran súbitamente y pudiesen causar problemas.

Sin embargo también presentan diferencias muy notables, las cuales observamos en la (tabla 2.24).

Las siguientes diferencias se relacionan con la fase de establecimiento de conexión:

Primera Diferencia: OSI utiliza nueve tipos diferentes de TPDU, en tanto que TCP sólo tiene uno. Esta diferencia trae como resultado que TCP sea más sencillo, pero al mismo tiempo también necesita una cabecera más grande, porque todos los campos deben estar presentes en todas las TPDU. El tamaño mínimo en la cabecera de TCP es de 20 octetos y en el modelo OSI es de 5 octetos. Los dos protocolos permiten campos opcionales, que pueden incrementar el tamaño de las cabeceras por encima del permitido.

CARACTERÍSTICA	OSI TP4	TCP
Numero de tipos de TPDU	9	1
Fallo de Conexión	2 conexiones	1 conexión
Formato de direcciones	No está definido	32 bits
Calidad de servicio	Extremo abierto	Opciones específicas
Datos del usuario en CR	Permitido	No permitido
Flujo	Mensajes	Octetos
Datos importantes	Acelerados	Acelerados
Superposición	No	Sí
Control de flujo explícito	Algunas veces	Siempre
Número de subsecuencia	Permitidos	No Permitido
Liberación	Abrupta	Ordenada

Tabla 2.24

***Segunda diferencia*:** Esta diferencia es con respecto a lo que sucede cuando los dos procesos, en forma simultánea, intentan establecer conexiones entre los mismos dos TSAP (es decir, una colisión de conexiones). En el modelo OSI se establecen dos conexiones duplex independientes; en tanto que con TCP, una conexión se identifica mediante un par de TSAP, por lo que solamente se establece una conexión.

Tercera diferencia: Con referencia al formato de direcciones que se utiliza. OSI no especifica el formato exacto de una dirección TSAP, mientras que TCP emplea números de 32 bits.

Cuarta diferencia: En el modelo OSI se tiene un mecanismo de extremo abierto, bastante elaborado, para una negociación a tres bandas sobre la calidad de servicio. Esta negociación incluye al proceso que hace la llamada, al proceso que es llamado y al mismo servicio de transporte. Se pueden especificar muchos parámetros, y pueden proporcionarse los valores deseados y mínimos aceptables. Mientras que TCP no tiene ningún campo de calidad de servicio, sino que el servicio subyacente IP tiene un campo de 8 bits, el cual permite que se haga una relación a partir de un número limitado de combinaciones de velocidad y seguridad.

Quinta diferencia: OSI permite que los datos del usuario sean transportados en la TPDU CR, pero TCP no permite que los datos del usuario aparezcan en la TPDU inicial. El dato inicial (como por ejemplo, una contraseña), podría ser necesario para decidir si se debe o no establecer una conexión. Con TCP no es posible hacer que el establecimiento dependa de los datos del usuario.

Las siguientes diferencias se relacionan con la fase de transferencia de datos:

La Primer diferencia básica es el modelo del transporte de datos:

- El modelo OSI es el de una serie de mensajes ordenados.
- El modelo TCP es el de un flujo continuo de octetos, sin que haya ningún límite explícito entre mensajes.

La segunda diferencia se ocupa de cómo son tratados los datos importantes que necesitan de un procesamiento especial:

- OSI tiene dos flujos de mensajes independientes, los datos normales y los acelerados multiplexados de manera conjunta. En cualquier instante únicamente un mensaje acelerado puede estar activo.
- TCP utiliza el campo Acelerado para indicar que cierta cantidad de octetos, dentro de la TPDU actualmente en uso, es especial y debería procesarse fuera de orden.

Como tercer diferencia se tiene la ausencia del concepto de superposición:

- En OSI y su presencia en TCP. Esta diferencia no es tan significativa como al principio podría parecer, dado que es posible que una entidad de transporte ponga dos TPDU, por ejemplo, DT y AK en un único paquete de red.

En cuarta diferencia contamos con la relaciona con la forma como se trata el control de flujo:

- OSI puede utilizar un esquema de crédito, pero también se puede basar en el esquema de ventana de la capa de red para regular el flujo.
- TCP siempre utiliza un mecanismo de control de flujo explícito con el tamaño de la ventana especificado en cada TPDU.

Y como quinta diferencia se relaciona con este esquema de ventana en ambos protocolos el receptor tiene la capacidad de reducir la ventana en forma voluntaria. Esta posibilidad genera potencialmente problemas, si el otorgamiento de una ventana grande y su contracción subsiguiente llegan en un orden incorrecto.

- En TCP no hay ninguna solución para este problema.
- En tanto OSI, lo resuelve por medio del número de subsecuencia que está incluido en la contracción, permitiendo de esta manera que el emisor determine si la ventana pequeña siguió, o precedió, a la más grande.

Finalmente, la sexta y última diferencia existente entre los dos protocolos, consisten en la manera como se liberan las conexiones:

- OSI utiliza una desconexión abrupta en la que una serie de TPDU de datos pueden ser seguidos directamente por una TPDU DR. Si las TPDU de datos se llegaran a perder, el protocolo no los podría recuperar y la información, al final se perdería.
- TCP utiliza una comunicación de ida-vuelta-ida para evitar la pérdida de datos en el momento de la desconexión. El modelo OSI trata este problema en la capa de sesión. Es importante hacer notar que la Oficina Nacional de Normalización de Estados Unidos estaba tan disgustada con esta propiedad de TP4, que introdujo TPDU adicionales en el protocolo de transporte para permitir la desconexión sin que hubiera una pérdida de datos.

2.7 LO MÁS IMPORTANTE

El protocolo TCP/IP es el medio de comunicación más importante en la actualidad ya que gracias a este y a todos los protocolos que lo conforman han reducido en gran medida las actividades diarias, por ejemplo; el enviar y recibir información a través de Internet e Intranet.

La prioridad del protocolo TCP/IP es la transferencia de información e Internet cuya herramienta sea convertido en una de las más novedosas e influyentes mundialmente y gracias a estos se puede transferir información de maquina a maquina (Protocolo **FTP**), tener control de una máquina remotamente como se estuviera trabajando en sitio con ésta (Protocolo **TELNET**) o aquel que permite la gestión remota de dispositivos de red (Protocolo **SNMP**), sin olvidar que en cada una de las capas (de Red, Internet, Transporte y Aplicación) que conforman el protocolo TCP/IP, cada una de ellas tiene una función en concreto en la manipulación de la información que es transmitida en paquetes y estos al ser recibidos en la máquina destino son unidos y así contar con la información tal cual es percibida por el usuario. Cabe hacer hincapié en las diferencias que se hacen con el modelo OSI, si bien se estudia es solo para contemplar éstas y ver debidamente el desarrollo que se tiene del protocolo TCP/IP.

CAPÍTULO III

1. APLICACIONES Y FUTURO DEL PROTOCOLO TCP/IP

El protocolo TCP/IP, así como su desarrollo es de suma importancia por las tantas aplicaciones en las que actualmente se emplea, por esta razón es el tema central del presente capítulo.

3.1 VoIP

Se entiende por voz sobre IP o VoIP (Voice Over Internet Protocol) a la digitalización de la voz y su transmisión a través de la red, mediante la conmutación de paquetes en los que la información se transfiere fragmentada. La conmutación de estos se envía de forma independiente con una misma dirección de destino donde vuelve a reagruparse y de esta forma es recuperada.

3.1.1 VENTAJAS DE LA VoIP

En el ahorro de costos Administrativos:

1. Todos los dispositivos telefónicos aprovechan el cableado Ethernet existente, con lo que se simplifica la instalación y mantenimiento del sistema.
2. Para instalar una nueva extensión telefónica solamente se enchufar a la red de computadoras y el sistema la detecta e instala automáticamente.
3. Los cambios en la configuración de la central se realizan a través de una interfase Web.

En la operatividad de los usuarios:

1. Al disponer de una operadora automática, se ahorra en costos de personal pues se evita tener a una recepcionista.

2. Las delegaciones pueden estar conectadas con la central a través de una conexión ADSL. Las llamadas entre las delegaciones y la central no tienen costo telefónico.
3. Un usuario que esté fuera de la oficina puede conectarse también al sistema y convertirse en una extensión más de la empresa.

Se contaría con una mejor operación:

1. Una integración total con los sistemas PC actuales. Un ejemplo de esta integración es que podemos marcar el teléfono al que queremos y llamar directamente desde Outlook.
2. Se puede usar un PC para establecer las comunicaciones telefónicas. No es necesario usar un teléfono físico. Los usuarios móviles disfrutan de mayor libertad.
3. La gestión de las llamadas se potencia a funciones como la operación automática, el listado de llamadas, desvíos, buzón de voz, etc.

3.1.2 PROTOCOLOS QUE INTERFIEREN EN LA VoIP.

PROTOCOLO H.323

El protocolo ***H.323*** es un conjunto de tecnologías y protocolos que permiten la transmisión de voz, sobre una red conmutada por paquetes mediante el protocolo IP y ha sido tradicionalmente más asociado con la Unión International de Telecomunicaciones.
Las entidades H.323, pueden proveer comunicaciones de datos, video o audio en tiempo real.

En la (figura 3.1) se ve la función y enfoque de los 4 dispositivos que difieren para llevar acabo el cumplimiento de una llamada.

1. Terminal
2. Gatekeeper
3. Gateway
4. Unidad de Control Multipunto (MCU)

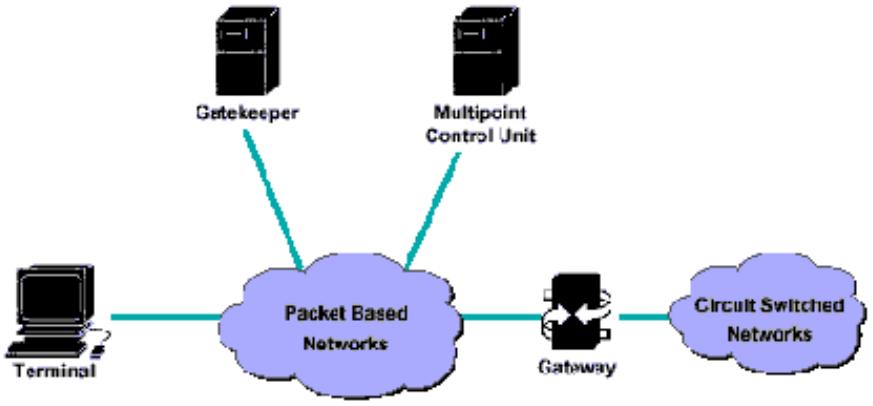

Figura 3.1

La terminal es el dispositivo que inicia una llamada, enviando la información de destino al Gatekeeper. En la norma H.323, el Gatekeeper (que puede estar integrado físicamente con el terminal), es el encargado de autorizar la llamada, y rutear (a través de la red IP) a su destino final. Si el destino final es un abonado a la red pública convencional, en algún punto, necesariamente, se debe producir la conversión de paquetes IP, a paquetes de voz digitalizada, capaces de atravesar una central pública (PSTN), y una red de conmutación de circuitos hasta llegar al abonado llamado. El elemento donde se produce esta conversión se denomina Gateway.

Finalmente, el MCU (Unidad de Control Multipunto) se utiliza en el caso de realizarse conferencias con múltiples participantes simultáneos, lo que es mucho más simple de hacer en IP que con líneas telefónicas convencionales.

El H.323, en realidad, no es un protocolo único, sino una especificación tipo "Paraguas", que abarca la transmisión de Audio / video propiamente dichos, la transmisión de fax, y todo lo relacionado con la señalización y el control de las llamadas, utilizando las normas H.225 y H.245. En la (figura 3.2) se muestra la arquitectura del protocolo H233, donde muestra la ubicación de estas normas.

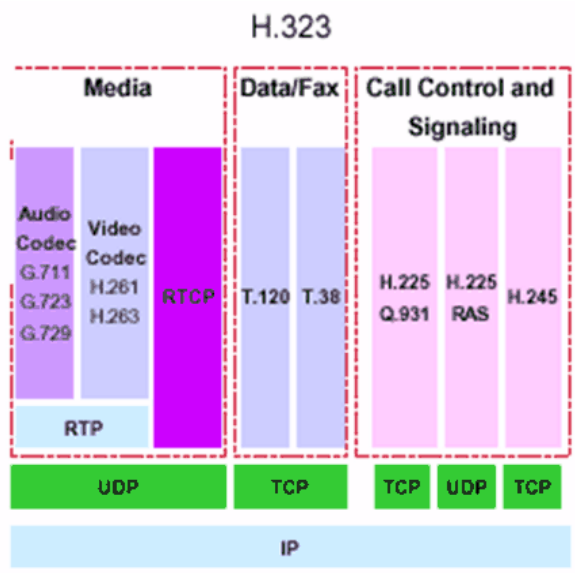

Figura 3.2

PROTOCOLO SIP

El protocolo ***SIP*** (Session Initiation Protocol) es un estándar para la iniciación, modificación y finalización de sesiones interactivas donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos en línea y realidad virtual. SIP es uno de los protocolos de señalización para voz sobre IP, acompañado de H.323.

DISEÑO DEL PROTOCOLO SIP

Los clientes SIP usan el puerto 5060 en TCP y UDP (User Datagram Protocol) para conectar con los servidores SIP. SIP es usado simplemente para iniciar y terminar llamadas de voz y video. Todas las comunicaciones de voz /video van sobre RTP (Real-time Transport Protocol).

Su objetivo fue aportar un conjunto de funciones de procesamiento de llamadas y capacidades presentes en la red pública conmutada de telefonía. Que permitan a un teléfono común a llamar a un número, provocar que un teléfono suene al ser llamado, escuchar la señal de tono o de ocupado.

Aunque existen muchos otros protocolos de señalización para Vo IP, SIP se caracteriza porque sus promotores tienen sus raíces en la comunidad IP y no en la industria de las telecomunicaciones. Ha sido estandarizado y dirigido principalmente por el IETF.

SIP funciona en colaboración con otros protocolos pero sólo interviene en la parte de señalización al establecer la sesión de comunicación. SIP actúa como envoltura al SDP, que describe el contenido multimedia de la sesión, por ejemplo qué puerto IP y códec se usarán durante la comunicación, etc. En un uso normal, las sesiones SIP son simplemente flujos de paquetes de RTP (Real-time Transport Protocol). RTP es el portador para el actual contenido de voz y video.

SIP es similar a HTTP y comparte con él algunos de sus principios de diseño y sigue una estructura de petición-respuesta. Los promotores de SIP afirman que es más simple que H.323. Sin embargo, actualmente se ha vuelto tan complejo como H.323. SIP comparte muchas códigos de estado de HTTP, como el familiar '404 no encontrado' (404 not found). SIP y H.323 no se limitan a comunicaciones de voz y pueden mediar en cualquier tipo de sesión comunicativa desde voz hasta video o futuras aplicaciones todavía sin realizar.

ELEMENTOS SIP DE RED.

Las terminales físicas, dispositivos con el aspecto y forma de teléfonos tradicionales, pero que usan SIP y RTP para la comunicación, están disponibles comercialmente gracias a muchos fabricantes. Algunos de ellos usan numeración electrónica (ENUM) o DUNDi para traducir los números existentes de teléfono a direcciones SIP usando DNS (Domain Name Server), así llaman a otros usuarios SIP saltándose la red telefónica. Hoy en día, ya son habituales los terminales con soporte SIP por Microsoft Windows Messenger usa SIP y Apple Computer anunció y publicó en fase beta su iChat, una nueva versión compatible con el AOL Instant Messenger que soporta charlas de audio y video a través de SIP.

SIP también requiere del proxy y elementos de registro para dar un servicio práctico, aunque dos terminales SIP puedan comunicarse sin intervención de infraestructuras SIP (razón por la que el protocolo se define como punto-a-punto), este enfoque es impracticable para un servicio público. Hay varias implementaciones de softswitch (de Nortell, Sonus y

muchas más) que pueden actuar como proxy y elementos de registro. También aporta funciones de registro que permiten al usuario informar de su localización actual a los servidores proxy.

A continuación en la (figura 3.3) representa un esquema básico de cómo se realiza la comunicación entre 2 terminales IP utilizando el protocolo SIP.

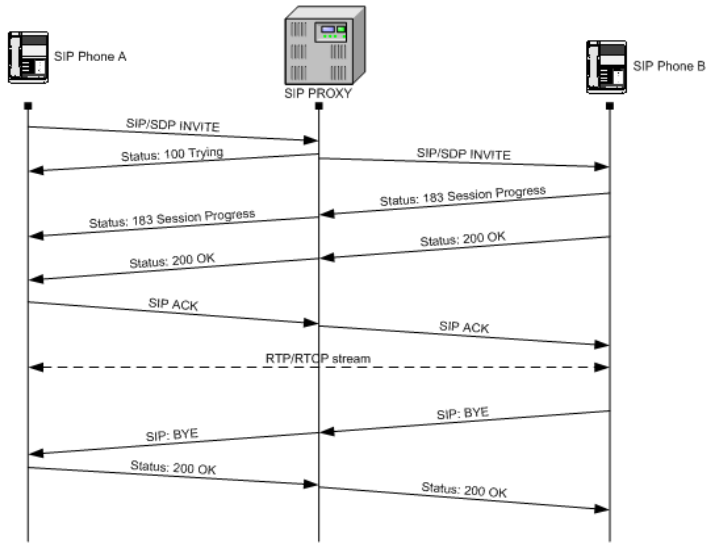

Figura 3.3

3.1.3 ELEMENTOS PARA IMPLEMENTAR UNA Vo IP

Para poder implementar un servicio Vo IP requerimos de los siguientes elementos: Un PBX IP (PBX IP Híbrido), un Call Manager, router o switches que distribuyan las llamadas y toda la información que se transmite por la red, y teléfonos IP, enseguida describimos cada uno de ellos:

PBX IP

Un PBX IP (Private Branch Exchante) es un sistema que conmuta llamadas entre los usuarios de VoIP en líneas locales y permite a los usuarios compartir cierto número de líneas telefónicas externas, como se muestra en la (figura 3.4). El PBX IP típico también

puede conmutar llamadas entre un usuario VoIP y un usuario de la telefonía tradicional, o entre dos usuarios de telefonía tradicional, en la misma forma en que lo hace un PBX convencional.

Con sistemas convencionales de PBX se requieren redes separadas para comunicaciones de voz y de datos. Una de las principales ventajas de un PBX IP es su utilización de convergencia de redes de voz y datos, es decir, el acceso a la Internet al igual que la comunicación por VoIP y la telefonía tradicional son todas posibles con una sola línea de acceso a cada usuario. Esto provee flexibilidad en la medida que las empresas crecen y pueden reducir los costos de operación y mantenimiento a largo plazo.

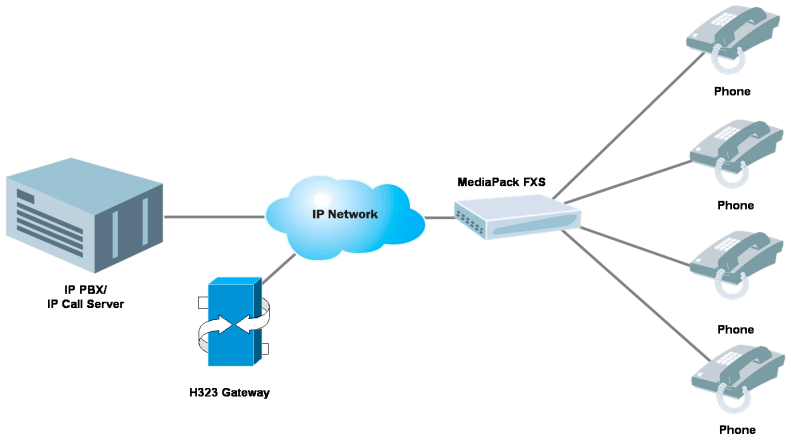

Figura 3.4

CALL MANAGER

Call Manager es el componente de llamar proceso, software basado en la solución de la telefonía del IP, tal y como lo muestra la (figura 3.5). El software amplía características y funciones de la telefonía de la empresa a los dispositivos de la red de la telefonía del paquete tales como teléfonos IP, medios que procesan los dispositivos, entradas voz-sobre-IP, y usos de multimedia. Los datos adicionales, la voz, y los servicios video tales como mensajería unificada, videoconferencia de multimedia, centros de colaboración del contacto, y sistemas interactivos de la respuesta de multimedia obran recíprocamente con la

solución de la telefonía del IP a través del interfaz de programación de uso abierto de la telefonía de CallManager (API).

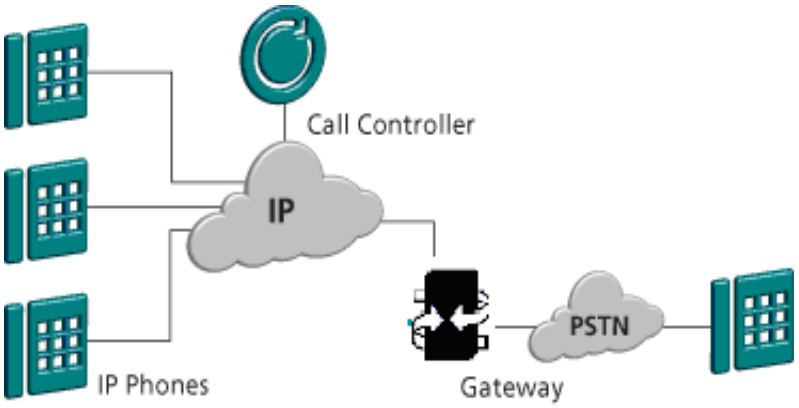

Figura 3.5

PSTN (Public Switched Telephone Network). Se refiere al sistema telefónico internacional basado en alambres de cobre que transportan datos analógicos de voz.

ROUTER

Un router (en español 'enrutador' o 'encaminador') es un dispositivo hardware o software de interconexión de redes de computadoras que opera en la capa tres del modelo OSI. Este dispositivo interconecta dispositivos de red o redes enteras, como se muestra en la (figura 3.6). Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red. Al igual de toma decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirigen los paquetes hacia el segmento y el puerto de salida adecuados. Sus decisiones se basan en diversos parámetros. Una de las más importantes es decidir la dirección de la red hacia la que va destinado el paquete Comer (Douglas, E. Prentice (2000) Redes Globales de Información con Internet y TCP/IP Principios Básicos. Protocolos y Arquitectura. (3ra. ed.)). Otras decisiones son la carga de tráfico de red en las distintas interfaces del router y establecer la velocidad de cada una de ellas, dependiendo del protocolo que se utilice.

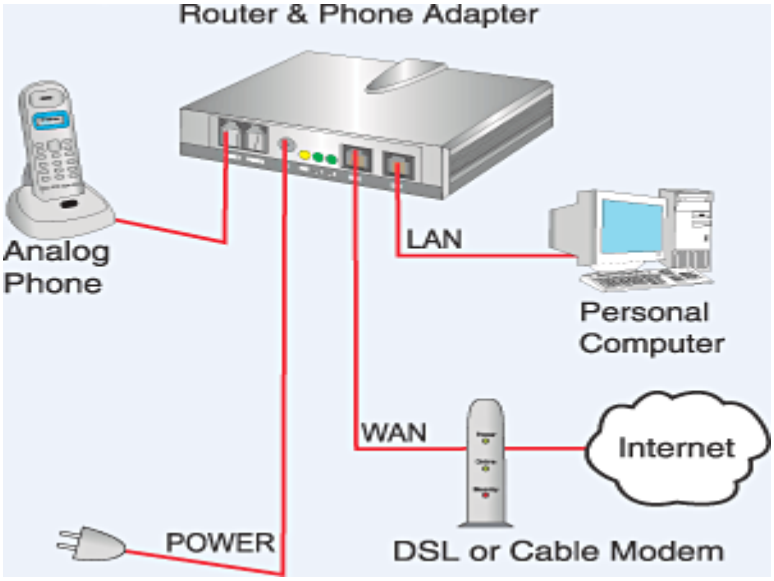

Figura 3.6

TELÉFONOS IP

Los teléfonos IP amplían nuestros servicios de telefonía basada en la Internet Protocol permitiendo a empresas y hogares una mayor productividad, movilidad y superioridad tecnológica.

Esta nueva tecnología proporciona varias ventajas que a continuación describimos:

Productividad

1. Función para controlar el historial de llamadas.
2. Dirección MAC para propósitos de autenticación.
3. Auto programación propia o en el navegador.

Movilidad

1. No requiere la computadora.
2. Permite asignarle un Número PSTN.
3. Permite seleccionar el tipo de llamada IP o de llamada analógica regular.

Superioridad Tecnológica

1. Un sistema de recuperación de pérdidas de paquetes de voz basado en un sistema que repite el último paquete de voz después de la pérdida.
2. Capaz de desplegar detrás de una muralla defensiva (Firewall).
3. Disponibilidad de NAT para permitir la funcionalidad del teléfono IP como un servidor DHCP.

En el mercado existen dos tipos de telefonía IP: híbrida y Pura. La híbrida consiste en añadir tarjetas IP a los PBX tradicionales, pero no ofrece las ventajas de la telefonía IP pura. Tales como la administración de una sola red y la variedad de servicios avanzados a los usuarios.

La híbrida tiene como ventaja que las empresas no desechen su PBX tradicional, los teléfonos digitales y demás componentes de la red de telefonía, pero sólo ofrece una pequeña parte de los beneficios de la telefonía IP pura.

3.1.4 FACILIDADES AVANZADAS DEL SISTEMA

Cada usuario tendrá asignada una extensión principal y 4 secundarias, una terminal y un password de acceso al sistema, la autenticación del usuario permite independizar la asociación del usuario a la terminal. Esto facilita tener un control independiente de cada usuario y cada uno de los recursos abajo descritos:

El servicio de localización por nombre.

1. Agenda corporativa.
2. Registro de llamadas recibidas, enviadas y perdidas.
3. Telemantenimiento y teléconfiguración remota.
4. Acceso al correo electrónico desde el terminal.
5. Mensajería corta con pasarela a SMS.

ALTERNATIVAS DEL TELÉFONO IP

1. Uso de dispositivos comerciales de adaptación para teléfonos Analógicos a terminales H.323.
2. Hace posible el uso del teléfono convencional.
3. Productos con estas características en el mercado:
    - Internet Phone Wizard de Actiontec
    - Adaptadores de ADDATEL: Surf 'n Talk
    - Adaptadores de Quicknet: Internet PhoneJACK y LineJACK

APLICACIONES DE LA VoIP

1. Administración inteligente de llamadas. El usuario elige el cómo responder a una llamada, por medio del chat, forma tradicional, seleccionar que su línea dé el tono de ocupado según quien llame.
2. Servicio de directorio. Acceso inmediato y directo a los números telefónicos de todos los integrantes de un grupo o empresa.
3. Mensajería unificada e instantánea.
4. Conferencia y videoconferencia entre más de dos usuarios.
5. Aplicaciones para empresas distribuidas. Para comunicar sucursales o usuarios móviles.
6. Integración con aplicaciones de misión crítica. Se puede acceder a información relacionada con ventas, producción, etc.
7. Comunicación multimedia. Además de la de voz, se puede intercambiar archivos.
8. Comunicación desde cualquier lugar.

3.1.5 FUTURO DE LA TELEFONIA IP

El futuro de la telefonía IP también se pinta sin cables. El auge de las redes locales con tecnología Wi - Fi ha dado paso a la telefonía inalámbrica.
Los sectores como la educación, salud, distribución y manufactura serán los primeros en adoptar esta tecnología puesto que al usar Wi-Fi, tendrán una mayor respuesta a sus demandas de trabajo.

WI- FI

Wi-Fi (Wireless Fidelity) es la tecnología utilizada en una red o conexión inalámbrica, para la comunicación de datos entre equipos situados dentro de una misma área (interior o exterior) de cobertura, tal y como se muestra en la (figura 3.7).

Conceptualmente, no existe ninguna diferencia entre una red con cables (cable coaxial, fibra óptica, etc.) y una inalámbrica. La diferencia está en que las redes inalámbricas transmiten y reciben datos a través de ondas electromagnéticas, lo que supone la eliminación del uso de cables y, por tanto, una total flexibilidad en las comunicaciones.

De entre todos los tipos de redes inalámbricas, son las redes inalámbricas IEEE 802.11b las que son conocidas como Wi-Fi (Wireless Fidelity), debido a su amplia difusión en el mercado. Los productos y redes Wi-Fi aseguran la compatibilidad efectiva entre equipos.

En una red inalámbrica cada ordenador dispone de un adaptador de red inalámbrico. Estos adaptadores se conectan enviando y recibiendo ondas de radio a través de un transceptor (transmisor-receptor), que puede situarse en cualquier lugar, interior o exterior, dentro del área de cobertura, sin la preocupación del cableado.

Las redes inalámbricas permiten la transmisión de datos a velocidades de 11 Mbps o incluso superiores, lo que proporciona rapidez suficiente para la mayoría de las aplicaciones.

Se puede decir que el entorno Wi-Fi es la solución idónea que unifica movilidad y conectividad en la transmisión de datos, ofreciendo una nueva posibilidad de "oficina móvil".

Figura 3.7

VENTAJAS AL USAR WI - FI

El Wi-Fi, debido a la eliminación de los cables, ofrece claras ventajas en las comunicaciones:

1. Movilidad: desde cualquier sitio dentro de su cobertura, incluso en movimiento.
2. Fácil instalación: más rapidez y simplicidad que la extensión de cables.
3. Flexibilidad: permite el acceso a una red en entornos de difícil cableado.
4. Facilidad: permite incorporar redes en lugares históricos sin necesidad de extender cable.
5. Adaptabilidad: permite frecuentes cambios de la topología de la red y facilita su escalabilidad.

Facilita la ampliación de nuevos usuarios a la red, sin necesidad de nuevos cables y permite la organización de redes en sitios cambiantes o situaciones no estables (lugares de emergencia, congresos, sedes temporales, etc.).

3.2 VIDEOTELEFONÍA

Entendemos por videotelefonía al servicio de comunicación audiovisual entre dos usuarios ubicados en diferentes puntos geográficos, es denominada también como videoconferencia escritorio a escritorio. Una videotelefonía es bidireccional, simétrica y en tiempo real lo que da la apariencia de conversar "cara a cara". El sistema desarrollado facilita la comunicación de dos personas en una red de área local, utiliza una cámara de video y un micrófono para cada estación de trabajo. La sincronización de audio y video se realiza para que un conjunto de personas puedan ser conectadas y simular una operadora de una central telefónica. Se proporciona además de una comunicación audiovisual, una comunicación instantánea escrita que es comúnmente conocida como "chat" en Internet. Existe una diversidad de estándares para almacenamiento y recuperación audiovisual, con los que se puede tener diferentes requerimientos de red para la transmisión para tener un bajo consumo en el ancho de banda de la red. Se tiene una interfaz muy amigable al usuario final, que es actualmente un factor muy importante para ser usado por las personas.

3.2.1 RESEÑA HISTÓRICA DE LA VIDEOTELEFONÍA

Básicamente, la videotelefonía consiste en dos emisiones simultáneas, y en sentido contrario, de *videostreaming* en directo, con la salvedad de que se realizan en tiempo real. La primera prueba de concepto comenzó a finales de 1998 y finalizó en octubre de 1999; y consistió en la conexión de dos PABX, mediante un enlace ATM dedicado PVC (*Permanent Virtual Circuit*).

Entre los años 2000 y 2001, se realizó el mismo experimento sobre redes IP, dando origen a lo que se denomina tecnologías de VoIP. Desde entonces, la videotelefonía se ha desarrollado sobre casi todas las redes de acceso público, incluyendo el desarrollo de terminales (videoteléfonos) basados en hardware, sobre el protocolo ATM (*Asynchronous Transfer Mode*), sobre RDSI y sobre redes IP. Hasta ahora, las redes de datos móviles no presentaban ni el ancho de banda ni la latencia necesarias (alrededor de 1.5 segundos) para proporcionar servicios de videotelefonía, pero con la implantación del sistema UMTS (Universal Móvil Telecomunication System), que amplía el ancho de banda y reduce notablemente la latencia, es factible este tipo de servicios.

Para UMTS la videotelefonía es una de las llamadas «killer application », a la que se ha dado gran importancia, comprobable por el hecho de que la mayoría de los primeros terminales comerciales se fabrican con hardware y software preparados para este servicio.

Esto incluye una serie de elementos de hardware, como una cámara de video enfocada al usuario (una cámara rotatoria, o dos cámaras, una en cada lado del terminal), y software, como la inclusión de los estándares necesarios; o la posibilidad de generar conexiones de datos de circuito a 64 kbits, además de las conexiones de datos de paquetes normales para otros servicios.

Por parte de las empresas operadoras también se aprecia un esfuerzo en cuanto a la inclusión de estos servicios, proporcionando el tipo de conexión de videotelefonía de 64 kbits. Diversos fabricantes como Ericsson o Radvision proporcionan *videogateways* que permiten la Interconexión de sistemas de videotelefonía entre varios tipos de redes.

3.2.2 LA VIDEOTELEFONÍA MÓVIL

La videotelefonía requiere, como mínimo, de las terminales de los clientes y de un sistema de red que permita localizar al usuario con el que se pretende establecer la comunicación. En un entorno real son necesarios varios elementos, ver (figura 3.8).

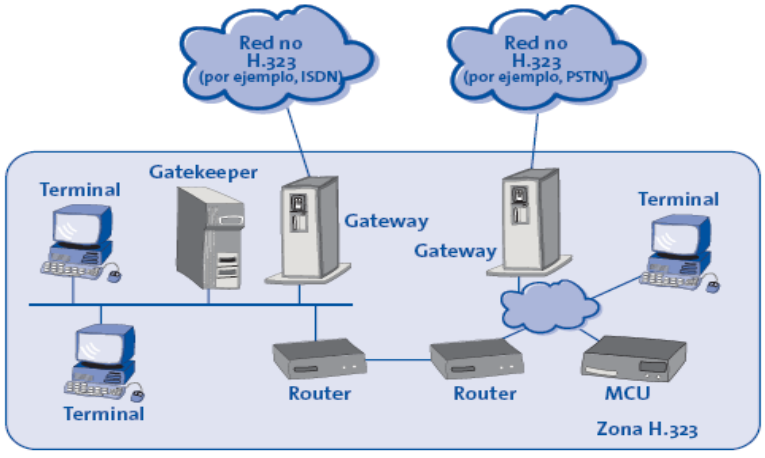

Figura 3.8

1. ***La terminal.*** Es el equipo del cliente cuyas funciones básicas consisten en obtener el video, el audio (para codificarlos y enviarlos) y de recibir los canales de video y audio codificados (para descodificarlos y, finalmente, presentarlos). Adicionalmente intercambia datos de control y señalización con la red.

2. ***El "gatekeeper".*** Se encarga de almacenar la información de las direcciones de los usuarios, así como controlar su estado y las sesiones abiertas. Al igual que de enrutar las señales de llamada en caso de ser necesario, y de realizar la admisión y control de las sesiones de usuario.

3. ***La pasarela ("gateway").*** Este nos permite la interconexión de redes. Su función es traducir los datos de control y de establecimiento de sesión, así como los datos multimedia entre redes (un paquete UDP de petición de conexión sobre una red IP, se traduce en un «*RING*» según la señalización de una PSNT). También es el encargado, en ciertos casos, de realizar la recodificación de los contenidos multimedia entre dos clientes que no posean un *codec* común.

4. ***La unidad MCU.*** Es un elemento que sólo es necesario para realizar la interconexión simultánea de varios clientes en una misma multiconferencia.

3.2.3 PERSPECTIVAS FUTURAS

Las perspectivas a futuro más destacables son principalmente dos y las cuales analizamos a continuación:

3.2.3.1 ESTÁNDAR DE CODIFICACIÓN DE VIDEO H.264

Para conseguir una mejora notable en las prestaciones de las tecnologías de V*ideostreaming* y videoconferencia es optimizar la codificación de vídeo.

Para anchos de banda bajos, existen básicamente dos estándares y multitud de adaptaciones.

Los dos estándares son:

1. H.263, desarrollado por el grupo *Video Coding Experts Group* (VCEG) perteneciente a la ITU-T.
2. MPEG-4, desarrollado por el grupo *Motion Picture Experts Group* perteneciente a la ISO/IEC. Ambos estándares son el resultado del desarrollo y evolución de otros anteriores.

En el año 2001, el grupo MPEG decidió unir esfuerzos con el VCEG para desarrollar un único codificador de vídeo universal, formándose el JVT (*Joint Video Team*), este mismo estándar se llama H.264 para la ITU-T, y MPEG-4 Part 10 para la ISO. El nombre común correcto es H.26L, pero por extensión se le llama H.264.

El cambio más notable de este esquema reside en el uso de los elementos, ya que se utiliza básicamente el mismo diagrama de flujo tanto para la codificación como para la descodificación.

Los cambios más destacables que hacen el codificador de vídeo H.264 dos veces más eficiente que MPEG-4, en cuanto a la estimación de movimiento, son:

1. El uso de submacrobloques desde 4x4 hasta 16x16 píxeles y predicción de movimiento a un octavo de píxel. En el futuro se soportarán incluso resoluciones mayores que un octavo.
2. El uso de múltiples imágenes reconstruidas para la predicción, tanto pasadas como futuras.
3. La búsqueda de vectores de movimiento más allá de los bordes de la imagen.

En lo que se refiere a la transformación espacial, los cambios más destacables son:

1. La predicción fina mediante bloques de 4x4 cuando mejore el rendimiento, y el uso de macrobloques de 16x16 para las partes planas de las imágenes.
2. Los modos de transformación dependientes de la dirección. Para poder utilizar los distintos modos es necesario realizar la transformación en el dominio espacial antes

de aplicar la DCT. Se definen cuatro modos para los bloques de 4x4 y nueve para los de 16x16.

3. El cálculo de los residuos de estimación mediante bloques de 4x4.
4. La aplicación de la DCT a zonas de tamaño variable en función de su correlación (por ejemplo, 4x8, 8x8, etc.).
5. Los algoritmos de transformación basados en aritmética entera sin el uso de multiplicaciones, lo que permite aplicar la IDCT sin pérdidas por redondeo.
6. El filtro de eliminación de efecto bloque interno a la transformación, lo que produce una mejora subjetiva de la calidad de la imagen sin coste de bits.

En cuanto a la codificación entrópica, se definen dos algoritmos alternativos:

1. El algoritmo CAVLC (*Context-Adaptive Variable Length Coding*), basado en el uso de tablas constantemente adaptadas mediante un estudio estadístico de los símbolos ya transmitidos.
2. El algoritmo CABAC (*Context-Adaptive Binary Arithmetic coding*), basado en el aumento de eficiencia en los casos en los que es estadísticamente mucho más probable la aparición de ciertos símbolos en lugar de otros.

3.2.3.2 CONVERGENCIA ENTRE VIDEOSTREAMING Y VIDEOTELEFONÍA.

La videotelefonía y el *videostreaming* parten del mismo principio: el envío de contenidos multimedia (típicamente audio y vídeo, pero no exclusivamente) a un receptor que los va mostrando simultáneamente a su llegada. Sin embargo, los requisitos de ambos servicios difieren en lo siguiente:

1. La videotelefonía es bidireccional, es un servicio P2P, mientras que el *videostreaming* es un servicio unidireccional cliente-servidor.
2. La videotelefonía requiere una demora sobre el tiempo real muy pequeña (típicamente de unos 100 a 200 milisegundos), esto es, requiere codificar, enviar,

recibir, descodificar y presentar los contenidos en menos de ese tiempo. Sin embargo, el *videostreaming* no es estrictamente un servicio en tiempo real, ya que los contenidos están pregrabados en el servidor y habitualmente se emplea algún mecanismo de *buffer* en el cliente.

Se han especificado estándares diferentes para cada tipo de servicio debido a las diferencias que se han enumerado en los requisitos, de manera que:

1. En lo que respecta a los servicios de videotelefonía, el 3GPP define un estándar basado en H.324 para videotelefonía sobre conmutación de circuitos, con ancho de banda y latencia garantizados.
2. En el caso del *videostreaming*, el 3GPP define un estándar basado en H.323 para *streaming* sobre redes de paquetes, sin ancho de banda ni tiempo de vuelo de los paquetes garantizados.

Para la integración de ambas tecnologías en un servicio es necesario contar con elementos de red que cambien de un estándar a otro «en el aire» y en tiempo real. Estos elementos de red son las pasarelas (*gateways*), que permiten transferir los datos multimedia y de control de un tipo de redes a otro. En la (figura 3.9) se muestra una infraestructura para la integración de ambas tecnologías.

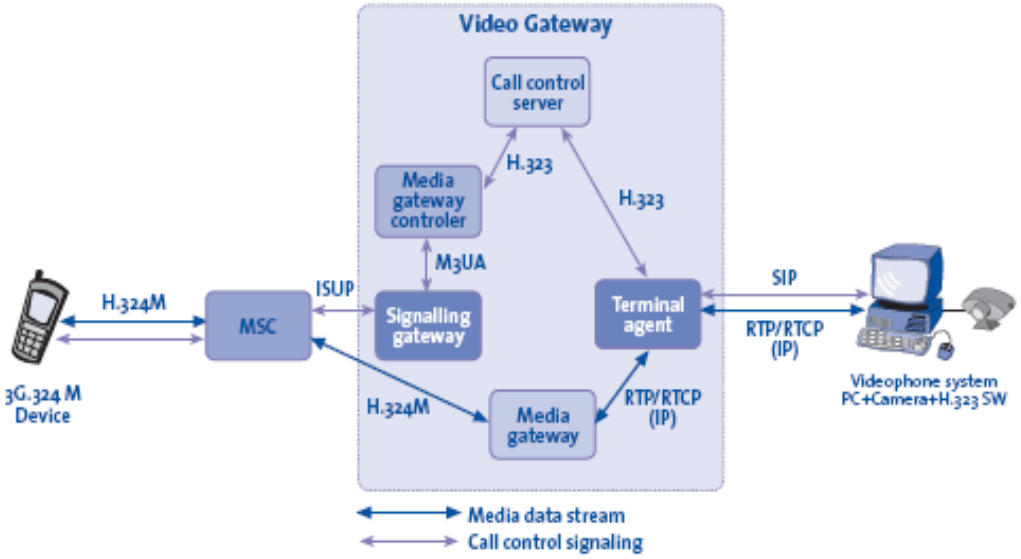

Figura 3.9

En algunas ocasiones hay que tener en cuenta que, además de cambiar la información de control, puede ser necesaria una recodificación del vídeo y audio entre dos terminales, y debe hacerse en tiempo real. Un operador dotado con esta clase de infraestructura podría ofertar servicios adicionales como mensajería multimedia. De manera similar a como funciona un buzón de voz, cuando un usuario intentara establecer una videoconferencia con otro y la terminal de este último no estuviera disponible, se conectaría la del primer usuario a un sistema de videoconferencia que grabaría el mensaje del usuario. Al conectar el segundo usuario su terminal, el sistema le suministraría el mensaje, bajo petición, mediante tecnologías de *streaming*

3.3 FUTURO DEL PROTOCOLO TCP/IP

LA NUEVA VERSIÓN DE IP (IPng)

La nueva versión del protocolo IP recibe el nombre de IPv6, aunque es también conocido comúnmente como IPng (Internet Protocol Next Generation). El número de versión de este protocolo es el 6 (que es utilizada en forma mínima) frente a la anterior versión utilizada en forma mayoritaria. Los cambios que se introducen en esta nueva son muchos y de gran importancia, aunque la transición desde la versión antigua no debería ser problemática gracias a las características de compatibilidad que se han incluido en el protocolo. IPng se ha diseñado para solucionar todos los problemas que surgen con la versión anterior, y además ofrecer soporte a las nuevas redes de alto rendimiento (como ATM, Gigabit Ethernet, etc.)

Una de las características más llamativas es el nuevo sistema de direcciones, en el cual se pasa de los 32 a los 128 bit, eliminando todas las restricciones del sistema actual.

Otro de los aspectos mejorados es la seguridad, que en anterior constituía uno de los mayores problemas. Además, el nuevo formato de la cabecera se ha organizado de una manera más efectiva, permitiendo que las opciones se sitúen en extensiones separadas de la cabecera principal.

FORMATO DE LA CABECERA.

El tamaño de la cabecera que el protocolo IP v6 añade a los datos es de 320 bit, el doble que en la versión antigua. Sin embargo, esta nueva cabecera se ha simplificado con respecto a la anterior. Algunos campos se han retirado de la misma, mientras que otros se han convertido en opcionales por medio de las extensiones. De esta manera los routers no tienen que procesar parte de la información de la cabecera, lo que permite aumentar de rendimiento en la transmisión. El formato completo de la cabecera, (figura 3.10) sin las extensiones es el siguiente:

1. ***Versión:*** Número de versión del protocolo IP, que en este caso contendrá el valor 6. Tamaño: 4 bit.
2. ***Prioridad:*** Contiene el valor de la prioridad o importancia el paquete que se está enviando con respecto a otros paquetes provenientes de la misma fuente. Tamaño: 4 bit.
3. ***Etiqueta de flujo:*** Campo que se utiliza para indicar que el paquete requiere un tratamiento especial por parte de los routers que lo soporten. Tamaño: 24 bit.
4. ***Longitud:*** Es la longitud en bytes de los datos que se encuentran a continuación de la cabecera. Tamaño: 16 bit.
5. ***Siguiente cabecera:*** Se utiliza para indicar el protocolo al que corresponde la cabecera que se sitúa a continuación de la actual. El valor de este campo es el mismo que el de protocolo en la versión 4 de IP. Tamaño: 8 bit.
6. ***Límite de existencia:*** Tiene el mismo propósito que el campo de la versión 4, y es un valor que disminuye en una unidad cada vez que el paquete pasa por un nodo. Tamaño: 8 bit.
7. ***Dirección de origen:*** El número de dirección del host que envía el paquete. Su longitud es cuatro veces mayor que en la versión 4. Tamaño: 128 bit.
8. ***Dirección de destino:*** Número de dirección de destino, aunque puede no coincidir con la dirección del host final en algunos casos. Su longitud y tamaño son iguales a la de dirección de origen.

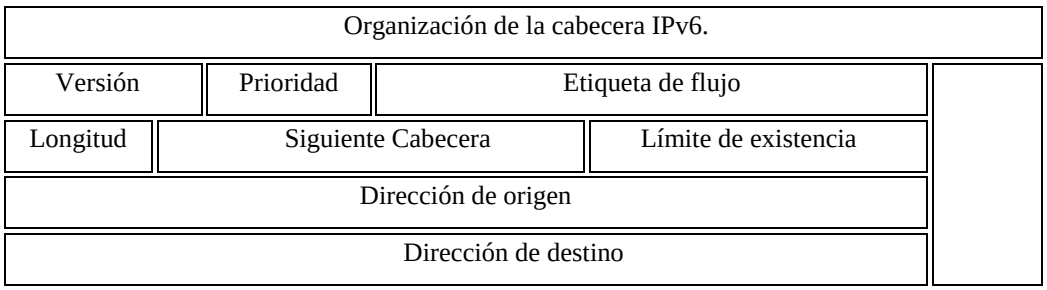

Figura 3.10

Las extensiones que permite añadir esta versión del protocolo se sitúan inmediatamente después de la cabecera normal, y antes de la cabecera que incluye el protocolo de nivel de transporte. Los datos situados en cabeceras opcionales se procesan sólo cuando el mensaje llega a su destino final, lo que supone una mejora en el rendimiento. Otra ventaja adicional es que el tamaño de la cabecera no está limitado a un valor fijo de byts como ocurría en la versión anterior.

Por razones de eficiencia, las extensiones de la cabecera siempre tienen un tamaño múltiplo de 8 bytes. Actualmente se encuentran definidas extensiones para routing extendido, fragmentación y ensamblaje, seguridad, confidencialidad de datos, etc.

DIRECCIONES EN LA IP v6

El sistema de direcciones es uno de los cambios más importantes que afectan a la versión 6 del protocolo IP, donde se han pasado de los 32 a los 128 bit (cuatro veces mayor). Estas nuevas direcciones identifican una interfaz o conjunto de interfaces y no a un nodo, aunque como cada interfaz pertenece a un nodo, es posible referirse a éstos a través de su interfaz.

El número de direcciones diferentes que pueden utilizarse con 128 bits es enorme. Teóricamente serían 2128 direcciones posibles, siempre que no apliquemos algún formato u organización a estas direcciones. Este número es extremadamente alto, pudiendo llegar a soportar más de 665.000 trillones de direcciones distintas por cada metro cuadrado de la superficie del planeta Tierra. Según diversas fuentes consultadas, estos números una vez

organizados de forma práctica y jerárquica quedarían reducidos en el peor de los casos a 1.564 direcciones por cada metro cuadrado, y siendo optimistas se podrían alcanzar entre los tres y cuatro trillones.

Existen tres tipos básicos de direcciones IPng según se utilicen para identificar a un interfaz en concreto o a un grupo de interfaces. Los bits de mayor peso de los que componen la dirección IPng son los que permiten distinguir el tipo de dirección, empleándose un número variable de bits para cada caso. Estos tres tipos de direcciones son:

1. ***Direcciones unicast:*** Son las direcciones dirigidas a un único interfaz de la red. Las direcciones unicast que se encuentran definidas actualmente están divididas en varios grupos. Dentro de este tipo de direcciones se encuentra también un formato especial que facilita la compatibilidad con las direcciones de la versión 4 del protocolo IP.
2. ***Direcciones anycast:*** Identifican a un conjunto de interfaces de la red. El paquete se enviará a una interfaz cualquiera de las que forman parte del conjunto. Estas direcciones son en realidad direcciones unicast que se encuentran asignadas a varias interfaces, los cuales necesitan ser configurados de manera especial. El formato es el mismo que el de las direcciones unicast.
3. ***Direcciones multicast:*** Este tipo de direcciones identifica a un conjunto de interfaces de la red, de manera que el paquete es enviado a cada una de ellos individualmente.

Las direcciones de broadcast no están implementadas en esta versión del protocolo, debido a que esta misma función puede realizarse ahora mediante el uso de las direcciones multicast.

3.4 LO MÁS IMPORTANTE

El protocolo TCP/IP juega un papel importante en la emisión de voz (Vo IP), videotelefonía y videoconferencia, claramente se entiende los protocolos que interfieren para este fin (protocolo H.323 y el SIP), cuya función es la de transmitir, iniciar y finalizar la comunicación de vos, video y audio entre los equipos. Para llevar acabo este fin se requiere de cierto equipo como un PBX IP, Call Manager, Rauter y por supuesto teléfonos IP, al utilizar esta tecnología las empresas adquieren ciertos beneficios tanto económicos, ahorro de tiempos y mejoras en la productividad de sus usuarios.

Gracias a esta tecnología y a la tecnología inalámbrica (Wi–Fi) es posible comunicarnos, ver con quien se habla, capacitarse con las videoconferencias, transmitir o transferir información, correos, optimización de videos, audio y buzón de voz aunque el receptor esté desconectado.

El protocolo TCP/IP está en constante desarrollo no es de extrañarse que en un futuro otras aplicaciones sean a través de esté, actualmente se estudia la versión IPv6, también conocida como IPng, proporcionando mejoras que su antecesor permitiendo soporte a redes de alto rendimiento transfiriendo 32 a 128 bit, mejorando la seguridad, así como la eficiencia de su formato de cabecera ya que ésta añade a los datos 320 bits, entre otras mejoras.

CONCLUSION

Como egresado de la Licenciatura Matemáticas Aplicadas y Computación sugiero que sus egresados tengan conocimientos en el área de las comunicaciones y redes, debido a que en el campo laboral es imprescindible y de suma importancia contar con ellos.

Cuando se estudia un tema, es de relevancia conocer sus orígenes para asignarles el peso que tiene en nuestros días para darles el enfoque y nivel adecuado.

El protocolo TCP/IP, es actualmente el mas influyente para el desarrollo de nuevas tecnologías y aplicaciones, este protocolo permite comunicarnos mundialmente, enviar y recibir videos, navegar en Internet, controlar remotamente otra máquina y todo esto gracias al conjunto de protocolos que lo conforman.

Actualmente se diseñan nuevas aplicaciones y tecnologías que facilitaran aún más las actividades cotidianas como es la telefonía IP, videotelefonía, videoconferencia, la comunicación y videocomunicación móvil (celulares). El protocolo TCP/IP no deja de sorprender y lanzó al mercado la nueva versión IPv6, mostrando mejoras para redes de alto rendimiento, seguridad, rendimiento en la transmisión y confiabilidad de datos.

Este trabajo muestra claramente cada unos de los aspectos del protocolo TCP/IP y va dirigido especialmente a toda la comunidad universitaria y carreras a fin a las comunicaciones, informática y sistemas de cómputo, por tal motivo cabe señalar que el objetivo central de dar a conocer los orígenes, características y aplicaciones del mismo de una forma concisa, concreta, sin tecnicismos y objetiva, se cumplió.

GLOSARIO

ADSL. Es una técnica de modulación para la transmisión de datos a gran velocidad sobre el par de cobre.

ANCHO DE BANDA. Es la capacidad de una línea para transmitir información.

CODIFICACIÓN ENTRÓPICA. La información posee una característica que le es muy peculiar, su cantidad siempre está en aumento y su calidad tiende a la uniformidad. Esta característica de la información se define como comportamiento entrópico

CRC (Códigos de Redundancia Cíclica). Es un mecanismo de detección de errores en sistemas digitales.

DCT (Transformada Discreta del Coseno). La imagen se divide en bloques y estos de (8x8) son transformados a una de dos dimensiones.

DHCP (Dynamic Host Configuration Protocol). Protocolo de Configuración de Hosts Dinámicos. Es un protocolo para asignar direcciones de IP dinámicas en una red.

H.225. Es un protocolo clave en la arquitectura de Vo IP H.323 definida por la ITU-T. Define la manera en que puede gestionarse el audio, video, datos e información de control en una red basada en paquetes para proveer servicios de conversación con equipos H.323. El H.225.0 tiene dos componentes destacados: la señalización de llamadas y el RAS (Registro, Admisión y Status).

H.323. Es un protocolo para la negociación de capacidades en mensajes para abrir o cerrar canales en streams multimediales.

HTTP (Hypertext Transfer Protocol). Protocolo de transferencia de hipertextos. Es un protocolo que permite transferir información en archivos de texto, gráficos, video, audio y otros recursos multimedia.

IETF (Internet Engineering Task Force). Es la organización que gestiona los estándares de Internet, diseñadores, operadores, vendedores y desarrolladores de redes relacionados con la evolución de la arquitectura de Internet y su buen funcionamiento.

ISDN (Integrated Services Digital Network). Es un servicio telefónico digital de alta velocidad para transmisión de datos y /o voz.

NAT (Network Address Translation). Es un standard de Internet que le permite a una red local (LAN) usar un grupo de direcciones de IP para el tráfico interno y otro grupo de direcciones para el tráfico externo.

NOVELL. Famosa empresa de software para redes. Su producto más conocido, Netware, fue el standard corporativo para construir LANs por más de una década. Novell se fundó en 1983.

NIC (Network Interface Card). Es un dispositivo electrónico que permite a una DTE (Data Terminal Equipment) ordenador o impresora acceder a una red y compartir recursos entre dos o más equipos (discos duros, cdrom, etc).

NSFNET. Es utilizado para hacer alusión a todas las actividades de red de las NSF (Fundación Nacional de Ciencia) fundadas.

NVT (Network Virtual Terminal). Es un dispositivo imaginario que posee una estructura básica común a una amplia gama de terminales reales. Cada host mapea las características de su propia terminal sobre las de su correspondiente NVT, y asume todos los demás hosts harán lo mismo.

PROXY.. Es un sistema que reenvía los paquetes recibidos a otra red, sin permitir el tráfico directo entre ellas, son usados en lugar de los routers.

P2P. Esta expresión viene de peer to peer (igual a igual) y hace referencia a las redes entre iguales.

SISTEMA ABIERTO. La organización de formulación de estándares define el término "sistema abierto" como un equipo informático que disfruta de compatibilidad con otros sistemas en el ámbito de programación; de sistemas operativos y de conectividad con otras máquinas del mismo o distinto fabricante, dando una impresión de que se trabaja en un sistema único.

SOCKET. Designa un concepto abstracto por el cual dos programas pueden intercambiarse cualquier flujo de datos, generalmente de manera fiable y ordenada. Queda definido por una dirección IP, un protocolo y un número de puerto.

SMS (Short Message Service). Servicio de mensajería para teléfonos celulares. Permite enviar/recibir a/desde un celular un mensaje de hasta 160 caracteres.

SNA (Systems Network Architecture). Es una arquitectura de red diseñada y utilizada para la conectividad de host —grandes ordenadores y servidores robustos que soportan millones de transacciones que por lo general son utilizados en bancos

UDP (User Datagram Protocol). Es un protocolo sin conexión que, como TCP, funciona en redes IP.

UMTS (Universal Mobile Telecommunication System) Sistema Universal de Telecomunicaciones Móviles.

X.25. Es un protocolo para que las redes de paquetes y las estaciones de usuario se puedan interconectar mediante mecanismos de control, siendo el mas importante desde el punto de vista de la red, el control de flujo, que sirve para evitar la congestión de la red.

XNS (Xerox Network System.). Fueron creados por Xerox Corporation para ser utilizados a través de una variedad de medios de comunicación, de procesadores, y de usos de la oficina.

REFERENCIAS

Barranco, B. (2001) *Mantenimiento a los Sistemas APCM* Tesis ENEP Aragón.

Cabrían, A., Borraz, E. (1993), Guía Practica de Comunicaciones y Redes Locales (2da. ed.). México: G. Pili, S.A. de C.V.

Carvallar, J. (1994), *"Internet "El Mundo en sus Manos"* (2da. ed.). AUA: Ra-Ma.

Davidson, J., Peters, J. (2000), *Voice Over IP Fundamentals SISCO System*. USA: Pearson.

Douglas, C., Prentice, E. (2000), *Redes Globales de información con Internet y TCP/IP Principios Básicos. Protocolos y Arquitectura* (2da. ed.).

Heywood, D. (2001). Redes *con Microsoft TCP/IP* (3ra. ed.). Pearson Education.

James, M. (1994), *TCP/IP Networking*. AUA: Prentice Hall.

Richard, S. W. (1999) TCP/IP Ilustrated Vol. 1. The Protocols. (2da. ed.). Wesley Professional Computing.

(1995), *Redes de Computadoras Protocolos, Normas e Interfaces*, (2da. ed.). México: Uyless Alfa Omega.

(2004), *Introduction to Internet Working*, Independence Study Tours. Education Service. 3com.