95

# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
"CAMPUS ARAGÓN"

## "IMPLEMENTACIÓN DE VOZ SOBRE IP PARA LA INTERCONEXIÓN DE CENTRALES TELEFÓNICAS REMOTAS"

**T E S I S**

QUE PARA OBTENER EL TITULO DE INGENIERO MECÁNICO ELECTRICISTA ELÉCTRICO-ELECTRÓNICA

P R E S E N T A :

GABRIEL RUBÉN CONTRERAS MAYEN



ASESOR: ING. J.J. RAMÓN MEJÍA ROLDÁN

MÉXICO 2002

# PAGINACION DISCONTINUA

**TEMA:**

Implementación de voz sobre IP para la interconexión de centrales telefónicas remotas

**OBJETIVO:**

Reducción de costos mediante generados por centrales telefónicas remotas implementando voz sobre IP a través del Multivoip 2000

***AGRADECIMIENTOS:***

*A mis padres;*
*en especial a mi madre,*
*por impulsarnos, respaldarnos*
*con el único fin de seguir adelante....*

*A mis hermanos;*
*Rita, Ricardo, Alejandra, Gustavo,*
*Rosario, Francisco y Martha,*
*por su apoyo, cariño y aprecio a*
*nuestra manera*

*Al Ing. J.J. Ramón Mejía Roldan, ya que su experiencia en la docencia, es la herramienta que marca la diferencia en la vida profesional.*

*En memoria al Ing. Juan Méndez*

*A la ENEP ARAGON, ya que desde el primer dia, significo un reto a enfrentar. Y ahora, es un honor representarla en cada momento*

*A todos con quienes he convivido, la gran experiencia de ser orgullosamente universitario y parte de la UNAM.*

*Y muy en especial a:*

***Angélica Romero Camacho,***
*por su apoyo, paciencia y amor*
*durante todo este tiempo...*

*Mil gracias Gely*

## ANTECEDENTES

A pesar de los grandes avances y del surgimiento de nuevos medios para la transmisión de información, el teléfono sigue conservando su posición estratégica y de gran influencia dentro de los modelos actuales de negocios.

Desde su invención, el teléfono tuvo que aguardar casi un siglo para modificar su funcionamiento original respecto a las nuevas implementaciones, que le permitieran transmitir información en tiempo real. Del teléfono desarrollado por Graham Bell, empleado para escuchar la voz de una habitación a otra, hasta la videotelefonía actual en el cual se transmiten las escenas de la guerra en tiempo real, que se presentan al otro lado del planeta, el teléfono ha representado un medio imprescindible para la cultura global de nuestros días.

Dentro de esta cultura de la globalización actual, la comunicación humana se manifiesta de una manera intangible y deshumanizada; perdiendo cada vez más el sentido interpersonal. Esta característica cuenta con una gran importancia, y al carecer de ella no se garantiza ninguna seguridad en la toma de decisiones criticas en ámbitos políticos, económicos, sociales, empresariales, etc.

Dentro de este contexto, el uso del teléfono permite disminuir la brecha interpersonal de la que se han separado otros los medios de comunicación y transmisión de información que se emplean cotidianamente. Cabe señalar, que esta característica, le ha permitido a posicionarse como el primer medio de comunicación, ya que cuenta con una inserción del 70% a nivel mundial. Es decir, el 71% de las localidades habitadas en el planeta cuentan con este servicio.

Esta inserción lo ubica como la herramienta de negocios más importante e indispensable dentro de las empresas. Su importancia es tal, que tan solo el

tráfico de llamadas que se realizan entre México y Estados Unidos se ubica dentro del segundo lugar de uso de telefonía global.[1]

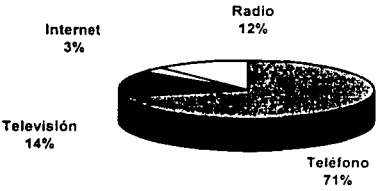





Figura 1: Inserción de Medios de Comunicación a Nivel Mundial
Fuente: ONU Junio 2001

Este tráfico surge como consecuencia de la globalización que desde la última década del siglo XX se da en el planeta, y que en especial ha experimentado el continente americano han experimentado económica, política y socialmente.

Sin embargo, a pesar de ser una herramienta de comunicación fundamental en esta globalización, y de que mantiene una gran demanda en el uso, el servicio telefónico actual, más allá de reducir los costos que su empleo genera dentro de la operación de las empresas, contrariamente se incrementa día a con día.

El gasto operativo del pago de servicios de telefonía, ocupa el primer lugar de las cuentas por pagar para el 100% de las empresas de capital privado, establecidas dentro del territorio nacional.[2]

Dentro del mismo contexto, pero con un costo por debajo del servicio de telefonía, se ubica el servicio de transmisión de datos con enlace a Internet. Este servicio adquirió una gran importancia e inserción dentro de las empresas desde mediados

[1] Fuente TELMEX. Reporte al tercer trimestre del 2001

de los años 90, hasta convertirse en una herramienta complementaria en los nuevos modelos de negocios.

Este servicio convirtió a las limitadas redes locales (LAN por sus siglas en inglés) instaladas dentro de las empresas, en nuevas redes de cómputo de grandes alcances y soluciones. Las redes dejaron de ser simples herramientas de impresión, para convertirse en un nuevo y poderoso medio de comunicación entre usuarios, clientes y proveedores de la misma.

La nueva aplicación, se presento inicialmente, mediante la adopción del correo electrónico (o E-MAIL), el cual se ha posicionado como un dato de identidad personal del mismo valor que un número telefónico local, celular, localizador o fax.

Con la rápida evolución de estas las redes de largo alcance (WAN), se desprendieron más servicios de las misma, fortaleciendo una vez más su posición estratégica como herramienta indispensable en la operación. Ya que, con la creación de redes virtuales (VPNs) protegidas por *firewalls* o barreras de seguridad, se ha logrado unir sucursales remotas de las empresas dentro de una sola red sin importar el lugar donde se ubiquen.

Esta unificación ha optimizado los tiempos de procesos y envío de información entre las mismas, reduciendo considerablemente los costos indirectos e incrementando a su vez la utilidad operativa de las empresas.

Los servicios de enlaces para transmisión de información con salida a Internet que adquieren las empresas, son proporcionados irónicamente por las principales compañías que ofrecen el servicio de telefonía comercial en nuestro país (TELMEX y AVANTEL[3]).

[2] Fuente Expansión Octubre 2001
[3] En septiembre del 2000, AVANTEL inicio con el servicio de telefonía local a empresas, mediante la implementación de T1

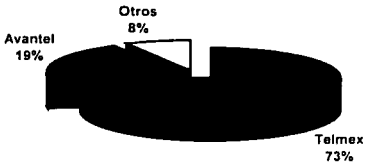



Figura 2 -
Distribución de clientes de los servicios de telefonía y enlaces con salida a Internet proporcionado por los principales ISP.

Fuente: Telmex Oct 2001

Para aquellas empresas que han contratado ambos servicios (Figura 3) a cualquier proveedor de servicio de Internet (ISPs), deberán pagar mensualmente (de acuerdo al tipo de servicio adquirido) la suma de dos facturas generadas por el uso de los servicios de telefonía y enlace para transmisión de datos con salida a Internet a un mismo o ambos proveedores.

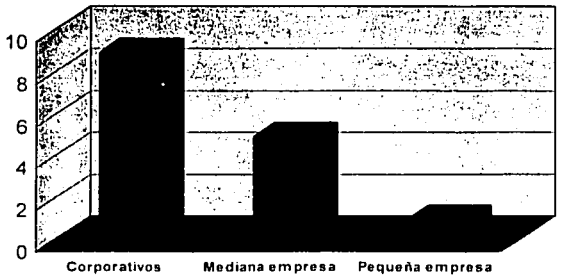





Figura 3 - Empresas privadas con servicio de transmisión de datos
Fuente Expansión Oct 2001, muestra de 10 a 1

La importancia con que estos servicios cuentan en la operación y procesos internos en las empresas, justifica los costos que son generados del uso de los mismos.

Para reducir la carga económica que presenta esta situación, es indispensable observar la evolución que la telefonía y los enlaces van experimentando. Esta observación, nos permitirá entender y optimizar procesos que antes eran mucho más complejos.

Como muestra, la telefonía ha emprendido una nueva evolución. Esta se observa, en que día a día el teléfono emplea cada vez más los servicios que una red de datos proporciona. Esta migración, es consecuencia de que el teléfono intentar mantener a como de lugar su importancia como el servicio de comunicación con mayor injerencia sobre el planeta. Sin que este paso reduzca el margen de costos.

Aunque las redes de datos, han logrado evolucionar de manera tal que pueden realizar la transmitir voz, no han logrado obtener la confiabilidad que una línea telefónica representa. Sin embargo, la reducción de costos presenta una reducción significativa en comparación a la línea telefonía convencional.

A pesar de que ambas tecnologías tienen por objetivo realizar las mismas funciones, las características de cada una es un limitante que trunca dicho objetivo.

Cada limitante que se presenta, es una nueva oportunidad de encontrar soluciones, diseños o implementaciones tecnologías que simplifique las funciones de una empresa en general.

La finalidad de este trabajo, es realizar el análisis actual y posterior, como mostrar los escenarios obtenidos una vez realizada la implementación de una solución tecnológica. Esta solución, deberá agilizar la operación y control de una empresa, sin que ello represente el consumo de grandes inversiones monetarias como de recursos humanos o de infraestructura.

# Capitulo I

# La red que emergió de la casualidad

## Capitulo I

## La red que emergió de la casualidad

### 1.1- TCP/IP , el resultado del la casualidad?

Al igual que cualquier otro tipo de proyecto científico la casualidad se ha presentado como una variable no controlada, la cual influye directamente en el resultado de la investigación y es la causa principal por la que nuestra vida cotidiana sufre un cambio radical. Esta variable no permaneció ajena durante el inicio de la investigación de Internet.

Actualmente, Internet se considera como la aplicación de computo más reciente dentro del concepto de globalización mundial que cada día nos cubre más. Sin embargo, la aplicación de Internet no es tan reciente como lo es ahora su concepto.

Ya que a más de 30 años de la idea original del proyecto, la casualidad la ha convertido en la herramienta más popular y cada día más indispensable dentro de las nuevas formas de hacer negocios y difundir información hacia cualquier lugar del breve mundo.

A diferencia de cualquier otro equipo o aplicación de computo, Internet no tiene una historia plenamente escrita, ya que sus inicios se remontan a los planes secretos de la Advanced Research Proyects Agency (ARPA) en 1969. Esta Oficina que estaba a cargo del Departamento de Defensa de los Estados Unidos, encomendó a un equipo de investigadores que junto con la asociación secreta de un grupo selecto de universidades tenían la función de desarrollar una estructura de red capaz de enlazar a todo tipo de computadoras ubicadas en oficinas gubernamentales y bases militares.

Esta red debería ser capaz de realizar la transmisión de información desde cualquier punto en tiempo real, sin importar las características de la plataforma de computo que se empleara. Sin embargo, el principio original del proyecto consistía en soportar el impacto y secuelas de un ataque nuclear emprendido por otros países considerados hostiles durante la Guerra Fría.

Durante los primeros años de la década de los años setenta esta red fue conocida como ARPANET. Las características físicas de esta, consistía en mantener una constante comunicación e integridad de la toda información generada en cualquier oficina o base militar; lo que permitirla realizar la toma decisiones acertadas con respecto a la movilización y avance de tropas de cualquier punto en donde surgiera la información.

Para lograr este objetivo era necesario superar el reto que representaba enlazar las diferentes plataformas de computo pertenecientes al ejercito. Sería posible diseñar una red que enrutara de manera eficiente el tráfico proveniente de todos los nodos que la conformaban, teniendo como aliada la poca tecnología desarrollada para redes en esa época?

Buscando cubrir esa requisición tecnológica, fueron presentadas cientos de alternativas para superar esta etapa, sin embargo, la solución que fue seleccionada, consistió en la propuesta que colocaba como primer punto de partida, identificar cual era la característica similar entre los equipos que conformarán la red. Está investigación se vio seriamente afectada en su desarrollo ante la serie de movilizaciones político, social y militar que sacudieron a los Estados Unidos durante la década de 1970 a 1980. La Guerra de Vietnam, Watergate, la Crisis del Petróleo y el asesinato de rehenes en Irán desviarón la atención y fondos autorizados del Congreso al Pentágono para el desarrollo de la investigación.

Estas situaciones permiten entender la falta de interés que obscureció la investigación y que opaco la aparición del protocolo TCP/IP (Transmition Protocol Common/Internet Protocol) obtenido en 1975 por la Advanced Research Projects Agency y que no fue aprobado hasta 1980 por la Defense Communications Agency como el protocolo estándar para la transmisión de archivos a través de ARPANET, y que se consolido como la parte integral de la red hasta 1983.

Hasta este punto, la red desarrollada era funcional para los propósitos planteados originalmente. Cabe señalar, que en estos años el proyecto ya no era considerado como un plan secreto del ejercito. Ya que a pesar de que solo algunos usuarios podían enlazarse a esta red, el tráfico fue incrementándose rápidamente entre los usuarios militares y la comunidad académica pertenecientes a las universidades involucradas en el proyecto.

Esta situación comenzó por disminuir el tiempo de respuesta en el acceso y uso de la red, ocasionando que su funcionalidad comenzará a decaer drásticamente. Este fenómeno obligo a realizar una segmentación de red* (como actualmente se conoce), está medida permito retomar la velocidad original a la red y estableció el criterio de privilegios en el acceso y uso de la red.

La segmentación que se realizó en esta fue de la siguiente forma.-

- **ARPANET**, este segmento se le designo a las universidades
- **MILNET**, este segmento perteneció solo para aplicaciones militares

Una de las características que debía contener la segmentación era la posibilidad de que ambas redes pudieran intercambiar la información sin problema alguno.

Más esta segmentación tuvo un arreglo secreto entre las agencias militares y las universidades. Este acuerdo consistía en que ARPANET solo sería para la investigación e intercambio de información entre universidades, y que en este

segmento se realizarían nuevos desarrollos que fortalecieran la estructura que conformaba el segmento de MILNET, por lo que estas soluciones no deberían ser aplicadas en ARPANET. Esto último ocasiono la desaparición gradual de este segmento y fortaleció el segmento dedicado a los militares.

Este acuerdo permitió conservar el segmento de que comprendía la parte original del proyecto, posteriormente con el cambio de gabinete MILNET cambio de nombre a DARPA, la cual se quedo bajo el control de la Defense Advanced Projects Agency. Este segmento de la red es conocido como el antecesor directo de lo que hoy se conoce como Internet.

A la par de la desaparición gradual de ARPANET y junto con las restricciones de acceso para usuarios ajenos a este proyecto, surgieron pequeños desarrollos de redes como BItnet (Because It's Time Network) y NSET (Complete Sciencie Network) que pretendía cubrir la demanda de intercambio de información entre usuarios conectadas a las mismas. Sin embargo, la estrategia para la sobrevivencia de estas nuevas redes no dependió de su crecimiento, sino de realizar la interconectividad en el flujo de información con ARPANET la cual tenia conexión directa con un segmento más robusto red (DARPA).

No fue hasta mediados de los años 80's, cuando finalmente ARPANET comenzó a declinarse para dar paso a una red más sólida conformada por DARPA, segmento de la red original que adquirió una fuerte estructura con las aplicaciones desarrolladas por ARPANET. En 1985, DARPA dejo de ser de parte de un proyecto militar y fue asumido nuevamente por las universidades, para las cuales no eran extrañas las aplicaciones desarrolladas por estos y donadas por tanto tiempo a los militares.

Durante 1985 la National Science Foundation (NSF) creó un desarrollo conocido como NSFNET. Este consistía en una serie de redes informáticas dedicas a la

difusión de los nuevos descubrimientos y la educación superior a distancia. Esta aportación se baso en las aplicaciones desarrolladas en ARPANET para MILNET.

La NSFNET estaba conformada por una estructura de red conectada a través de un "backbone" o "carrier" el cual era proporcionado por una compañía telefónica. Este enlace tenia la función de conectar a toda institución dentro de Estados Unidos dedicada a la investigación o educación.

Una de las características principales de esta estructura era la alta velocidad de transmisión con la que se realizaba el intercambio de información entre los puntos que conformaban los nodos de la red.

Inicialmente la transmisión de los datos se realizaba para redes de tamaño mediano, las cuales contaban con un ruteador*, el cual tenia como función, realizar el intercambio de datos entre los equipos conectados a la red. Con el empleo de estos sistemas de transmisión y ruteo surgió el concepto de supercarretera de la información. Este último comenzó a cobrar fuerza entre los usuarios solicitantes de información económica, legal, gubernamental e investigaciones realizadas en universidades.

Las altas velocidades de transmisión alcanzadas por NSFNET se lograban gracias al empleo de líneas de fibra óptica, sistemas de microondas y enlaces satelitales. La configuración original de estos medios consistía en la aplicación de líneas de transmisión de datos a velocidades de 56 kbps.

Esta velocidad se mantuvo como estándar hasta la aparición en 1989 de líneas de transmisión a 1.5 Mbps (conocidas como T1*). Y no es de extrañar que en el mundo de la ingeniería los avances no sean demasiados prolongados uno al otro, por lo que en 1992 el sistema de transmisión optimizó su velocidad con la aplicación de enlaces dedicados a velocidades a 45 Mbps (T3). Actualmente, estas líneas han crecido a velocidades de 2.0Gbps (E1) en su ancho de banda,

estas velocidades se han obtenido gracias al empleo de fibra óptica y la avanzada tecnología desarrollada en los servidores de comunicaciones en los extremos de los nodos.

La NSFNET baso su crecimiento gracias al interés del público, ya que representaba una potencial herramienta para la investigación e intercambio de información entre los usuarios, la que paralelamente se robustecía al incorporar nuevas y mejoradas aplicaciones de comunicaciones y redes en los equipos de computo obteniendo un mejor acceso al sistema de información.

De igual manera este crecimiento se apoyo mediante el interés e inversión monetaria de corporaciones privadas como Sprint y MCI, las cuales iniciaron la construcción de sus propias redes, que posteriormente enlazaron con la NSFNET. Estas inversiones tienen como objetivo principal, asumir el cargo de las operaciones de las mayores arterias de Internet, y obligar a la NSF dejar de brindar soporte directo a la estructura de la red.

Aún a pesar de las millonarias inversiones por parte de firmas comerciales, la NSFNET como red se ha expandido en universidades y centros de investigación en más de 80 países, conectando a 40 millones de computadoras por segundo, lo que da vida a la red de computo más grande del mundo, la red que emergió como resultado de la casualidad en el ingenio que distingue a la raza humana.

### 1.2- Una vez establecida la red, ¿De quién es Internet?

Algunos escritores sobre el genero han descrito en demasiadas ocasiones el nombre de Vint Cerf como el creador del concepto de Internet, y en alguno casos, este último ha sido nombrado como el "Padre de Internet". Sin embargo, la historia miente con respecto a este dato cronológico, ya que Vint Cert colaboró directamente con el grupo de investigadores el desarrollo del protocolo TCP/IP durante 1973. Aunque su investigación contribuyó a la obtención del protocolo, el

concepto de Internet ya era empleado entre la comunidad científica de esa época y al igual que ahora Internet carece de un dominio absoluto en una un grupo específico que asuma el control de la misma.

Al bifurcar la historia de Internet, se logra observar que el 90% de la estructura de la red se encuentra dentro de los Estados Unidos, por lo que en un principio la NSFNET coordinó en su totalidad todas las funciones de la misma. Posterior al establecimiento de la red, apareció la necesidad de regular y controlar la inserción de los servidores que se anexaban rápidamente a los beneficios que ofrecía la red, esto ocasiono que la NSFNET creará un servicio de registro conocido como InterNIC.

InterNic como servicio permite realizar el registro de cada una de las direcciones IP* y DNS* de los servidores que se inscriben a la red, teniendo como finalidad, permitir al usuario conocer la dirección exacta del servidor; es decir, describir el enmascaramiento de cada una de las direcciones homologadas y obtener la información en cada búsqueda que realice dentro de Internet.

Posteriormente y como consecuencia de la globalización del mercado mundial, los principales proveedores de líneas de transmisión iniciaron su guerra interna por asumir el control de la funciones de NSFNET, es por ello, que actualmente el control del servicio de InterNIC se encuentra a cargo de AT&T y Network Solutions, Inc. Es importante señalar, que estas compañías emplean las mismas soluciones desarrolladas por NSFNET para la realización del registro de direcciones, y lo único que la difiere de su antecesor es el cobro de inscripción por parte de estos Corporativos.

La segunda estructura desarrollada para una red global se encuentra en Canadá (CA*Net), la cual permite intercambiar información entre todos los institutos de investigación y universidades de todo ese país, esta red queda conectada al la red

global mediante una conexión entre la Universidad de Cornell en Pricenton Canadá a la Universidad de Washington en los Estados Unidos.

Otros de los países que cuentan con una mayor estructura de red que permite realizar la interconectividad entre con otras redes globales son, Japón, Francia, Alemania, Inglaterra y Australia. Actualmente en esto países operan más de 1000 redes, las cuales se conectan a la NSFNET a través de los enlaces entre universidades, centros de investigación e instituciones gubernamentales, manteniendo el concepto de Internet como la mejor herramienta con la que se cuenta actualmente para realizar la transmisión de información en cualquier punto hacia cualquier punto sin importar fronteras.

Durante 1997 el uso de Internet, ha registrado una demanda aproximada de 40 millones de usuarios por segundo alrededor del mundo, por lo que a finales del mismo en Estados Unidos se presento el proyecto de Internet2. Esta red sería un camino alterno que permitirá reducir y filtrar el tráfico de la red actual, por lo que se consideraba emplear para este proyecto la abandonada red ARPANET.

Para consolidar este proyecto a principios de 1998, IBM aporto la cantidad de 3.5 millones de dólares para la construcción de una nueva estructura red, la cual inicio con el equipamiento en hardware y software de siete universidades, entre las que destacan la de Chicago, Northwestern y la de Michigan en donde toda la comunidad de investigadores cuenta con el acceso ilimitado a Internet.

Este proyecto se encuentra orientado a incrementar la calidad de la educación superior y la colaboración entre las universidades en proyectos de educación a distancia, contando con una óptima velocidad que no se logra obtener dentro de la estructura de la actual Internet. Cabe señalar, que este punto fue parte esencial en discurso emitido el 13 de abril de este año por el Vicepresidente de Estados Unidos, el cual indico, "con la nueva velocidad de Internet2 sería posible la

transmisión de los 30 volúmenes de la Enciclopedia Británica en tan solo un segundo desde Chicago hasta los Angeles".

Cabe señalar, que Internet2 ha tenido un desarrollo visible y transparente para todos los usuarios de esta herramienta, lo cual difiere del desarrollo de la anterior red. Más la historia se repite cuando las compañías inversionistas y gobierno han indicado que Internet2 será solo para el uso exclusivo de una comunidad de investigación y negocios dentro de Estados Unidos.

Finalmente, a pesar de las grandes inversiones que se realicen por compañías de comunicaciones, computo y gobierno, no existe dueño absoluto de la red. Ya que el único valor visible de la red, no es el pago por el acceso del servicio, ni la velocidad de la red sino la información que se encuentra disponible en cualquier sitio y para cualquier usuario.

# Capitulo II

# Descripción del Protocolo TCP/IP

## Capitulo II

## Descripción del Protocolo TCP/IP

### 2.1- ¿Qué es TCP/IP?

TCP/IP (Transmission Control Protocol e Internet Protocol) es un conjunto de distintos protocolos, que realizan una serie procesos de compactación de paquetes, que permite garantizar la transmisión e integridad de la información que se encuentra viajando en una red LAN.

Las funciones principales del protocolo TCP/IP dentro de una red son:

- Permite la independencia de la tecnología usada en la conexión a bajo nivel y la arquitectura del ordenador
- Ofrece, contar con una conectividad universal a través de toda la red
- Reconocimientos de extremo a extremo
- Establece el uso de protocolos estandarizados

### 2.2- Estructura Interna del protocolo TCP/IP

La estructura de TCP/IP (Transmission Control Protocol e Internet Protocol) agrupa a docenas de distintos protocolos, que implementan funciones a todos los niveles de las capas OSI excepto en el nivel físico.

TCP/IP, del mismo modo que Internet, se encuentra basado en una arquitectura de capas, la cual permite que la implementación del conjunto de protocolos TCP/IP sea transparente y sencilla.

El modelo de capas de TCP/IP es algo diferente al propuesto por ISO (*International Standard Organization*) para la interconexión de sistemas abiertos (OSI), ambos modelos son descritos en las siguientes imágenes.

Figura 2.1- Relación del modelo TCP/IP basado en el modelo OSI

<table>
<tr><td>Aplicación<br>Presentación<br>Sesión</td><td colspan="2">TELNET</td><td>FTP</td><td>SNMP</td><td>SMTP</td><td>DNS</td><td>HTTP</td></tr>
<tr><td>Transporte</td><td colspan="7">TCP</td></tr>
<tr><td>Red</td><td colspan="7">IP</td></tr>
<tr><td rowspan="2">Liga de Datos</td><td colspan="6">802.2</td><td>X.25</td><td>LLC/SNAP</td></tr>
<tr><td>802.3</td><td colspan="3">802.5</td><td colspan="2">LAPB</td><td>ATM</td></tr>
<tr><td>Física</td><td>Ethernet</td><td colspan="2">Token Ring</td><td>FDDI</td><td colspan="2">Línea Síncrona WAN</td><td>SONET</td></tr>
</table>

Modelo de capas de TCP/IP

Figura 2.2- Modelo de capas del Protocolo TCP/IP




Para simplificar el uso del modelo TCP/IP, se ha determinado que la de red es conocida como capa de Internet y la capa de acceso a la red se le conoce como capa de enlace.

1. La relación existente entre el modelo de las capas de TCP/IP y las capas del modelo OSI se define de la siguiente manera:

2. La capa de aplicación de TCP/IP, corresponde a las capas de aplicación, presentación y sesión de las capas del modelo OSI.

3. La capa de transporte de TCP/IP corresponde a la capa de transporte del modelo OSI.

4. La capa red de TCP/IP corresponde a la capa de red y son intersectadas con la capa de enlace del modelo OSI.

5. La capa enlace de TCP/IP corresponde a las capas de enlaces y físicas del modelo OSI.

Para entender como son empleadas las capas en forma práctica, analicemos en siguiente caso.

Consideremos que algún usuario desea visitar la página principal de la dirección http://www.paraentender.com.mx , siendo esta insertada en el browser (este programa corre la capa de aplicación) que emplea el usuario en su máquina.

El browser realizará una petición a la capa de transporte para que este cree una conexión punto a punto (PPP) con el servidor de Web en la dirección http://www.paraentender.com.mx, en el que requerirá la página de inicio llamada index.html.

De igual manera similar, la capa de transporte utilizará los servicios de la capa de red, la cual es la encargada de recibir y enviar los paquetes de información durante este proceso. A su vez, la capa de red empleará los servicios que le brinda la capa de enlace, que se encargará de enviar a través de la red local o mediante un ruteador (en caso del que el usuario intente acceder a la red vía remota) la información de una computadora a otra.

Para obtener un resultado aceptable durante el proceso anterior, se requiere que cada capa realice su función de manera correcta. El no ser así nos llevará a obtener

una visualización defectuosa y en algunos casos el fracaso de nuestras solicitudes de información.

Para entender la importancia del trabajo en conjunto de las capas involucradas, a continuación se describen el funcionamiento y las características de cada una.

### 2.3- Capa de Aplicación

En esta capa, se encuentran las aplicaciones que se encuentran disponibles para el usuario. Debido a que, algunas aplicaciones son demasiado comunes entre sí, se tomo la decisión de estandarizarlas, ya que dentro de estas aplicaciones se encuentran:

- El acceso remoto (telnet y login)
- La transferencia de archivos vía (FTP)
- Correo electrónico (SMTP)
- WEB (http) entre otros.

#### 2.3.1- BOOTSP (Bootstrap Protocol)

El protocolo bootstrap, tiene la finalidad de proporcionar la dirección IP y la información sobre su sector de arranque a una máquina que es iniciada por vez primera. Este método tiene algunas ventajas respecto al uso del protocolo ____.

Para realizar su función, el protocolo BOOTSP, cuenta con un formato del mensaje, y se encuentra constituido de los siguientes campos:

- Type (Tipo): Este campo identifica si el mensaje es una solicitud o una respuesta

- Header (Cabecera): Este campo identifica el tipo de dirección de *hardware*

- H-Length (Longitud-H): Este campo identifica la longitud de la dirección de *hardware* en octetos

- Hop Count (Contador de saltos): Se emplea cuando el protocolo BOOTP es utilizado a través de varios Gateways. Cada paso por un *Gateways* aumenta en uno el contador.

- Transaction ID (ID de Transacción): Es empleado por la estación de trabajo para asignar las respuestas a las solicitudes

- Seconds (Segundos): Es utilizado para determinar el tiempo transcurrido desde el envió de la solicitud hasta la recepción de la respuesta.

- Client IP Address (Dirección IP del Cliente): Este campo deberá ser completado por el cliente, si conoce la dirección IP correspondiente. En caso contrario se pone a cero.

- Server IP Address (Dirección IP del Servidor): Puede ser introducido por el cliente, si la conoce la dirección IP del servidor. Sin embargo, cuando el valor es diferente de cero, solamente el servidor podrá contestar a la solicitud. De esta forma, el servidor se ve forzado a proporcionar la información de arranque.

- Gateway IP Address (Dirección IP de la puerta de enlace): Este campo deberá permanecer en cero en el cliente. Si la solicitud la obtiene un *Gateway*, este deberá escribir la dirección IP del mismo en este campo.

- Client Hardware Address (Dirección de *Hardware* del Cliente): Este campo deberá ser completado por el cliente

- Server Host Name (Nombre del Servidor *Host)*: Este campo es opcional, y puede ponerse en cero tanto para el servidor como para el cliente.

- Boot File Name (Nombre del Archivo de Arranque): Este campo puede ponerse a cero por el cliente, o poner un nombre genérico. El servidor reemplazara este campo por la ruta completa del archivo completo.

- Vendor Specific Area (Area del Fabricante): Contiene un código escrito por el cliente.

**Figura 3.1- Formato del mensaje BOOTP**

**Formato del mensaje BOOTP**

| *Octet +0* | *Octet +1* | *Octet +2* | *Octet +3* |
|---|---|---|---|
| 7 6 5 4 3 2 1 0 | 7 6 5 4 3 2 1 0 | 7 6 5 4 3 2 1 0 | 7 6 5 4 3 2 1 0 |
| *Type* | *Header Type* | *H-Length* | *Hop Count* |
| *Transaction ID* | | | |
| *Seconds* | | *Zero* | |
| *Client IP Address* | | | |
| *Response IP Address* | | | |
| *Server IP Address* | | | |
| *Gateways IP Address* | | | |
| *Client Hardware Address (16 Octets)* | | | |
| *Server Host Name (64 Octets)* | | | |
| *Boot File Name (128 Octets)* | | | |
| *Vendor-Specific Area (64 Octets)* | | | |

## 2.4- DNS (Domain Name Server)

El DNS (Servidor de Nombre de Dominio) es la traducción de una dirección IP a un nombre que se pueda recordar fácilmente. En Internet, normalmente cada computadora tiene una dirección IP que la distingue de manera única en la red

(excepto gateways y ruteadores que comúnmente cuentan con más de una dirección IP).

El Sistema de Nombres de Dominio (DNS –Domain Name System) es una base de datos distribuida cuyo protocolo indica cómo convertir números IP a nombres de dominio de computadoras en la red y viceversa.

El acceso a la base de datos DNS se hace a través de las funciones "gethostbyname" y "gethostbyadrr", las cuales obtienen el nombre de la computadora o el número IP, respectivamente. Las computadoras que responden a dichas requisiciones son llamadas servidores de nombres.

Es decir, los usuarios prefieren utilizar un nombre que sea sencillo de recordar que una dirección numérica. Para realizar esto, un servidor debe transformar la dirección IP en el nombre en la dirección del Host correcta. Anteriormente, sobre Internet se realizaba esta función, mediante el uso de una tabla única situada en un servidor central, el cual contenía todos los nombres de *Host de* unos cientos de servidores. Debido al gran aumento en el número de servidores, fue necesario descentralizar el servidor de nombres y dividirlo en múltiples DNS (servidores de nombres de dominio), los cuales están a cargo de los carriers.

Esto redujo considerablemente el tiempo de respuesta del servidor, y disminuyendo por consecuencia él trafico en la red.

La tarea de convertir el nombre de dominio a número IP, o viceversa, está a cargo de la capa de aplicación. El DNS tiene un esquema jerárquico donde cada hoja del mismo representa (en general) una computadora.

La estructura del sistema de dominios (DNS), es similar a la estructura que presentan los directorios del DOS o del UNIX. Es una estructura en forma de árbol, y cada uno de los archivos están identificados con una ruta de acceso. La única diferencia es

que en el DNS, la ruta empieza con el nombre del nodo en vez del directorio raíz. Y que, las rutas en un servidor DNS se escriben en sentido inverso a las del DOS.

La forma en que se ejecuta esta función es muy simple, ya que, el programa inicia proporcionando un nombre de dominio, y el DNS le regresa la dirección IP de este.

### 2.4.1- Nombres de Dominio

Se define como Nombre de Dominio, a la secuencia de etiquetas de los nodos (cada nodo del árbol tiene una etiqueta) necesarios para ir desde una hoja hasta el nodo raíz de la computadora que corresponde a dicha hoja. A cada sufijo de un nombre se le conoce también como un nombre de dominio. Esta secuencia, se visualiza como las palabras que son insertadas por el usuario, y que se encuentran listadas de izquierda a derecha, y la que representa la zona más cercana al usuario es la primera.

Los programas DNS manipulan el nombre del dominio proporcionado por el usuario de manera que sea fácilmente interpretado por otros programas. Para los programas, cada nombre de dominio contiene una secuencia de etiquetas, y cada etiqueta contiene un octeto de longitud seguido por una cadena de caracteres de un subconjunto de caracteres ASCII. Este subconjunto está formado por caracteres alfa (A-Z), dígitos (0-9) y un signo menos (-).

### 2.4.2- Arquitectura del DNS

El DNS es un protocolo que se localiza dentro de la capa de aplicación, y esta se encuentra clasificado como una gran utilidad por convenio entre los usuarios y el administrador del sistema, en vez de una parte integrada en los servicios de usuario.

**a) Elementos de programas de DNS**

De acuerdo al modelo Cliente/Servidor, el DNS consiste en un usuario, un cliente, un servidor de nombres local y un servidor de nombres remoto.

Dentro de los términos de las especificaciones, el DNS consiste en un programa de usuario, un cliente, un servidor de nombres, y un servidor de nombres remoto. Por lo que, cada *Host* debe implementar un mecanismo utilizando el cliente DNS para convertir los nombres del *Host* en direcciones IP.

**b) Elementos de Datos de DNS**

Los nodos DNS se representan por una etiqueta en el interior del nombre de dominio, y todos estos nodos cuentan con archivos de recursos (*resource records (RRs)*), los cuales, contienen información que habilita al programa DNS, con la finalidad de encontrar el nombre de dominio solicitado.

**Figura 4.1- Tipos de Resource Records**

| Tipos de *Resource Records* | | |
|---|---|---|
| **Valor** | **Codigo** | **Significado** |
| 1 | A | La direccion de un *Host* |
| 2 | NS | Un servidor de nombres autorizado |
| 5 | CNAME | El nombre canonico de un alias |
| 6 | SOA | Inicio de la zona de autoridad |
| 11 | WKS | Descripcion de un servicio conocido |
| 12 | PTR | Un puntero de nombre de dominio |
| 13 | HINFO | Información de un *Host* |
| 14 | MINFO | Información del Mailbox o de una lista de correo |
| 15 | MX | Intercambio de correo |
| 16 | TXT | Cadena de texto |
| 22 | NSAP | Cadena hacia un servicio de transporte OSI |
| 23 | NSAP-PTR | Puntero de nombre de dominio NSAP |
| 252 | AXFR | Solicitud de tranferencia de un a zona entera |
| 253 | MAILB | Solicitud de los archivos del Mailbox |
| 255 | | Solicitud de todos los archivos |

El formato en que se encuentra constituido de Resource Record, es la siguiente:

- Owner Name o SNAME (Nombre del propietario), es el nombre del nodo al cual pertenece el Resource Record. Este nombre será comparado con el nombre proporcionado por el programa del usuario. El nombre se encuentra en formato DNS, con unos octetos de longitud seguido por cadenas ASCII.
- Type (Tipo), es un entero de 16 bits que describe el tipo de Resource Record.
- Class (Clase), es un entero de 16 bits que define la clase del Resource Record. Por ejemplo, un Resorce Record de Internet tiene el campo igual a 1.
- Time to Live (Tiempo de vida), es un entero de 32 bits, que determina el intervalo de tiempo en el cual el RR debe ser almacenado en la memoria cache, antes de que sea actualizado con la información del origen. Si el valor fuera cero, el RR deberá ser utilizado solo en la transacción en progreso, y no será almacenado. De mismo modo, el valor a cero, es utilizado para datos muy volátiles.
- RDLength (Longitud RD), es un entero de 16 bits especifica la longitud en octetos del campo RDATA.
- Rdata, es una cadena de longitud variable de octetos que describen el recurso. El formato de esta información varia de acuerdo al tipo y clase del RR. Por ejemplo, para el tipo A RR (Internet), el campo RData contiene una dirección IP de 32 bits.

Es importante señalar, que otro elemento de datos del DNS, es el SLIST. El SLIST es una estructura que describe los servidores de nombres y la zona donde el cliente esta intentando enviar una solicitud actualmente.

**Figura 4.2- Formato de un Resource Record**

**Figura 2.**
**Formato de un *Resource Record***

| msb | | | | | | | lsb |
|---|---|---|---|---|---|---|---|
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| *Owner name* | | | | | | | |
| *Type* | | | | | | | |
| *Class* | | | | | | | |
| *Time to live* | | | | | | | |
| *RDLength* | | | | | | | |
| *Rdata* | | | | | | | |
| $2^7$ | $2^6$ | $2^5$ | $2^4$ | $2^3$ | $2^2$ | $2^1$ | $2^0$ |

### c) Funcionamiento del DNS

El funcionamiento del DNS puede describirse de la siguiente manera:

Un programa envía una solicitud a un cliente (*resolver*), la que contiene un nombre de dominio para el cual se requiere la dirección IP asociada. Esta solicitud, se realiza con una subrutina, o un puntero hacia el nombre de dominio que se encuentra en la pila del sistema. Los nombres de dominio en el cache del *Resolver* (cliente), se encuentran en un formato estándar contenido en Resource Record (RRs).

Una vez realizado esto, existen tres posibles respuestas de un *Resolver* al programa de usuario.

- Uno o más Resource Records (RRs) contienen la dirección IP solicitada. Para el caso de que, el nombre proporcionado fuera un alias, el *Resolver* devolverá simplemente el nombre de dominio al que hace referencia el alias.

- Envía un mensaje de error en el nombre, que significa que el nombre proporcionado no existe.
- Un error de datos no encontrados. Lo que significa, que el nombre proporcionado existe, pero no tiene referencia a ninguna dirección IP.

**d) Formato de un mensaje DNS**

El Protocolo DNS utiliza mensajes enviados por el UDP para trasladar solicitudes y respuestas entre servidores de nombres. La transferencia de zonas completas, es realizada a través del TCP

El formato de un mensaje DNS consta de cinco partes, que son:

1. Cabecera; define el formato de las otras partes
2. Pregunta; es el objetivo que debe resolver
3. Respuesta; es la resolución del objetivo
4. Autoridad; realiza la referencia a un servidor autorizado
5. Adicional; es información relacionada, pero que no es la respuesta.



**i) Formato de la cabecera**

La cabecera del DNS esta contenida por los siguientes campos:

**Figura 4.3- Formato de la cabecera DNS**

**Formato de la cabecera DNS**

| | *Octet +0* | | | | | | | | *Octet +1* | | | | | | | | *Octet +2* | | | | | | | | *Octet +3* | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| +0 | ID | | | | | | | | | | | | | | | | QR | Opcode | | | | A | T | RQ | RA | Z | | | Rcode | | | | |
| +4 | QDCOUNT | | | | | | | | | | | | | | | | ANCOUNT | | | | | | | | | | | | | | | | |
| +8 | NSCOUNT | | | | | | | | | | | | | | | | ARCOUNT | | | | | | | | | | | | | | | | |

Donde;

- ID es un campo de 16 bits que es utilizado para relacionar solicitudes y respuestas.
- QR es un campo de 1 bit , que identifica el mensaje como una solicitud como (0) o una respuesta como (1).
- OPcode es un campo de 4 bits, que describe el tipo de mensaje. (Ver Tabla 2)
- A es un campo de 1 bit, que cuando contiene como valor 1, indica que la respuesta la ha realizado un servidor autorizado
- T es un campo de 1 bit, que cuando asume el 1, indica que el mensaje ha sido truncado
- RQ es un campo de 1 bit, que cuando el valor es 1, indica que es una solicitud de un servicio recursivo por parte del servidor de nombres. Este servicio normalmente no esta disponible.
- RA es un campo de 1 bit , que señala la disponibilidad del servicio recursivo.
- Z es un campo de 3 bits reservado para un uso futuro, por lo que su valor debe ser 0.
- RCode es un campo de 4 bits, que es llenado el servidor de nombres, y sirve para indicar el estado de la búsqueda. (Ver Tabla 3)
- QDCount es un campo de 16 bits, que indica él número de entradas en la sección de Preguntas.
- ANCount es un campo de 16 bits, que señala él número de Resource Records en la sección de Respuesta.
- NSCount es un campo de 16 bits, el cual define él número de Resource Records en la sección de Autoridad.
- ARCount es un campo de 16 bits, que señala él número de Resource Records en la sección de Archivos Adicionales.

Figura 2.4- Código de operación/tipo de mensaje

| Código de Operación/Tipo de mensaje | |
|---|---|
| **Código** | **Descripción** |
| 0 | Solicitud normal (nombre a dirección) |
| 1 | Solicitud Inversa (dirección a nombre) |
| 2 | Solicitud del estado del servidor |

**Figura 2.5- Tabla de estado de la búsqueda**

| Estado de la búsqueda | |
|---|---|
| **Código** | **Descripción** |
| 0 | Sin errores |
| 1 | Error de Imposible para interpretar el formato de la búsqueda |
| 2 | Error de Imposible para procesar el servidor |
| 3 | Error de nombre inexistente |
| 4 | Tipo de búsqueda no soportado |
| 5 | Solicitud rechazada |

### ii) Formato de la sección Preguntas

Esta sección la construye el cliente, y siempre se encuentra presente. Contiene el nombre de dominio objetivo, seguido por los campos Qtype y Qclass. De igual forma, esta sección, es similar en longitud y formato que la definida para los campos CName, tipo y clase de un Resource Record.



### iii) Formato de la sección Respuesta

Esta sección esta constituida de uno o más Resource Records (RRs)

**iv)Formato de la sección Autoridad**

La sección de Autoridad contiene uno o más Resource Records (RRs), que apuntan hacia el origen de la información autorizada.

**v) Formato de la sección Adicional**

Esta sección esta contenida por uno o más Resorce Records (RRs), los cuales proporcionan las fuentes adicionales de la información.

## 2.5- Echo Protocol

La función principal del Echo Protocol, es la de escuchar las solicitudes de echo provenientes del cliente, para lo cual, utiliza el puerto de la UDP número 7. Sin embargo, el cliente utiliza un número de puerto UDP libre como puerto de origen, y envía un mensaje por medio del UDP al servidor echo. Una vez que el servidor echo recibe la solicitud, este intercambia las direcciones de origen, destino, las identificaciones de puertos, devolviendo el mensaje al cliente.

## 2.6- NTP (Network Time Protocol)

El protocolo NTP (Network Time Protocol), es empleado para sincronizar los servidores conectados con una precisión establecida en nanosegundos.

El formato del mensaje de NTP se encuentra constituido por los siguientes campos:

**Figura 2.6- Formato del NTP**

**Formato del NTP**

| | *Octet +0* | | | | | | | | *Octet +1* | | | | | | | | *Octet +2* | | | | | | | | *Octet +3* | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| +0 | LI | | VN | | 0 | 0 | 0 | | *Statum* | | | | | | | | *Poll* | | | | | | | | *Precision* | | | | | | | |
| +4 | *Synchronizing Distance* | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | |
|---|---|
| +8 | *Estimated Drift rate* |
| +12 | *Reference clock Identifier* |
| +16 | *Reference clock Timestamp* |
| +24 | *Originate Timestamp* |
| +32 | *Receive Timestamp* |
| +40 | *Transmit Timestamp* |

Donde;

- **Leap Indicator (LI) (Indicador de Ajuste):** Es un campo de 2 bits, que indica el ajuste generado por el periodo de rotación de la Tierra.

Figura 2.7- Tabla de indicador de ajuste

| **Indicador de Ajuste** | |
|---|---|
| **Valor** | **Significado** |
| 00 | Sin advertencias |
| 01 | -1 segundo |
| 10 | +1 segundo |
| 11 | Condición de alarma (Reloj no sincronizado) |

- **Versión Number (Número de Versión) (VN):** Es un campo de 3 bits, el cual, indica el número de la versión.
- **Reserved (Reservado):** Es un campo de 3 bits, en el que su valor es cero.
- **Stratum (Estrato):** Este campo tiene una longitud de 8 bits, y es utilizado para indicar el estrato local del reloj.

**Figura 2.8- Tabla de Stratum (estrat) del reloj local**

| **Estrato del reloj local** | |
|---|---|
| **Valor** | **Significado** |
| 0 | Sin especificar |
| 1 | Referencia primaria |
| 2..n | Referencia secundaria (vía NTP) |

- **Poll:** Este campo tiene una longitud de 8 bits. Indicando, el intervalo máximo de tiempo entre los mensajes.
- **Precision:** Este campo tiene una longitud de 8 bits, e indica la precisión del reloj local.
- **Sincronize Distance (Distancia de Sincronía):** Este es un campo de 32 bits, que indica el retraso aproximado de la primera ruta de sincronización.
- **Estimated Drift Rate (Nivel de Velocidad Aproximado):** Es un campo de 32 bits, que indica el nivel de velocidad del reloj local.
- **Reference Clock Identifier (Identificador del Reloj de Referencia):** Es un campo de 32 bits, el cual señala un reloj de referencia particular.

**Figura 2.9- Identificador de reloj de referencia**

| Identificador de reloj de referencia | | |
|---|---|---|
| **Valor** | **Codigo** | **Significado** |
| 0 | DCN | Determinado por el algoritmo DCN |
| 1 | WWVB | Radio Reloj WWVB (60 KHz) |
| 1 | GOES | Reloj de satelite GOES (450 MHz) |
| 1 | Radio Reloj WWV | WWV (5/10/15 MHz) |

- **Timestamps (Fecha y Hora) :** Existen 3 Timestamps de 64 bits cada uno.

## 2.7- SNMP (Simple Network Management Protocol)

La función del protocolo SNMP, es la de administrar múltiples redes físicas de diferentes fabricantes. Es decir, para Internet, en donde no existe un protocolo común en la capa de Enlace. La estructura del protocolo SNMP, se encuentra orientada a utilizar la capa de aplicación, evitando el contacto con la capa de enlace. El formato del mensaje del protocolo SNMP, se encuentra dividido en tres partes, que son:

- **Versión Number (Número de Versión):** El cual se utiliza para identificar el nivel de SNMP

- **Community String (Cadena de Comunidad):** Que es utilizada en la seguridad, restringiendo el acceso a los datos.
- **Protocol Data Units (PDU):** Esta parte contiene los comandos y respuestas, llamados PDU.

## 2.8.- ICMP (Internet Control Message Protocol)

La función del protocolo ICMP (Internet Control Message Protocol), es la de proporcionar, el medio para que el software de los hosts y gateways intermedios se comuniquen entre sí. El protocolo ICMP cuenta con un número de protocolo (numero 1), el cual lo habilita para utilizar el IP directamente. La implementación de ICMP es obligatoria como un subconjunto lógico del protocolo IP. Los mensajes de error de este protocolo los genera y procesa TCP/IP, y no el usuario. Esto se debe a que, Internet es un sistema autónomo que no dispone de ningún control central .

### a) Formato del mensaje ICMP

Cada Mensaje del protocolo ICMP, se encuentra compuesto por los siguientes campos:

- Tipo (Ver Tabla 7)
- Código
- Checksum
- Otras variables

**Figura 2.10- Tipos de mensaje ICMP**

| Tipos de mensaje ICMP | |
|---|---|
| Tipo | Tipo de Mensaje |
| 0 | Respuesta de Eco |
| 3 | Destino Inalcanzable |
| 4 | Origen saturado |
| 5 | Redirección (cambiar ruta) |

| | |
|---|---|
| 8 | Solicitud de eco |
| 11 | Tiempo excedido para un datagrama |
| 13 | Problema de parametros en un datagrama |
| 13 | Solicitud de fecha y hora |
| 14 | Respuesta de fecha y hora |
| 17 | Solicitud de nascara de direccion |
| 18 | Respuesta de mascara de direccion |

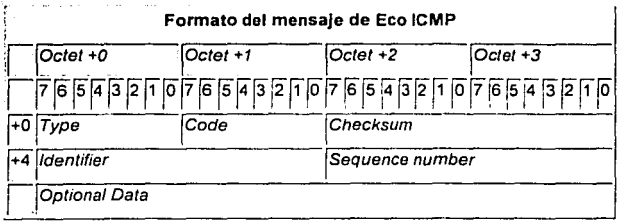
**b) Solicitud de Eco**

Para que un *Host* pueda comprobar si otro *Host* es operativo, debe mandar una solicitud de eco que le proporcione esta información. El receptor de esta solicitud, devuelve a su origen esta solicitud. Esta aplicación recibe el nombre de *Ping*.

Esta utilidad (Ping) encapsula la solicitud de eco del ICMP (tipo 8) en un datagrama IP y lo a través de una dirección IP.

El receptor de la solicitud de eco intercambia las direcciones del datagrama IP, cambia el código a 0 y lo devuelve al origen.

Figura 2.11- Formato del mensaje de Eco ICMP

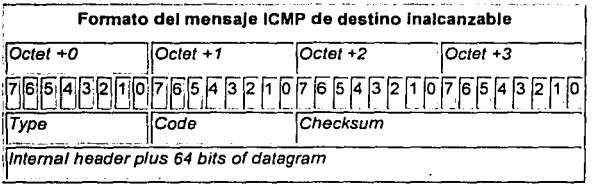


### c) Informes de Destinos Inalcanzables

Cuando un *Gateways* no puede enviar un datagrama a la dirección de destino, este mandara un mensaje de error ICMP al origen.

El formato de Destino Inalcanzable, se describe de la manera siguiente:

**Figura 2.12- Formato del mensaje de ICMP de destino inalcanzable**




El valor del campo tipo es 3, y el tipo de error se da de acuerdo al campo del código. Los códigos se encuentran descritos de la siguiente tabla:

**Figura 2.13- Descripción de mensaje de códigos inalcanzables**

**Tabla 8.**
**Códigos de Inalcanzable**

| Código | Descripción |
|---|---|
| 0 | Red no alcanzable |
| 1 | *Host* no alcanzable |
| 2 | Protocolo no alcanzable |
| 3 | Puerto no alcanzable |
| 4 | Necesaria fragmentacion con la opcion DF |
| 5 | Fallo de la ruta de origen |
| 6 | Red de Destino desconocida |
| 7 | *Host* de Destino desconocido |
| 8 | Fallo del *Host* de Origen |
| 9 | Red prohibida administrativamente |

| | |
|---|---|
| 10 | *Host* prohibido administrativamente |
| 11 | Tipo de servicio de Red no alcanzable |
| 12 | Tipo de servicio de *Host* no alcanzable |

**d) Control de Flujo**

El Control de flujo, se presenta cuando el buffer contenido dentro de los Gateways se haya saturado, por lo que, cada datagrama descartado, obliga al *Gateways* a que envié un mensaje ICMP de control de flujo al origen. Esto informa de que un mensaje ha sido descartado. Y en ese momento el *Gateways* descarta todos los mensajes que recibe, hasta que su nivel de *buffer* se convierte en aceptable para seguir operando.

Anteriormente, el mensaje ICMP de control de flujo se enviaba cuando el *buffer* estaba lleno, pero esta información llegaba demasiado tarde, y ya el sistema se encontraba saturado.

Esto motivo, a que el algoritmo fuera modificado, para que el mensaje ICMP de control de flujo se enviara cuando el *buffer* estuviera al 50% de su capacidad.

**e) Formato del Mensaje**

El formato del mensaje de control de flujo es idéntico al mensaje de inalcanzable, excepto que el tipo es 4 y el codigo es 0.

**f) Cambio de ruta (Redireccionamiento)**

El Cambio de ruta o (redireccionamiento), se presenta cuando la ruta por seleccionada por defecto no es la mas adecuada, por lo que, el *Gateways* envía un mensaje de redireccionamiento ICMP al *Host* indicándole que contiene la ruta

correcta. Esto se logra gracias a que los Gateways en cualquier Internet contienen las tablas de redireccionamiento más comunes.

**i) Formato del mensaje**

El formato del mensaje ICMP de control de flujo es similar al del mensaje de Inalcanzable, excepto que el tipo es 5 y el valor del código es variable entre 1 y 3. Las razones de la redirección y sus códigos son señaladas en la siguiente tabla.

**Figura 2.14- Tabla de códigos de redirección**

| Códigos de Redirección | |
|---|---|
| **Código** | **Razón para la redirección** |
| 1 | Por el *Host* |
| 2 | Por el tipo de servicio y red |
| 3 | Por el tipo de servicio y *Host* |

**g) Tiempo de Vida Excedido**

Para prevenir los bucles en la redirección, el datagrama IP contiene un tiempo de vida definido por el origen. A medida que cada *Gateway* procesa el datagrama, el valor del campo va disminuyendo en una unidad. Posteriormente el *Gateway,* verifica si el valor del campo es 0. Cuando este detecta un 0,, el *Gateway* manda un mensaje de error ICMP y descarta al datagrama.

**i) Formato del Mensaje**

El formato del mensaje de error es igual al del mensaje de inalcanzable, pero el tipo es 11, y el código es igual a 0 (contador sobrepasado), o 1 (tiempo de reensamblaje de fragmento excedido).

**h) Errores de Parámetros**

Los errores de parámetros se presentan cuando, el que origina el datagrama lo construye mal o el datagrama se encuentra dañado. Si un *Gateway,* encuentra un error en un datagrama, envía un mensaje ICMP de error de parámetros al origen y descarta el datagrama.

**i) Formato del mensaje**

El formato del mensaje ICMP de error de parámetros es igual al de inalcanzable, pero su tipo es 12, y el código es 0 si se utilizan punteros, o 1 si no son utilizados.

**i) Mensaje de Fecha y Hora del ICMP**

El Mensaje Fecha y hora del ICMP es una herramienta de gran utilidad para diagnosticar problemas, y recoger información acerca del rendimiento de Internet. El protocolo NTP (Network Time Protocol), puede utilizarse para marcar el tiempo inicial, y puede guardar una sincronización en milisegundos del reloj.

**ii) Formato del Mensaje**

El formato del mensaje se encuentra distribuido de acuerdo a la siguiente tabla.

**Figura 2.15- Formato de ICMP de fecha y hora**

| Formato ICMP de fecha y hora | | | |
|---|---|---|---|
| *Octet +0* | *Octet +1* | *Octet +2* | *Octet +3* |
| 7 6 5 4 3 2 1 0 | 7 6 5 4 3 2 1 0 | 7 6 5 4 3 2 1 0 | 7 6 5 4 3 2 1 0 |
| *Type* | *Code* | *Checksum* | |
| *Identifier* | | Sequence number | |
| *Originate Timestamp* | | | |
| *Receive Timestamp* | | | |
| *Transmit Timestamp* | | | |

El mensaje Fecha y hora contiene los siguientes campos:

- Tipo; que es igual 13 para el origen y 14 para el *Host* remoto.
- Código; que es igual a cero.
- Checksum
- Identificador; se usan para identificar la respuesta.
- Número de secuencia; se emplea para identificar la respuesta.
- Fecha y hora original; es el tiempo en el que el emisor inicia la transmisión.
- Fecha y hora receptor; es el tiempo inicial en el que el receptor recibe el mensaje.
- Fecha y hora de transmisión; es el tiempo en que el receptor inicia el retorno del mensaje.

**j) Mascara de Subred**

Cuando un *Host* quiere conocer la mascara de subred de una LAN física, puede mandar una solicitud ICMP de mascara de subred.

**i) Formato del Mensaje**

El formato es igual a los primeros ocho octetos del ICMP Fecha y hora. El valor del campo tipo es 17 para la solicitud de mascara de subred y 18 para la respuesta. El código es 0, y tanto el identificador como el número de secuencia se utilizan para identificar la respuesta.

**2.9- IGMP (Internet Group Management Protocol)**

La función de protocolo GMP (Internet Group Management Protocol), es la de operar, como una extensión del protocolo IP.

Este protocolo, es utilizado exclusivamente por los miembros de una red multicast, el cual les permite mantener su status de miembros, o para propagar la información del direccionamiento.

Es decir; un *Gateways* multicast manda mensajes una vez por minuto como máximo. El *Host* receptor responde con un mensaje IGMP, que señala al *Host* como miembro activo. Si un *Host* no responde al mensaje, este es señalado como inactivo en las tablas de direccionamiento de la red multicast.

## 2.10- Protocolos para actualizar la Tabla de Direccionamiento

Los siguientes protocolos que se describen a continuación, son utilizados para el proceso automático de actualización de la tabla de direccionamiento.

### a) EGP (Exterior *Gateways* Protocol)

Un dominio de direccionamiento es un grupo que se encuentra formado de redireccionadores que emplean un IGP (Internal *Gateways* Protocol) común entre sí. Una manera de reducir el volumen de información intercambiada se basa, en que un dominio de redireccionmiento utiliza un *Gateways* seleccionado para trasmitir la información de direccionamiento con los Gateways seleccionados de otros dominios. El *Gateway* que ha sido seleccionado, es considerado como un *Gateway* exterior, y el protocolo usado entre los Gateways exteriores es el EGP.

El protocolo EGP se compone de tres partes:

- *Neighbor Adquisition Protocol*
- *Neighbor Reachability Protocol (NR)*
- *Network Reachability Determination*

Donde;

El *Neighbor Adquisition Protocol,* es utilizado simplemente para establecer comunicación. Y se constituye solamente de una solicitud y una respuesta.

El *Neighbor Reachability Protocol* , se emplea para determinar si la comunicación es continua. Se encuentra constituido por un mensaje "Hello" (comando), y una respuesta "I heard you".

El mensaje *Network Reachability* se utiliza para comprobar si el siguiente "vecino" es un camino valido para llegar a un destino particular.

El único inconveniente del protocolo EGP, es que genera una estructura en forma de arbol; es decir, que si se presentan en Internet, los Gateways solo determinan que existen problemas en el *Gateways* exterior.

**b) BGP-3 (Border *Gateways* Protocol)**

El problema del protocolo EGP, fue el que impulso a diseñar e implementar el protocolo BGP.

El protocolo BGP es un protocolo interno del sistema autónomo. El sistema autónomo, contiene múltiples dominios de direccionamiento, cada uno, cuenta con su propio protocolo interno de sistema autónomo, o IGP.

Dentro de cada sistema autónomo, pueden existir Gateways que se pueden comunicarse con Gateways pertenecientes a otros sistemas. Asimismo, para obtener un informe de la información en que se realiza el direccionamiento, se logra con solo elegir un *Gateway* del sistema autónomo. En cualquier caso, un sistema autónomo, se presenta ante otro sistema autónomo como un direccionador consistente. Esto permite eliminar la estructura de árbol del protocolo EGP.

**c) GGP (*Gateways*-to-*Gateways* Protocol)**

Los primeros Gateways de Internet utilizaban un IGP llamado *Gateways*-to-*Gateways* Protocol , que fue el primer IGP utilizado. Empleando este protocolo, cada *Gateway* envía un mensaje a todos los otros Gateways de su grupo autónomo. Este mensaje, contiene una tabla con las direcciones que el *Gateways* ha direccionado, con su vector de distancia asociado.

**d) RIP (Routing Information Protocol)**

El protocolo RIP (Routing Information Protocol) es un IGP que fue desarrollado bastante despues del protocolo GGP. El protocolo RIP, se encuentra basado en el vector/distancia. Es decir, si un *Gateways* conoce varias rutas para llegar a un destino, asigna un coste a la ruta en función de los saltos de Gateways que deba realizar.

Entre mas Gateways tenga este que cruzar, mas saltos deberá realizar. Por lo que, cada 30 segundos, envía un mensaje que contiene su tabla de direccionamiento a los demás Gateways, que deberán actualizan sus tablas con los datos recibidos. El único inconveniente de este envío, es el incremento del trafico de red.

Sin embargo, este algoritmo presenta fallas, como por ejemplo, es incapaz de detecta bucles en la transmisión de la ruta. Esto genera un problema de consistencia cuando dos rutas que se llamen entre ellas estarían trasmitiéndose tablas de direccionamiento indefinidamente.

Otro error que presenta el algoritmo, es que no obliga a que se realice la autentificación de los intercambios, por lo que cualquier persona podría recibir información de las rutas enviadas por los Gateways.

Existen dos versiones RIP que son:

- RIP I
- RIP II

Ambas soportan mascaras de subred.

**e) Hello Protocol**

Un IGP similar al protocolo RIP es el Hello Protocol. La diferencia básica entre el protocolo RIP y el protocolo Hello es que, el protocolo RIP, realiza un conteo de los saltos de Gateways, mientras que el protocolo Hello mide la distancia por el tiempo transcurrido.

El protocolo Hello presenta un problema asociado al vector de distancia, el cual se presenta en dos etapas, que son:

1. La primera etapa, se presenta cuando los Gateways descubren una ruta más corta para llegar a un determinado destino. Como esta ruta es más corta y más rápida, ocasiona que el tráfico de red utilice esta nueva ruta.

2. La segunda etapa, esta empieza cuando los Gateways descubren que la nueva ruta es más lenta que la ruta anterior, ya que al desviar el tráfico de la red hacia la nueva ruta, esta es saturada, por lo que, todos los usuarios vuelven a la ruta anterior.

**f) OSPF (Open Shortest Path First)**

Uno de los protocolos IGP más nuevos es el OSPF (Open Shortest Path First). Este protocolo, cuenta con un mayor grado de sofisticación basado en las características de: Rutas basadas en el tipo de servicio, la distancia, nivel de carga, etc.

El formato del mensaje OSPF es más complejo que el RIP. Ya que, contiene una cabecera fija de 24 octetos, y una parte variable para especificar el tipo del mensaje. Existen cinco tipos de mensaje, como se puede ver en la siguiente tabla.

**Figura 2.16- Tabla de mensaje OSPF**

| Tipos de mensaje OSPF | |
|---|---|
| **Tipo** | **Significado** |
| 1 | Hola (Utilizado para comprobar la accesibilidad) |
| 2 | Descripción de la Base de Datos |
| 3 | Solicitud del estado del enlace |
| 4 | Actualización del estado del enlace |
| 5 | Reconocimiento del estado del enlace |

## 2.3- La Capa de Transporte

La función principal de esta capa es permitir la comunicación directa del remitente a los destinatarios. Esta consta de dos protocolos: TCP, cuya función principal es el permitir la comunicación libre de errores tipo orientada a la conexión; y UDP (User Datagram Protocol, Protocolo de Datagramas de Usuario), cuya función principal es permitir el uso directo de datagramas IP.

Es decir, provee la comunicación extremo a extremo desde un programa de aplicación a otro. Así como, proveer un medio transporte confiable, asegurándose de que los datos lleguen a su destino sin errores y en la secuencia correcta. Coordinando a múltiples aplicaciones que se encuentren interactuando con la red simultáneamente, de tal manera, que los datos que transmita una aplicación sean recibidos correctamente por la aplicación remota.

En esta capa se encuentran los protocolos UDP y TCP.

Las características principales de TCP son:

- El dividir la información que recibe de la capa de aplicación en segmentos que pasarán a la capa de red.
- Al enviar un segmento inicializa un reloj, en espera de una contraseña (indicando que el mensaje se recibió); si el reloj expira antes que esta última se reciba, reenvía el segmento –suponiendo que el segmento se ha perdido.
- Cuando el TCP recibe un mensaje, envía al remitente una contraseña confirmando la recepción.
- Implementa algoritmos para verificar que la información recibida fue la misma que la enviada; en caso de que el segmento llegue dañado a su destino, se indica al remitente del hecho y este último lo reenvía.
- Debido a que el IP no garantiza el orden de llegada de los segmentos que envía, TCP debe reordenarlos si es necesario.
- Implementa algoritmos de control de flujo
- Da la impresión a una aplicación de tener una línea directa en ambos sentidos (full duplex) a través de la cual se realiza la comunicación.

El protocolo TCP, otorga a la capa de aplicación una comunicación libre de errores punto a punto (de fuente a destino) que aparenta ser orientada a la conexión (aún cuando siempre se implemente mediante servicios no orientados a la conexión); a este enlace se le conoce como conexión TCP.

De igual manera, TCP define un nivel de direccionamiento, llamado puerto, que permite distinguir entre diferentes conexiones que se estén realizando simultáneamente. Cada puerto es identificado con un número de 16 bits. El empleo de este protocolo se observa en el modelo cliente-servidor.

Para que el cliente pueda conectarse con el servidor, es necesario que el primero sepa dónde encontrar al segundo; para resolver este problema, varios números de

puertos están reservados para algunas aplicaciones (correo electrónico, telnet, ftp, Web, etc.). Los números de puerto son asignados por IANA (Internet Assigned Number Authority, Autoridad Asignadora de Números en Internet). Esta agencia reserva números a los servicios que puede ofrecer un servidor.

Es decir, el número de puerto del servicio de FTP* es el 21, el de TELNET* es el 23, el del WEB* es el 80.

En general, los números de puertos entre el 1 y 255 los asigna la IANA. Un cliente de Web sabe que para conectarse con un servidor (también de Web), debe establecer una conexión TCP al puerto 80 de la máquina en cuestión.

### 2.3.1- UDP (User Datagram Protocol)

El protocolo UDP (User Datagram Protocol) tiene como función, proporcionar aplicaciones con un tipo de servicio de datagramas orientado a transacciones. El servicio proporcionado por el protocolo UDP, es similar al protocolo IP en el sentido de que no es fiable, y que no se encuentra orientado a la conexión.

El protocolo UDP es muy simple, eficiente e ideal para aplicaciones como el TFTP y el DNS. Debido a que una dirección IP sirve para dirigir el datagrama hacia un equipo en particular, y el número de puerto de destino en la cabecera UDP, es utilizado para dirigir el datagrama UDP hacia un proceso especifico localizado en la cabecera IP. La cabecera UDP, contiene además, un número de puerto origen, el cual le permite al proceso recibido conocer la forma de responder al datagrama.

Formato del mensaje del protocolo UDP puede apreciarse en la siguiente tabla.

**Figura 2.17- Tabla de formato del protocolo UDP**

**Formato del protocolo UDP**

| | *Octet +0* | | | | | | | | *Octet +1* | | | | | | | | *Octet +2* | | | | | | | | *Octet +3* | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

| | | |
|---|---|---|
| +0 | *Source Port* | *Destination Port* |
| +4 | *Message Length* | *Checksum* |
| | *UDP Data* | |

El datagrama UDP contiene cuatro campos, que son:

a) Número del Puerto de Origen
b) Número del Puerto de Destino
c) Longitud del mensaje
d) Checksum.

Donde ;

**Números de Puerto de Origen y Destino**

Los números de puerto de origen y destino, junto con las direcciones IP definen el punto final de la comunicación. El número del puerto de origen, puede contener valor cero si no es empleado. El número del puerto de destino, solo tiene sentido en el contexto de un datagrama UDP y una dirección IP en particular. Tanto el número de puerto de origen como el de destino, son un campos que contiene 16 bits de longitud.

**Longitud del Mensaje**

Este campo tiene una longitud de 16 bits y contiene el número total de octetos que forman el datagrama, incluida la cabecera.

**Checksum**

El uso del *checksum* es opcional, y este campo debe ponerse a cero si no es utilizado. Mientras que el *checksum* del datagrama IP solo tiene en cuenta la cabecera del mensaje, el UDP tiene su propio *checksum* para garantizar la integridad

de los datos. La longitud de este campo es de 16 bits, y esta formado por la suma de los campos del UDP, y algunos campos del IP.

Para incluir los campos del IP, se construye una pseudo cabecera UDP. Esta pseudo cabecera esta formada de 12 octetos, y se utiliza únicamente a efectos de calcular la suma.

**Figura 2.18- Tabla de Pseudo-Cabecera UDP**

| Pseudo-Cabecera UDP | | | |
|---|---|---|---|
| | Octet +0 | Octet +1 | Octet +2 | Octet +3 |
| | 7 6 5 4 3 2 1 0 | 7 6 5 4 3 2 1 0 | 7 6 5 4 3 2 1 0 | 7 6 5 4 3 2 1 0 |
| Pseudo Header | Source IP Adress | | | |
| | Destination IP Address | | | |
| | Zero | Protocol ID | Length | |
| | Source Port | | Destination Port | |
| | Message Length | | Checksum | |
| | UDP Data | | | |
| | UDP Data | Zero | | |

## 2.3.2- TCP (Transmision Control Protocol)

La función principal del protocolo TCP, es la de proporcionar un servicio de comunicación que forme un circuito; es decir, que el flujo de datos entre el origen y el destino sea continuo. Para ello, el protocolo TCP proporciona un circuito virtual el cual es llamado una conexión.

Al contrario que los programas que utilizan el protocolo UDP, los que utilizan el TCP cuentan con un servicio de conexión entre los programas que son llamados y los que llaman, chequeo de errores, control de flujo y capacidad de interrupción.

### 2.3.3- Interfaces TCP

Existen dos tipos de interfaces entre la conexión TCP y los otros programas que son:

La primera consiste en, utilizar la pila de los programas de la capa de red. Como en esta capa solo esta el protocolo IP, la interfase la determina este protocolo.

El segundo tipo es la interfaz del programa de usuario. Esta interfase varia según el sistema operativo, pero en generalmente tiene las siguientes características.

El interfase envuelve al programa del usuario llamando a una rutina, la cual agrega entradas a una estructura de datos llamada, Bloque de Control de Transmisión (TCB). Estas entradas se ejecutan inicialmente en la pila de *hardware* y son transferidas al TCB mediante una rutina del sistema. Estas entradas, permiten al TCP asociar a un usuario con una conexión particular, de modo que pueda aceptar comandos de un usuario y enviarlos a otro usuario en la otra parte de la conexión. El protocolo TCP utiliza unos identificadores únicos para cada parte de la conexión. Esto es utilizado para recordar la asociación entre dos usuarios. Al usuario se le asigna un nombre de conexión para utilizarlo en futuras entradas del TCB. Los identificadores para cada extremo de la conexión se conocen como sockets. El socket local, se construye concatenando la dirección IP de origen y el número del puerto de origen. El socket remoto se obtiene concatenando la dirección IP de destino y el número de puerto de destino.

El par de sockets de una conexión forman un único número en Internet. El protocolo UDP, cuenta con los mismos sockets, pero no los recuerda. Esta es una de las diferencias entre un protocolo orientado a conexión y no orientados a conexión.

A continuación se describen cuales son los comandos más:

- ***Open***: Inicia una conexión o comienza a escuchar un socket. El usuario tiene un nombre de conexión local, la que actúa como un puntero dentro del TCB.
- ***Send***: El comando *Send* manda datos del *buffer* especificado.
- ***Receive***: Es el mensaje de error que se envía, si el nombre local proporcionado no es utilizado antes con el comando *Open*.
- ***Close***: El comando *Close* cierra la conexión. Se produce un error si la conexión especificada no ha sido abierta, o si no se cuenta con la autorización para cerrar la conexión.
- ***Status***: El comando *Status* solo tiene una variable asociada, que es el nombre de la conexión.
- ***Abort***: El comando *Abort*, hace que todos los comandos Send y Receive asociados al nombre de la conexión local se interrumpan. La entrada del usuario del TCB se elimina y en enviado un mensaje especial de reinicio a la entidad del otro lado de la conexión.

El protocolo TCP, recuerda el estado de cada conexión mediante el uso del TCB. Ya que al abrir una conexión, se efectúa una entrada única en el TCB. Un nombre de conexión le es asignado al usuario para activar los comandos de la conexión. Y cuando es cerrada la conexión, se elimina su entrada del TCB.

### 2.3.4- Control de Flujo

El protocolo TCP, controla la cantidad de datos que debe enviar mediante el uso del campo *Window*. El campo Window, indica el número máximo de octetos que pueden ser recibidos. El receptor de un segmento con el campo *window* a cero, no puede enviar mensajes al emisor, excepto cuando sean mensajes de prueba. Un mensaje de prueba, es un mensaje de un solo octeto, que es utilizado para detectar redes o *hosts* inalcanzables.

El segmento TCP consiste en una cabecera y datos, como se aprecia en la siguiente tabla.

**Figura 2.19- Tabla de Formato del mensaje TCP**

| Formato del mensaje TCP | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Msb | | | | | | | lsb |
| | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| TCP Header | *Source Port* | | | | | | | |
| | *Destination Port* | | | | | | | |
| | *Sequence Number* | | | | | | | |
| | *Acknowledgement Number* | | | | | | | |
| | *Header Length* | | | | *Reserved* | | | |
| | *RSV* | | *Code Bits* | | | | | |
| | *Window* | | | | | | | |
| | *Checksum* | | | | | | | |
| | *Urgent Pointer* | | | | | | | |
| | *Options* | | | | | | | |
| | *Padding* | | | | | | | |
| | *TCP Data* | | | | | | | |
| | $2^7$ | $2^6$ | $2^5$ | $2^4$ | $2^3$ | $2^2$ | $2^1$ | $2^0$ |

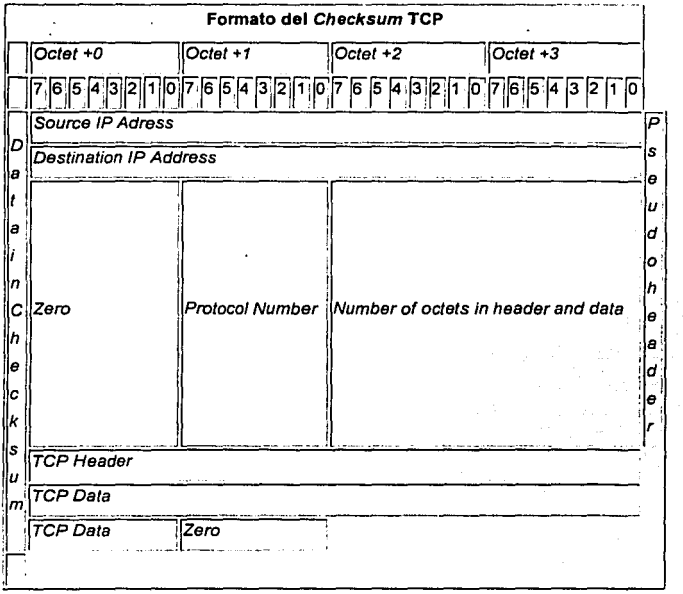
A continuación, se describen los campos del segmento TCP.

- ***Source/Destination Port Numbers*** **(Numero de puerto del Origen / Destino)**. Este campo contiene una longitud de 16 bits.
- ***Secuence Numbers*** **(Números de Secuencia):** Existen dos números de secuencia en la cabecera TCP. El primer número se conoce como es el número de secuencia final (*SSN*). Este es un numero de 32 bits. El segundo número de secuencia es el Numero de Secuencia Esperado de Recepción, o también llamado; Número de Reconocimiento (*acknowledgement number*).

- ***Header Length* (Longitud de la Cabecera): La** longitud de este campo es de 4 bits y contiene un entero que es igual al número de octetos que forman la cabecera TCP dividido por cuatro.
- ***Code Bits* (Código de Bits):**Este campo indica el motivo y contenido del segmento TCP. La longitud de este campo es de seis bits. Donde;
  - *Bit URG (bit +5):* Este bit identifica datos urgentes.
  - *Bit ACK (bit +4):* Cuando este bit se pone a 1, el campo reconocimiento es valido.
  - *Bit PSH (Bit +3):* Aunque el *buffer* no este lleno, el emisor puede forzar a enviarlo.
  - *Bit RST (Bit +2): Colocando* este bit, se aborta la conexión. Todos los buffers asociados se vacían.
  - *Bit SYN (Bit +1):* Este bit sirve para sincronizar los números de secuencia.
  - *Bit FIN (Bit +0):*Este bit seemplea solo cuando se esta cerrando la conexión.
- ***Window* (Ventana):** Este campo contiene un entero de 32 bits. Se emplea para indicar el tamaño de *buffer* disponible que tiene el emisor para recibir datos.
- **Opciones (*Options*):** Este campo permite que una aplicación negocie durante la configuración de la conexión características como, el tamaño máximo del segmento TCP. Si este campo tiene el primer octeto a cero, esto indica que no hay opciones.
- ***Padding* (Relleno):**Este campo consiste en un número de octetos (de uno a tres), que tienen valor cero, y sirven para que la longitud de la cabecera sea divisible por cuatro.
- ***Checksum*:** Mientras que el protocolo IP no tiene ningún mecanismo que garantice la integridad de los datos, ya que este solo comprueba la cabecera del mensaje. El protocolo TCP, dispone de su propio método que garantiza esta integridad.

Al igual que el *Checksum* del protocolo TCP, son incluidos campos del protocolo IP, es necesario construir una pseudo-cabecera TCP, la que se considera únicamente para efectos de calculo.

**Figura 2.20- Formato del Checksum TCP**




### 2.3.5- Estados del TCP

Para el inicio, mantenimiento y cierre de una conexión, se requiere que el TCP recuerde toda la información relativa de cada conexión. Esta información, es almacenada en una entrada para cada conexión dentro del TCB. Cuando se abre una conexión, la entrada en el TCB se ejecuta con todas las variables inicializadas con sus respectivos valores. Durante la conexión, la entrada del TCB es actualizada a medida que cambia la información.

A continuación se describen algunos de los estados del TCP:

- **0. CLOSED:** No existe, solo se usa como referencia.
- **1. LISTEN:** Indica que, se encuentra esperando solicitud de conexión de un TCP remoto.
- **2. SYN-SEN:** Indica que, se encuentra esperando un mensaje de solicitud de conexión después de haber enviado una solicitud de conexión.
- **3. SYN-RECEIVED:** Indica que, espera la confirmación de una solicitud de reconocimiento de conexión, después de que envió y recibió una solicitud de conexión.
- **4. ESTABLISHED:** Representa que la conexión se encuentra abierta. Los datos recibidos pueden ser enviados a un protocolo de una capa superior. Este, es el estado normal de la fase de transferencia de la conexión.
- **5. FIN-WAIT-1:** Señala que, se encuentra esperando la solicitud de fin de conexión de un TCP remoto, o un reconocimiento de una solicitud del fin de la transmisión enviada anteriormente.
- **6. FIN-WAIT-2:** Indica que, aguarda a una solicitud de fin de conexión de un TCP remoto.
- **7. CLOSE-WAIT:** Espera una solicitud de fin de conexión de un protocolo que pertenece a una capa superior.
- **8. CLOSING:** Espera la solicitud del final de la conexión de un TCP remoto.
- **9. LAST-ACK:** Este mensaje, indica que se encuentra, esperando el conocimiento de una solicitud de final de conexión enviada anteriormente al TCP remoto.
- **10. TIME-WAIT:** Este mensaje, señala que, se encuentra esperando el tiempo necesario para que el TCP remoto haya recibido el conocimiento de la solicitud del fin de conexión.

## 2.4- La Capa de Red

La función de la Capa de Red, es la de controlar la comunicación entre un equipo y otro. Conforma los paquetes IP que serán enviados por la capa inferior. Desencapsula los paquetes recibidos pasando a la capa superior la información dirigida a una aplicación.

Esta capa es el corazón de Internet. Ya que realiza la entrega de paquetes (llamados datagramas) de una computadora fuente a otra destino. De igual manera, implementa algoritmos para el ruteo, esto evita congestionamientos y realiza la interconexión de redes (gateways y ruteadores). Los servicios que esta capa provee no son orientados a la conexión (connectionless). Es importante señalar, que toda la información que se transmite a través de Internet es mediante datagramas IP. Esta capa no es confiable, es decir, no se encarga de verificar que un datagrama haya sido recibido o de volverlo a mandar en caso de existir algún error.

El protocolo central de esta capa es el IP y realiza las siguientes tareas:

- Esta capa recibe de la capa de transporte la información que se va a enviar a través de pequeños paquetes llamados segmentos, los cuales incluyen la dirección IP del destinatario.
- Realiza el encapsulamiento de dichos segmentos en datagramas.
- Determina cuál es la ruta que debe seguirse para entregar cada datagrama. El IP es sólo capaz de entregar paquetes a computadoras físicamente conectadas en la misma red local. Por lo que, si se desea enviar un datagrama a otra red, será necesario que el IP determine cuál es el ruteador o gateway al que deberá enviarle la información. Una vez determinada la dirección de la siguiente computadora a contactar, le entrega a la capa de enlace el datagrama el cual incluye la dirección IP del destino.
- Cuando la computadora recibe un data grama, verifica si está destinado para ella. Si es así, lo reconstruye en segmentos y lo pasa a la capa de transporte, Si no

está destinado para ella, realiza nuevamente la operación descrita en el punto anterior.

Otro protocolo importante de esta capa es el Protocolo de Mensajes de Control de Internet (ICMP –Internet Control Message Protocol) que se encarga de realizar las siguientes funciones:

- Control de flujo. Evita que una computadora envíe más datagramas de los que el receptor puede procesar.
- Detección de errores en las rutas que siguen los datagramas. Esto se debe, a que en ocasiones, algunas rutas no estarán disponibles, y si el IP desea comunicarse con una computadora para la que no haya ruta, ICMP se encarga de notificarle el error.
- Verificación de que una computadora esté conectada y su capa de red se encuentre funcionando correctamente.

### 2.4.1- IP (Internet Protocol) Versión 4

El Protocolo IP proporciona un sistema de distribución que es poco fiable incluso con una base sólida. El protocolo IP especifica que la unidad básica de transferencia de datos dentro del TCP/IP es el datagrama.

Los datagramas pueden ser retrasados, perdidos, duplicados, enviados en una secuencia incorrecta o fragmentados intencionadamente para permitir que un nodo con un *buffer* limitado pueda tomar todo el datagrama. La responsabilidad del protocolo IP, es la de reensamblar los fragmentos del datagrama en el orden correcto. En algunos casos de error, los datagramas son descartados sin mostrar ningún mensaje, mientras que en otras situaciones, son enviados mensajes de error a la maquina origen (esto lo realiza el protocolo ICMP). El protocolo IP define cual será la ruta inicial por la que enviara los datos.

Es normal, que cuando los datagramas viajan de unos equipos a otros, atraviesen diferentes tipos de redes. Por lo que, el tamaño máximo de estos paquetes de datos puede variar de una red a otra, dependiendo del medio físico que sea utilizado para su transmisión. A este tamaño máximo se le denomina MTU (*Maximum Transmission Unit*), y ninguna red puede transmitir un paquete de tamaño mayor a esta MTU.

El datagrama consiste en una cabecera y datos como se aprecia en la siguiente tabla.

**Figura 2.21- Formato del Datagrama IP**

**Formato del Datagrama IP**

| | Msb | | | | | | lsb | |
|---|---|---|---|---|---|---|---|---|
| | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | |
| IP Header | *Version* | | | | *Header Length* | | | | +0 |
| | *Type of Service* | | | | | | | | +1 |
| | *Total Length* | | | | | | | | +2 |
| | | | | | | | | | +3 |
| | *Identification* | | | | | | | | +4 |
| | | | | | | | | | +5 |
| | *Flags* | | | | *Fragment Offset* | | | | +6 |
| | | | | | | | | | +7 |
| | *Time to Live* | | | | | | | | +8 |
| | *Protocol* | | | | | | | | +9 |
| | *Header Checksum* | | | | | | | | +10 |
| | | | | | | | | | +11 |
| | *Source Address of Originating Host* | | | | | | | | +12 |
| | | | | | | | | | +13 |
| | | | | | | | | | +14 |
| | | | | | | | | | +15 |
| | *Destination Address of Target Host* | | | | | | | | +16 |
| | | | | | | | | | +17 |

| | | |
|---|---|---|
| | | +18 |
| | | +19 |
| | *Options* | +20 |
| | | +21 |
| | | +22 |
| | *Padding* | +23 |
| | *IP Data* | +0 |
| | | +1 |
| MSB | | +n |

Donde;

**a) Longitud de la Cabecera**

La longitud de este campo ocupa 4 bits, y representa el número de octetos de la cabecera dividido por cuatro, lo que ocasiona, que este sea el número de grupos de 4 octetos en la cabecera.

**b) Versión**

El campo Versión ocupa 4 bits. Este campo permite que diferentes versiones del protocolo IP puedan operar en la Internet. En este caso se trata de la versión 4.

**c) Tipo de servicio**

Este campo ocupa un octeto dentro de la cabecera IP, y especifica la precedencia y la prioridad del datagrama IP. Los tres primeros bits del octeto indican la precedencia. Los valores de la precedencia pueden ser de 0 a 7. Donde el 0 (cero) es la precedencia normal, y 7 esta reservado para control de red. Muchos Gateways ignoran este campo.

Los otros 4 bits definen el campo prioridad, que tiene un rango de 0 a 15. Las cuatro prioridades que están asignadas son: 0, (por defecto, servicio normal), 1 (minimizar el coste monetario), 2 (máxima fiabilidad), 4 (Maximizar la transferencia), 8 (El bit +4 igual a 1, define minimizar el retraso). Estos valores son utilizados por los routers para direccionar las solicitudes de los usuarios.

**d) Longitud Total**

Este campo es utilizado para identificar el número de octetos en el datagrama total.

**e) Identificación**

El valor del campo Identificación, consta de un numero secuencial asignado por el *Host* de origen. Este campo ocupa dos octetos. Los números oscilan entre 0 y 65.535, que al ser combinados con la dirección del *Host* forman un numero único en la Internet. Este número se usa para ayudar en el reensamblaje de los fragmentos de datagramas.

**f) Fragmentos Offset**

Cuando el tamaño de un datagrama excede el MTU, este es segmentado. El fragmento Offset representa el desplazamiento de este segmento desde en inicio del datagrama entero.

**g) Flags**

El campo flag se constituye de 3 bits y contiene dos flags. El bit +5 del campo flags, es utilizado para indicar el último datagrama fragmentado cuando toma valor cero. El bit +7, lo emplea el servidor de origen para evitar la fragmentación. Cuando este bit toma valor diferente de cero y la longitud de un datagrama excede el MTU, el

datagrama es descartado y es enviado un mensaje de error al *Host* de origen por medio del protocolo ICMP.

**h) Tiempo de Vida**

El campo tiempo de vida ocupa únicamente un octeto. Este campo, representa el número máximo de segundos que un datagrama puede existir en Internet, antes de que sea descartado. Un datagrama puede existir un máximo de 255 segundos. El número recomendado para IP es 64. El originador del datagrama manda un mensaje ICMP cuando el datagrama es descartado.

**i) Protocolo**

El campo protocolo, es utilizado para identificar la capa de mayor nivel más cercana usando el IP. Este es un campo de 0 bits, que normalmente identifica tanto en la capa TCP (valor 6), como en la capa UDP (valor 17) en el nivel de transporte, pero puede identificar hasta 255 protocolos de la capa de transporte.

**j) Checksum**

El Checksum proporciona la seguridad para que el datagrama no sea dañado ni modificado. Este campo tiene una longitud de 16 bits. El checksum incluye todos los campos de la cabecera IP, incluido el mismo, cuyo valor es cero a efectos de calculo. Si *Gateways* o nodo realiza alguna modificación en los campos de la cabecera (por ejemplo en el tiempo de vida), deberá recalcular el valor del Checksum antes de enviar el datagrama.

Los usuarios del IP deben proporcionar su propia integridad en los datos, ya que el Checksum es solo para la cabecera.

**k) Dirección de Origen**

Este campo contiene un identificador de red (Netid) y un identificador de *Host* (Hostid). Este campo tiene una longitud de 32 bits. La dirección de este puede ser de clase A, B, C. (ver Direcciones IP).

**l) Dirección de Destino**

Este campo contiene el Netid y el Hostid del destino. Este campo tiene una longitud de 32 bits. La dirección puede ser de clase A, B, C o D (ver Direcciones IP).

**m) Opciones**

Este campo se encuentra determinado por la longitud de la cabecera, ya que este campo es de longitud variable. Si esta es mayor de cinco, por lo menos deberá existir una opción.

Aunque un *Host* se encuentra obligado a ofrecer opciones, puede aceptar y procesar opciones recibidas en un datagrama. Cada octeto esta formado por los siguientes campos:

- Copia; la función de este campo se realiza cuando un datagrama va a ser fragmentado y viaja a través de nodos o Gateways. Cuando tiene valor 1, las opciones son las mismas para todos los fragmentos, pero si toma valor 0, las opciones son eliminadas.
- Clase de Opción; es un campo que al tener como valor 0, indica datagrama o control de red; Cuando tiene valor 2, indica depuración o medida. Los valores 1 y 3 están reservados para un uso futuro.
- Numero de Opción; este campo indica la realización de una acción especifica

**Figura 2.22- Tabla de Características de la opción IP**

| Caracteristicas de la Opción IP | | | |
|---|---|---|---|
| Clase de Opcion | Numero de Opcion | Octetos | Descripcion |
| 0 | 0 | 1 | Fin de alineamiento |
| 0 | 1 | 1 | Para alinear dentro de una lista de opciones |
| 0 | 2 | 11 | Seguridad (aplicaciones militares) |
| 0 | 3 | Var | Ruteo del Origen |
| 0 | 7 | Var | Grabar/trazar ruta |
| 0 | 9 | Var | Ruteo estricto del Origen |
| 2 | 4 | Var | Fecha y hora de Internet |

**n) Padding**

Este campo Pad, consiste en 1 a 3 octetos puestos a cero, si es necesario, para hacer que el número total de octetos en la cabecera sea divisible por cuatro.

**o) Datos**

El campo Datos consiste en una cadena de octetos. Cada octeto tiene un valor entre 0 y 255. El tamaño de la cadena puede tener un mínimo y un máximo, dependiendo del medio físico. El tamaño máximo esta definido por la longitud total del datagrama. Para determinar, el tamaño del campo Datos en octetos es igual a:

***(Longitud Total del Datagrama) - (Longitud de la cabecera)***

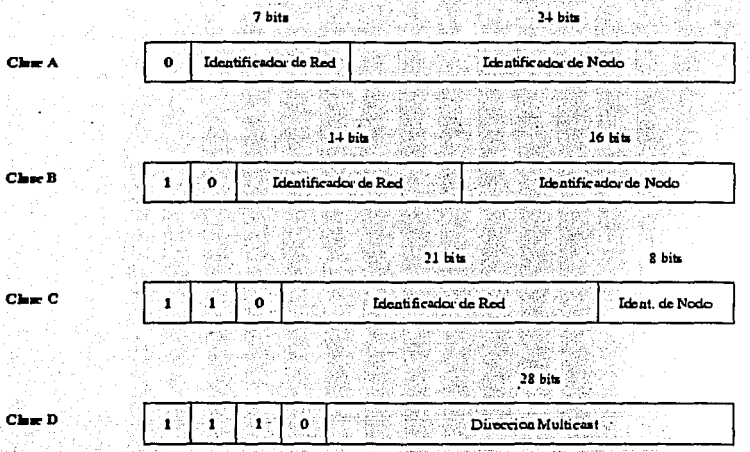
### 2.4.2- Direcciones IP de la Versión 4

Las direcciones IP permiten que realiza la transmisión de datos entre las máquinas de forma que sea eficaz, de manera al que se utilizan los números de teléfono.

Las direcciones IP constan de 32 bits, y se encuentran formadas por cuatro campos de 8 bits separados por puntos. Cada campo, puede tener un valor comprendido entre 0 y 255. Y se encuentra compuesta por una dirección de red, seguida de una dirección de subred y de una dirección de host.

Existen cinco clases de subredes, las que se muestran la Figura 2.23

Figura 2.23- Clases de Direcciones IP






Donde;

- La clase A contiene 7 bits para direcciones de red, por lo que permite tener hasta 128 redes, con 16.777.216 ordenadores cada una. Las direcciones estarán comprendidas entre 0.0.0.0. y 127.255.255.255, y la mascara de subred será 255.0.0.0.

- La clase B contiene 14 bits para direcciones de red y 16 bits para las direcciones del hosts. El número máximo de redes es 16.536 redes, con 65.536 ordenadores por red. Las direcciones estarán comprendidas entre 128.0.0.0. y 191.255.255.255, y la mascara de subred será 255.255.0.0.

- La clase C contiene 21 bits para direcciones de red y 8 para direcciones de hosts, lo que permite tener un total de 2.097.142 redes, cada una de ellas con 256 ordenadores. Las direcciones estarán comprendidas entre 192.0.0.0. y 223.255.255.255, y la mascara de subred será 255.255.255.0.

- La clase D se reserva todas las direcciones para multidestino (multicast); es decir, un ordenador transmite un mensaje a un grupo especifico de ordenadores de esta clase. Las direcciones estarán comprendidas entre 224.0.0.0. y 239.255.255.255.

- La clase E, se emplea exclusivamente para fines experimentales. Las direcciones se encuentran comprendidas entre 240.0.0.0. y 247.255.255.255.

### 2.4.3- IP (Internet Protocol) Versión 6

IP V6, es una nueva versión del protocolo IP, que también es conocida como IPng *(Internet Protocol Next Generation)* que equivale a la versión 6, debido a que la numero 5 no paso de la fase experimental. La compatibilidad con la versión IP4 es prácticamente total, ya que se han incluido características de compatibilidad. Algunas de las modificaciones, se encuentran encaminadas a optimizar la seguridad en la red, que apenas existía en la versión 4.

Esta cabecera ocupa el doble que la de la versión IP4. Sin embargo, ha sido simplificada, omitiendo algunos campos y haciendo que otros sean opcionales. De esta manera, los *routers* no tienen que procesar demasiada información.

**Figura 2.24- Formato de la cabecera de IP v6**

**Formato de la Cabecera del IPv6**

| *Octet +0* | | | | | | | | *Octet +1* | | | | | | | | *Octet +2* | | | | | | | | *Octet +3* | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| Versión | | | | | | | | Prioridad | | | | | | | | Etiqueta de flujo | | | | | | | | | | | | | | | |
| Longitud | | | | | | | | | | | | | | | | | | | | Siguiente cabecera | | | | | | | | Tiempo de vida | | | |
| Dirección de Origen (128 bits) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Dirección de Destino (128 bits) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Donde;

- Versión: Este campo ocupa 4 bits, y contiene el número de versión del IP, para este caso 6.
- Prioridad: Ocupa 4 bits, y indica la importancia del paquete que sé esta enviando.
- Etiqueta de Flujo: Ocupa 24 bits. Indica que el paquete requiere un tratamiento especial por parte de los *routers* que lo soporten.
- Longitud: Ocupa 16 bits. Indica la longitud en bytes de los datos del mensaje
- Siguiente Cabecera: Ocupa 8 bits e indica a que protocolo corresponde la cabecera que esta a continuación de la actual.
- Tiempo de vida: Ocupa 8 bits y tiene la misma función que el campo de la versión 4.
- Dirección de origen: Ocupa 128 bits (16 octetos), y es el número de dirección del origen.
- Dirección de Destino: Ocupa 128 bits (16 octetos). Es el número de dirección del destino.

### 2.4.4- Direcciones IP de la Versión 6

El cambio más significativo en las direcciones ha sido, que ahora, se hace referencia a una interfaz y no a un nodo, aunque como cada interfaz pertenece a un nodo, es posible referirse a estos mediante su interfaz.

Es importante señalar, que el número de direcciones diferentes se ha multiplicado de una manera exagerada. Ya que, teóricamente es posible contar con $2^{128}$ direcciones diferentes. Este número, indica, que se podrían llegar a tener mas de 665.000 trillones de direcciones por metro cuadrado, aunque de seguir una jerarquía, este número disminuirá hasta 1564 direcciones por metro cuadrado en el peor caso o tres trillones siendo optimistas.

En el IPv6 existen tres tipos de direcciones básicas que son:

- **Direcciones *Unicast***: Estas direcciones, se encuentran dirigidas a la única interfaz en la red. Actualmente se dividen en varios grupos, y existe un grupo especial que facilita la compatibilidad con las direcciones de la versión 4.
- **Direcciones *Anycast***: Estas direcciones, identifican a un conjunto de interfaces de red. El paquete será enviado a cualquier interfaz que forme parte del conjunto. En realidad son direcciones *unicast* que se encuentran asignadas a varias interfaces.
- **Direcciones *Multicast***: Estas direcciones, identifican a un conjunto de interfaces de la red, de manera que cada paquete es enviado a cada uno de ellos individualmente.

**2.5- La Capa Física**

Esta capa, corresponde al *hardware*. Y dentro de este nivel se encuentran los protocolos ARP y RARP.

La capa física o de enlace se encuentra implementada en el device driver, que se encuentra contenida en el sistema operativo y en la tarjeta de interfaz que conecta a la computadora con la red. Esta capa tiene a su cargo los detalles de la comunicación en la parte física (hardware) así como garantizar la confiabilidad de ésta. La capa de red le entrega a la capa de enlace paquetes de información llamados datagramas. Cada datagrama contiene el número IP (o dirección IP, el cual es un número de 32 bits) de su destinatario. Las principales funciones de la capa de enlace son:

- Realiza la conversión de los datagramas a tramas (frames). Es decir, las tarjetas de red requieren que la información que estas envíen esté encapsulada en forma de tramas.

- Convierte el número IP del destinatario en su dirección física. Cuando una computadora desea enviar una trama de una computadora a otra es necesario que conozca la dirección física de la computadora destinatario (cada tarjeta de red tiene una dirección única e irrepetible alrededor del mundo, está dirección se conoce como dirección física de la tarjeta); esto se debe a que a ese nivel, las direcciones IP no son significativas. La traducción del número IP a dirección física se realiza mediante el Protocolo de Resolución de Direcciones (ARP –Address Resolution Protocol). Mediante ARP se evita que las capas superiores requieran conocer direcciones físicas.

- Enviar la información a esta computadora, utilizando el protocolo que la red local especifique a los protocolos SLIP (Serial Line Internet Protocol, Protocolo Internet de Línea Serial), CSLIP (Compressed SLIP, SLIP Comprimido) o PPP (Point to Point Protocol, Protocolo de Punto a Punto) si se trata de una línea telefónica.

- Finalmente, realiza la conversión de regreso de las tramas recibidas en datagramas para entregarlas a la capa de enlace que se encuentra ubicada en el lado del receptor.

### 2.5.1- ARP (Address Resolution Protocol)

La función del protocolo ARP (Address Resolution Protocol), es la de convertir las direcciones IP en direcciones de la red física.

El funcionamiento del protocolo ARP es bastante simple y opera de la manera siguiente.

Cuando una máquina desea transmitir un mensaje a otra máquina que se encuentra conectada a través de una red (ethernet) se enfrenta al problema, de que, la dirección IP de la máquina en cuestión es diferente a la dirección física de la misma. La máquina que quiere enviar el mensaje sólo conoce la dirección IP del destino, por

lo que tendrá, que encontrar la forma de traducir la dirección IP a la dirección física. Esto se realiza mediante el uso del protocolo ARP.

Este protocolo, emplea una tabla denominada Tabla de Direcciones ARP, la cual, contiene la correspondencia entre direcciones IP y direcciones físicas utilizadas recientemente. Si la dirección solicitada se encuentra en esta tabla el proceso se termina en este punto, puesto que la máquina que origina el mensaje ya dispone de la dirección física de la máquina destino.

En el caso, de que la dirección buscada no se encuentre en la tabla el protocolo ARP, este envía un mensaje a toda la red. Ya que, cuando un ordenador reconoce su dirección IP envía un mensaje de respuesta que contiene la dirección física. Cuando la máquina origen recibe este mensaje ya puede establecer la comunicación con la máquina destino, y esta dirección física se guarda en la Tabla de direcciones ARP.

El mensaje ARP se encuentra formado por 28 octetos. En los campos que se describen a continuación se supone sobre una Interfaz Ethernet. Formato del mensaje ARP.

**Figura 2.25- Tabla de formato del ARP**

**Formato del ARP**

| | *Octet +0* | *Octet +1* | *Octet +2* | *Octet +3* |
|---|---|---|---|---|
| | 7 6 5 4 3 2 1 0 | 7 6 5 4 3 2 1 0 | 7 6 5 4 3 2 1 0 | 7 6 5 4 3 2 1 0 |
| +0 | *Hardware* | | *Protocol* | |
| +4 | *Length HW Addr* | *Protocol Length* | *Operation* | |
| +8 | *Source Hardware Address* | | | |
| +12 | *Source Hardware Address* | | *Source IP Address* | |
| +16 | *Source IP Address* | | *Destination Hardware Address* | |
| +20 | *Destination Hardware Address* | | | |
| +24 | *Destination IP Address* | | | |

**Donde;**

**a) Tipo de *Hardware***

El campo *Hardware* indica el tipo de la interfaz de *Hardware*. Por ejemplo, el valor de una red Ethernet es 1.

**Figura 2.26- Tipo de Interfaz de Hardware**

| Tipo de Interfaz de *Hardware* | |
|---|---|
| **Tipo** | **Descripcion** |
| 1 | Ethernet (10mb) |
| 2 | Experimental Ethernet (3 mb) |
| 3 | Amateur Radio X.25 |
| 4 | Proteon ProNET Token Ring |
| 5 | Chaos |
| 6 | IEEE 802 Network |
| 7 | ARCNET |
| 8 | Hyperchannel |
| 9 | Lanstar |
| 10 | Autonet Short Address |
| 11 | LocalTalk |
| 12 | LocalNet |

**b) Números de Protocolo**

El campo protocolo identifica el protocolo Ether usado. Por ejemplo el valor del interfaz Ethernet es 0800 hex.

**c) Longitud de la dirección *Hardware***

El valor para Ethernet es 6, lo que proporciona 48 bits para una dirección Ethernet (12 semi-octetos) .

**d) Longitud del Protocolo**

Este campo se usa para definir la longitud de la dirección de red. Para una red IP es 4.

**e) Operación**

Especifica el código de la operación. La solicitud ARP tiene valor 1, y la respuesta ARP tiene valor 2.

**f) Dirección *Hardware* del Origen**

Los campos Dirección *Hardware* del Origen, Dirección IP del Origen, y Dirección IP del Destino los completa el emisor (si los conoce). El receptor añade la Dirección *Hardware* del Destino y devuelve el mensaje al emisor con el código de operación 2. (El código de la Respuesta ARP).

La dirección *Hardware* de Origen (para Ethernet) esta formada por octetos que representan una dirección Ethernet de 48 bits, o un número.

**g) Dirección IP de Origen**

La dirección IP de Origen puede ser una dirección de clase A, B o C. (Ver Direcciones IP para obtener una definición de estas clases).

**h) Dirección *Hardware* de Destino**

Este campo esta formado igual que el campo Dirección *Hardware* de Origen.

**i) Dirección IP de Destino**

Este campo es igual que el campo Dirección IP de Origen

### 2.5.2- RARP (Reverse Address Resolution Protocol)

El protocolo RARP (Reverse Address Resolution Protocol) es el encargado de asignar una dirección IP a una dirección física.

#### a) Formato del Mensaje RARP

El formato del RARP es similar al del ARP. El valor del código de operación para una solicitud es 3, y el valor para una respuesta es 4.

# Capitulo III

# Función del protocolo H.323

## Capitulo III

## Función del protocolo H.323

### 3.1- ¿Qué es el protocolo H.323?

El protocolo H.323 fue establecido por la UIT (Unión Internacional de Telecomunicaciones) en 1996. El protocolo H.323. establece los estándares para la comunicación de voz y vídeo sobre redes de área local (LAN), sobre cualquier protocolo, que debido a su propia naturaleza presentan una gran latencia y no garantizan una determinada calidad del servicio (QoS) de transmisión.

Asimismo, este estándar, se apoya en la norma T.120, con lo que en conjunto de ambas soportan las aplicaciones multimedia. Las terminales y equipos que emplean a H.323 pueden transmitir voz en tiempo real, datos y vídeo, incluida videotelefonía.

Dentro de este estándar se contempla el control de la llamada, la gestión de la información y el ancho de banda empleado para una comunicación punto a punto y multipunto, dentro de la red LAN, asimismo, este define las interfaces entre la red LAN y otras redes externas, como puede ser la RDSI. Esta es, una parte de una serie de especificaciones necesarias para videoconferencia sobre distintos tipos de redes, que incluyen desde los estándares H.320 a la H.324, estos dos válidos para RDSI y RTC, respectivamente.

El protocolo H.323, fija cuales serán los estándares en que se realizará la compresión y descompresión de audio y vídeo, garantizando que equipos de distintos marca sean compatibles entre sí. Por lo que, los usuarios no se deberán preocupar, de que su equipo es de distinta marca con el que desean comunicarse. De igual manera, establece la administración del ancho de banda con el que cuenta dentro de la red, evitando con ello que la comunicación se colapse de

audio y vídeo. Por ejemplo, controla y limita el número de conexiones simultáneas del servicio, esto garantiza que se bloque el servicio una vez que sean superadas el número de conexiones establecidas.

Como estándar el H.323, emplea los procedimientos de señalización de los canales lógicos contenidos en la norma H.245, en los que el contenido de cada uno de los canales se define cuando se abre.

Estos procedimientos fijan el servicio que se determina del emisor y receptor, el establecimiento de la llamada, intercambio de información, terminación de la llamada y como se codifica y decodifica.

Es decir, cuando se solicita una llamada sobre la red, las dos terminales deberán establecer cual de ellos ejerce el control de la misma, de manera tal que sólo uno de ellos origine los mensajes especiales de control. Una parte importante de esto, es que se deben determinar la capacidad con que cuenta el sistema, de tal forma que no se permita la transmisión de datos si no pueden ser gestionados por el receptor.

Figura 3.1- Estructura del protocolo H.323

Una característica de la telefonía sobre una red LAN o sobre Internet es que se realiza la transmisión de información de vídeo sobre la de audio (videoconferencia), la que se comprime de acuerdo al estándar H.261 o H.263, formando parte de la carga que utiliza el paquete RTP; dado que solo envía los cambios entre cuadros, lo que resulta muy sensible a la pérdida de paquetes, originando la distorsión de la imagen recibida.

### 3.2- ¿Cómo funciona el protocolo H.323 ?

La función principal del protocolo H.323, es proporciona la base esencial en donde se realiza la transmisión de voz, datos y vídeo sobre una red LAN o Internet que no se encuentra orientada a conexión*, la cual no ofrece una calidad del servicio.

* En las redes no orientadas a conexión se realiza el llamado "mejor esfuerzo" para entregar los paquetes que son transmitidos, pero cada uno y en función del estado de los enlaces puede seguir una ruta distinta, por lo que el orden secuencial se puede ver alterado, lo que se traduce en una pérdida de calidad. Si contemplamos las redes IP, con TCP se garantiza la integridad de los datos y con UDP (datagrama) no. Por lo tanto, las redes que ofrezcan un alto grado de servicio y garanticen el ancho de banda necesario, se conocen como orientadas a la conexión; es decir, que se negocia y establece desde el inicio de la comunicación la ruta que han de seguir todos y cada uno de los paquetes y se reserva el ancho de banda que le ha sido determinado.

Esto se debe a que dentro de una red LAN, la transmisión de paquetes no se realiza en tiempo real, y que la transmisión de paquetes de datos, no se ve afectada por el retraso, desorden o pérdida, ya que estos se reconstruyen en el extremo lejano de la transmisión. Mientras que los servicios de transmisión de voz o video, son altamente sensibles a los retrasos en la entrega de los paquetes.

La topología de red que emplea el protocolo H.323, consiste desde un sencillo segmento o un anillo de red, o múltiples segmentos (es el caso de Internet) con una topología compleja, lo que da como resultado un grado variable de rendimiento.

Con el uso del protocolo H.323. hace posible que las aplicaciones y productos que conforman la red puedan interactuar entre sí, estableciendo la comunicación entre los usuarios, sin la necesidad de que éstos se preocupen por la compatibilidad entre sus equipos.

### 3.3- ¿Componentes que definen al estándar H.323?

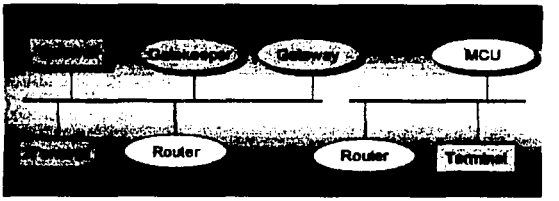
El estándar H.323 se encuentra constituido por cuatro componentes principales que le permiten establecer sistema de comunicaciones sobre la red, estos componente son los siguientes:

- Terminales
- Gateways
- Gatekeepers
- MCUs.

### 3.3.1- Terminales

Se definen como Terminales, a todos los clientes finales que se encuentran conectados en la red LAN, y que cuentan con una comunicación bidireccional en tiempo real. Todas estas terminales deberán soportar la comunicación de voz, ya que las transmisiones de vídeo y datos serán opcionales. Esto se muestra en el siguiente gráfico.

Figura 3.2- Zona de Control del protocolo H.323




Además, estas terminales deberán soportar la norma H.245, la cual se emplea para la negociación del uso del canal y sus prestaciones. Q.931 que establece de la llamada y la señalización. El protocolo RAS (Registration/ Admission/Status), que se utiliza para la comunicación con el Gatekeeper y sólo si éste está presente en la red; y deberá contar con el soporte para RTP/RTCP (Real-time Transport Protocol/Real-time Transport Control Protocol), que fija la secuencia de los paquetes de audio y vídeo. Como opción para la transmisión de video y conferencia de datos, las terminales pueden incorporar un codec, de acuerdo ala norma T.120 y MCU (Multipoint Control Unit).

Para realizar una conferencia y obtener la confirmación sobre si es posible hacerla, se utilizará otro protocolo del IETF, el RSVP (Resource Reservation Protocol) y aunque no es parte del H.323, se emplea para solicitar la reserva de un determinado ancho de banda y otros recursos, a lo largo de toda la red, esto es algo esencial si se quiere mantener una videoconferencia sobre una red LAN.

***RTP (Protocolo de transferencia en tiempo real)***

*El protocolo RTP(Protocolo de Transferencia en Tiempo Real), ha sido propuesto por el IETF, para facilitar y garantizar la confiabilidad de las comunicaciones multimedia (voz y video) dentro de una red LAN, Ya que a pesar de que el protocolo TCP/IP es utilizado en múltiples comunicaciones y que es un protocolo de transferencia seguro (gracias a que utiliza TCP), lo que asegura la transmisión*

*libre de errores, pero no garantiza que los paquetes lleguen ordenados a su destino en tiempo real, lo que causa problemas para la transmisión de voz o de vídeo.*

### 3.3.2- Gateway

El Gateway es un elemento opcional en una conferencia H.323, ya que proporciona muchos servicios dentro de la red incluida la adaptación con otras normas del UIT. En general, su misión principal es la de establecer la comunicación con otras terminales ubicados dentro de la RTB o RDSI.

### 3.3.3- Gatekeeper

La función del Gatekeeper es la de preservar la integridad de la red LAN. Esto lo realiza a través de las siguientes funciones:

Realiza la traslación direcciones de las terminales de la LAN, a las correspondientes IP o IPX, tal y como se describe en la especificación RAS.

Administra el ancho de banda proporcionado, fijando el número de conferencias que pueden estar realizándose simultáneamente en la red LAN y rechaza las nuevas peticiones que superen el nivel establecido. Con esto, se garantiza el ancho de banda para las aplicaciones de datos que corren sobre la red LAN.

El Gatekeeper proporciona todas las funciones anteriores para los terminales, Gateways y MCUs, que están registrados dentro de la denominada Zona de control H.323.

### 3.3.4- MCU (Multipoint Control Units)

La función de la MCU (Unidad de Control Multipunto), es la de permitir la conferencia entre tres o más puntos, bajo el estándar H.323. Su diseño le permite establecer la negociación y determinar las capacidades comunes entre las terminales dentro del proceso de audio y vídeo, así como controlar la multidifusión.

La comunicación bajo H.323 contempla la transmisión de las señales de audio y vídeo. La transmisión de cada una se realiza de la siguiente manera:

- La señal de audio es digitalizada y se comprime bajo uno de los algoritmos soportados, tales como el G.711 o G.723,

- La señal de vídeo (opcional en la comunicación) es manejada bajo la norma H.261 o H.263 respectivamente.

- Los datos (opcional) son manejados bajo el estándar T.120, el cual permite compartir las aplicaciones dentro de conferencias punto a punto y multipunto.

# Capitulo IV

# Descripción del MultiVOIP

## Capitulo IV

## Descripción del MultiVOIP

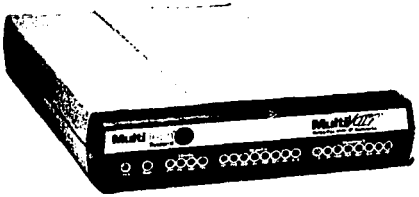


### 4.1- ¿Qué es un MultivOIP?

El MultiVOIP es un equipo, que permite la comunicación analógica de voz y fax sobre redes IP ya sean Punto a Punto o sobre Internet. Este equipo, hace posible la transmisión de voz y fax, reduciendo de forma considerable los gastos generados por el uso de telefonía de Larga Distancia entre los headquarters y oficinas regionales. El MultiVOIP puede ser conectado directamente a sistemas telefónicos locales y Centrales Telefónicas (PBX)

La operación del MultiVOIP, no requiere nada más que la conexión a la red IP existente. A pesar de que, esta red tradicionalmente es utilizada sólo para datos, la implementación del MultiVOIP no requere de ningún equipo adicional para su conexión y operación.

Figura 4.1- Imagen MultiVOIP de Multitech LTD



Es importante señalar, que la topología de red entre los headquarters y las oficinas regionales, no tienen que ser un enlace Punto a Punto necesariamente. Sin embargo, es necesario que para la configuración del MultiVOIP, las redes cuenten con un servicio de enlace de transmisión de datos con salida a Internet. Este servicio es proporcionado por un Proveedor del Servicio de Internet (ISP), a través de la instalación de una línea dedicada, cable MODEM, HDSL, etc.

Lo anterior es necesario, ya que el MultiVOIP, opera como un gateway, el cual incorpora el servicio de voz o fax dentro del tráfico de datos dentro de una red IP.

Para su operación, este equipo emplea dos canales independientes para voz y fax (con tres interfaces de voz y fax cada uno), una interfaz de LAN Ethernet de 10 Mbps y un puerto de comandos para la configuración. Donde, los canales de voz y fax son separados por el gateway y enviados a los teléfonos respectivamente.

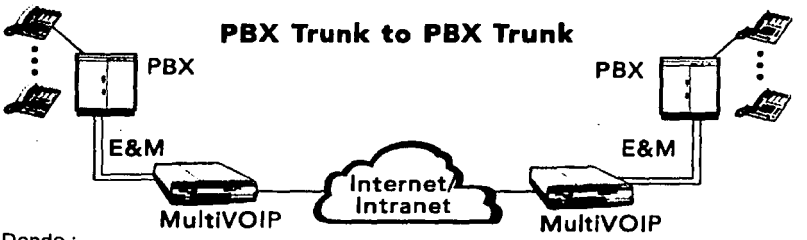
### 4.2- ¿Cómo funciona el MultiVOIP?

En funcionamiento principal del VOIP, consiste en establecer la transmisión de voz entre dos o más localidades remotas. Mediante la atención a las solicitudes de comunicación, generadas de las extensiones telefónicas pertenecientes a las centrales telefónicas de ambas redes. Este proceso, es realizado por el MultiVOIP, mediante la conversión del número de extensión telefónica solicitada a una dirección IP.

Una vez realizada esta conversión, es comprimida la señal de la voz para ser enviada a través de la red de datos. Es decir; la conversión de la señal análoga de voz y fax es convertida para su envío en un paquete de datos.

El MultivOIP permite la transmisión de voz y fax entre ambas redes utilizando la misma ruta que las comunicaciones tradicionales de datos. Este proceso puede visualizarse de la siguiente manera:

Figura 4.2- Conexión de MultiVOIP para conexión remota de centrales




Donde ;

Donde;

1- Se realiza la solicitud al MultiVOIP para la transmisión de voz o fax, a través de los equipos telefónicos conectados a la central telefónica.

2- El MultiVoip, inicia la compresión de la voz o fax en paquetes de datos

3- Una vez concluida la compresión, el MultiVoip establece la conexión con el gateway remoto utilizando la red externa (Punto a Punto o Internet). Esta conexión, la realiza mediante las tablas de gateway remotos configurada previamente.

4- El MultiVOIP remoto (esclavo) recibe la solicitud y la procesa mediante la descompresión de los paquetes de voz o fax enviados.*

* Para ambos casos (Voz y fax) las solicitudes remotas de comunicación pueden ser procesadas por las centrales telefónicas. Esta puede proveer una mayor cantidad de servicios (solicitudes de discado a números telefónicos fuera de las oficinas, celulares, fax, etc) o realizar las conexiones directas hacia los destinos solicitados.

### 4.3- Ventajas del uso del MultiVOIP

Las ventas principales del MultiVOIP en su instalación, operación y mantenimiento son:

**a) Instalación**

- Se instala sobre la red de datos existente sin realizar cambio alguno en esta
- Puede emplear cualquier tipo de enlace o conexión a Internet existente
- Emplea el sistema telefónico existente y no requiere modificación en la central telefónica. En algunos casos de centrales PBX digitales 100%, se requiere un convertidor Digital / analógico para la conexión.
- Genera un impacto mínimo sobre la red de datos y voz
- Permite utilizar al PSTN como backup

**b) Operación**

- Puede optimizar el uso del ancho de banda
- No se requiere de la operación de una computadora (PC)
- No depende del proveedor de Internet
- Utiliza el protocolo H.323
- Emplea las compresiones G.729, G.723
- Realiza la supresión de silencios
- Realiza un servicio diferencial
- Cancela los ecos
- Realiza la corrección de errores
- Ejecuta Interpolación de malos cuadros así como de Jitter buffers dinámicos

**c) Administración**

- Se realiza utilizando Windows 95/98/2000/NT
- Para administración remota, se emplea un web browser, telnet, FTP, etc

### 4.4- ¿Cuáles son las características del MultiVOIP?

De acuerdo a las necesidades de la implementación y del tráfico de llamadas, el MultiVOIP puede contar con 1, 2, 4, 8, 24 o 30 puertos.

Y los requerimientos físicos para su conexión en la red son:

- Ethernet LAN (IP Network)
- Deberá contar por lo menos con 14K de ancho de banda por cada canal de voz
- Tener asignada una dirección IP fija, rotativa u homologada

Su conexión a la red no requiere de ningún hardware adicional.

### 4.5- Descripción de Centrales telefónicas 3Com NBX 100

Actualmente, las centrales telefónicas o conmutadores, se han convertido en la pieza esencial de las empresas o instituciones que requieren de un consumo telefónico distinto al de un usuario residencial.

Recordemos que el modelo actual de telefonía indica que para cada llamada se realiza desde un lado a otro utilizando una sola línea durante el proceso ( ya sea de un servicio estándar análogo).

De acuerdo a este modelo, las empresas deberían contar con el mismo número de líneas por cada usuario que desee llamar a otro punto, incluso estando dentro de la misma oficina. Esto ocasiona, que los servicios brindados por las empresas, compañías, instituciones, etc. se vean afectados ante la poca agilidad de los servicios telefónicos, aumentando el costo de operación ante la contratación de un sin número de líneas necesarias para brindar el servicio.

Para el desarrollo de este trabajo, la central telefónica que se empleara es 3 Com modelo NBX100. Este sistema NBX 100 de 3Com proporciona los siguientes servicios:

- Conferencias
- Correo de voz
- Identificación de llamadas entrantes
- Reenvío de llamadas y marcación rápida
- Teléfonos virtuales PcXset
- CTI y mensajería unificada.



La ventaja fundamental de la central 3Com NBX100, es que opera directamente utilizando el cableado de una red de datos categoría 5. Ello evita, la instalación de un nuevo cableado para telefonía. Esta ventaja se basa, en que la central telefónica NBX 100 cuenta con una arquitectura Ethernet. Esta arquitectura, le permite desplegar mas y nuevos servicios como aplicaciones dentro de la infraestructura de comunicaciones ya existente.

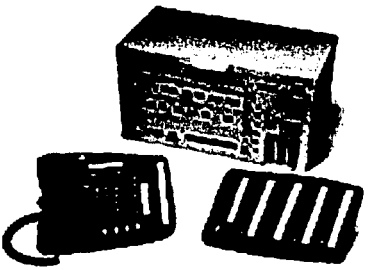


Figura 4.3- Central Telefónica 3Com modelo NBX 100

Otras ventajas del uso de esta central se hacen presentes en los bajos costos de inversión que se requieren para su instalación y administración, en comparación con los mismos generados del uso de una central de la telefonía convencional.

El sistema NBX 100 de 3Com es la mejor solución de comunicaciones para ser instaladas headquarters, empresas medianas y sucursales. Ya que cuenta, con una capacidad de gestión de las llamadas manteniendo en todo momento una calidad en la voz fiable. Esta calidad aumenta considerablemente la productividad de las redes de área local (LAN) y las de área extensa (WAN) con la calidad de servicio (QoS) de un extremo a otro de la red. Permitiendo generar servicios de líneas privadas de conexión entre las distintas localidad, mediante el re-encaminamiento de las llamadas de teléfono internas de la empresa a través de la WAN.

Cabe señalar, que la central NBX 100 de 3Com puede aprovechar nativamente los servicios de voz sobre IP mediante el empleo del protocolo H.323. Para lograr esto, es necesario agregar y adecuar equipos NBX ConneXions H.323 a la estructura de red local.

Este equipo, permite conectar oficinas principales con las sucursales de una empresa. Esta conexión permite emplear cualquier plataforma de la red WAN, incluidos RDSI, ATM, Frame Relay, xDSL y los módem de cable e incluso sobre redes Ethernet inalámbricas.

El equipo NBX ConneXions H.323, cumple la función de ser un Gatekeeper. El cual preserva la integridad de la red LAN. Administrando el ancho de banda proporcionado a los equipos, fijando a su vez el número de conferencias que pueden estar realizándose simultáneamente en la red LAN y rechaza las nuevas peticiones que superen el nivel de demanda establecido. Con esta restricción, se garantiza el ancho de banda para las aplicaciones de datos que corren sobre la red LAN.

Sin embargo, la desventaja de esta unificación, es la inversión que representa la adquisición de estos equipos.

La compra de cada equipo NBX ConneXions H.323 equivalen en promedio al costo generado en la adquisición de cinco Centrales 3Com NBX 100, incluidos quince teléfonos de escritorio y una licencia de diez teléfonos virtuales PcXset respectivamente.

Debido a que la limitante es financiera antes que tecnológica, la implementación del servicio de voz sobre IP utilizando las propiedades nativas de la central 3 Com NBX 100, no representa ser una solución viable y de bajo costo para enfrentar este problema.

# Capitulo V

# Conexión de las centrales telefónicas con VOIP

# Capitulo V
# Conexión de las centrales telefónicas con VOIP

## 5.1- Configuración del MultiVOIP

Para iniciar con la implementación del MultiVOIP, se debe considerar que para realizar una instalación sencilla o típica se requiere de dos o más MultiVOIP que se encontraran ubicados en las localidades en donde se realizara la comunicación.

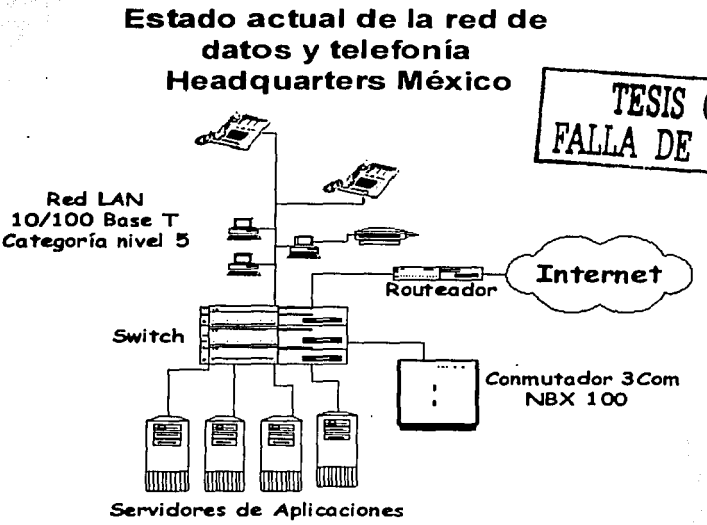
Por lo que, en cada localidad se tendrá que conectar el MultiVOIP a la red de cada una de estas. Una vez conectado, a cada MultiVOIP se le asignara una dirección IP estática (la que tendrá que ser accesible desde Internet) y se deberá crear el directorio telefónico para la comunicación entre los MultiVOIP.

Para cada implementación, es indispensable configurar un MultiVOIP como un equipo "maestro", en el cual se creará el directorio telefónico. Cualquier otro MultiVOIP instalado e la implementación, operará como "esclavo", y estos tendrán que descargan el directorio telefónico que se ha creado previamente en el MultiVOIP "maestro".

Es decir, si los teléfonos analógicos se encuentran conectados directamente a canales de voz y fax, el usuario simplemente tendrá que descolgar el teléfono y marcar la extensión de otro MultiVOIP (la cual, ha sido registrada previamente en el directorio del equipo "maestro"), el teléfono del MultiVOIP remoto sonará y podrá iniciarse la conversación.

Esto se debe a que, cada marcación de número de teléfono corresponderá a la dirección IP de MultiVOIP y a un número de canal de voz y fax que han sido asociados. Si posteriormente se desea agregar algún equipo adicional a la red, tan sólo se deberá actualizar el directorio telefónico del MultVOIP "maestro".

El estado actual de las redes antes de la implementación se muestra a continuación.





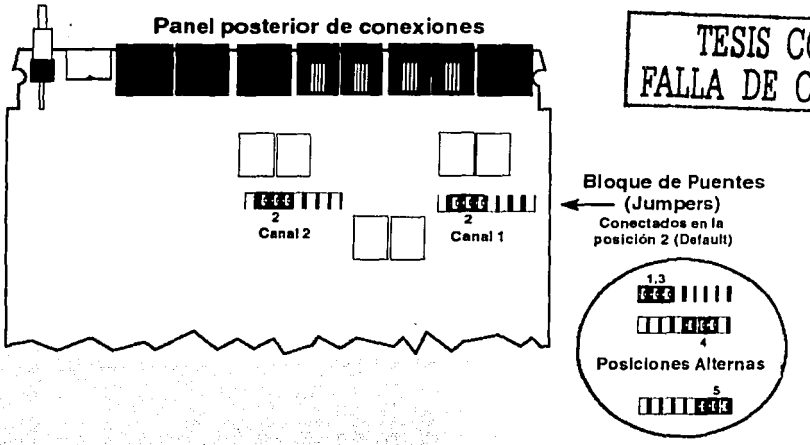

### 5.1.1- Configuración del bloque de puentes de E&M

El inicio de la instalación de los equipos MultiVOIP, comienza con la configuración del bloque de puentes para avanzar hacia la instalación de los cables para las conexiones correctas con la corriente eléctrica, puerto de comandos, sistema telefónico e Internet.

Cada canal de voz y fax del MultiVOIP contiene un bloque de puentes (jumpers) E&M individuales. Estos se encuentran colocados próximos a los conectores del panel posterior del MultiVOIP. Estos bloques se encuentran constituidos de ocho pares de patillas con un conector de puente sobre tres pares de patillas adyacentes.

El conector del puente deberá estar centrado en el número que indica el tipo de E&M correspondiente a la conexión E&M para ese canal.

**Figura 5.1- Configuración de puentes internos del MultiVOIP**






Si se requiere cambiar la posición predeterminada (tipo 2) del bloque de puentes de E&M, deberá realizarse el siguiente procedimiento.

1.- Desconectar el suministro de corriente eléctrica hacia el MultiVOIP.
2.- Desmontar el tornillo de situado en la parte posterior central del.
3.- Colocar el MultiVOIP con el lado derecho hacia arriba y, a continuación, deslice la base en la parte posterior de la caja para quitarla.

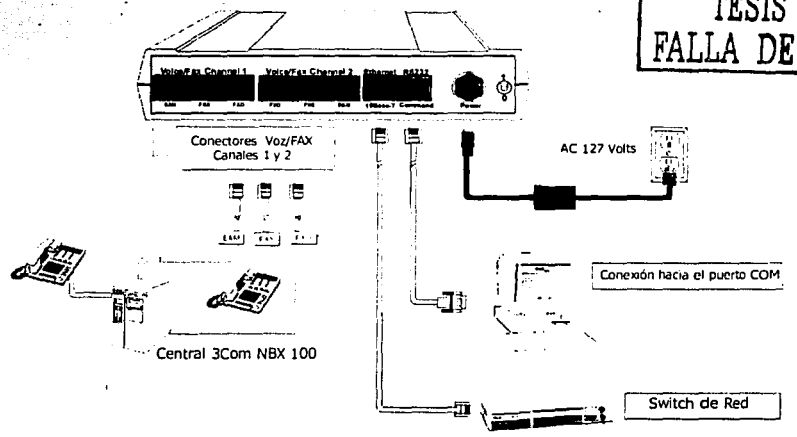
**Nota:** Para cambiar la posición de un puente, se debe levantar el conector correspondiente del bloque de puentes; a continuación, muévalo a la nueva posición, asegurándose de que el puente situado en medio del bloque queda centrado en el número que indica el tipo de E&M (1,3 ó 5).

### 5.1.2- Procedimiento para la instalación de los cables del MultiVOIP

El procedimiento para la conexión entre el MultiVOIP y la central telefónica es el siguiente:

Figura 5.2- Conexión de cables del MultiVOIP






1.- Se deberá conectar el alimentador de corriente del MultiVOIP (es un conector DIN circular de 7 patillas) a una toma de corriente alterna de 127 Volts,60 Hz. y deberá contar con tierra física.

2.- El puerto de comandos del MultiVOIP deberá ser conectado al puerto COM de una PC (el sistema operativo deberá ser Windows 95, 98, ME ó 2000 respectivamente), mediante el cable RJ-45 a DB9 (hembra) que es suministra con el equipo.

3.- La inserción del MultiVOIP a la red local, se realizará utilizando un cable de red Ethernet categoría 5 proveniente del Swicth de la red LAN hacia el puerto Ethernet Base 10-T colocado en el panel posterior del MultiVOIP. (En este caso, en cable

provienen directamente del Swicth, ya que el MultiVOIP, se encuentra colocado en el mismo Rack de equipos activos de la red)

4.- Debido a que la extensión asignada al MultiVOIP, pertenece a una central telefónica PBX digital, se deberá conectar el extremo más pequeño del cable adaptador especial hacia la conexión especificada como **Canal 1 de voz y fax FXO** ubicada en la parte posterior del MultiVOIP, y el otro extremo del cable, deberá ir hacia la central PBX.

Para este caso, las extensiones asignadas de la central telefónica al MultiVOIP, serán configuradas empleando un adaptador analógico / digital, el cual tendrá la función de atender las solicitudes de comunicación provenientes de cualquier extensión de la central telefónica

5.- Una vez realizadas las conexiones anteriores, el MultiVOIP tendrá que ser encendido colocando el interruptor en la posición 1 (arriba, On). El equipo estará listo, cuando el indicador Boot del MultiVOIP se restablezca, esta operación puede demorar unos minutos antes de concluir.

### 5.2- Configuración del MultiVOIP maestro

La implementación del MultiVOIP, requiere necesariamente generar que al menos uno de los equipos opere como "maestro", el cual, como anteriormente se ha señalado, tendrá la función de administrar el directorio telefónico de la red de MultiVOIP que se encuentren conectados en la red.

Debido a la arquitectura concerniente a la seguridad que debe contar una red LAN, es necesario realizar la apertura de puertos pertenecientes al servidor de seguridad (firewall) de la red. Los puertos UDP que deben agregarse para la instalción del MultiVOIP son los siguientes:

Q.931 Signaling, Ch1[900] Q.931 Signaling, Ch2 [902]
Ch1 RTP [5004] Ch1 RTCP [5005]
Ch2 RTP [5006] Ch2 RTCP [5007]

En caso de servidores PROXY, la IP asociada, debe ser excluida del grupo de IP que requiere este servidor, ya que la seguridad de datos se encuentra protegida en la tabla primaria del ruteador.

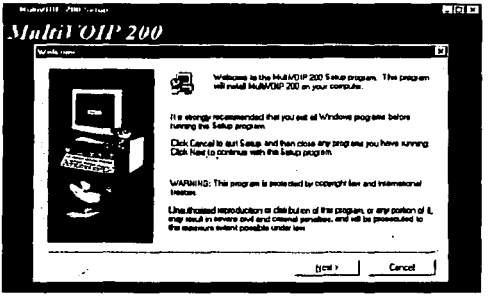
### 5.2.1- Carga del software

La configuración del MultiVOIP maestro requiere la carga y configuración de software.

1.- Introduzca el disco 1 del MultiVOIP en la unidad de disco de la PC que ha sido conectada al MultiVOIP. Como se ha mencionado anteriormente, el sistema operativo deberá que deberá ser Windows 95, 98 ME o 2000

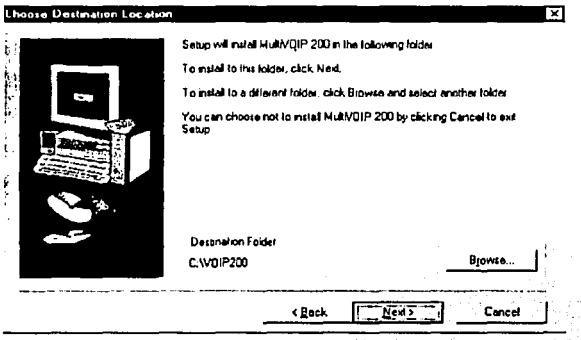
2.-De la barra principal de Windows seleccione el icono de Inicio, posteriormente Ejecutar. Escriba a:/Setup en el cuadro de diálogo de Ejecutar y a continuación, haga clic en Aceptar.

3.- Una vez realizada esta operación, aparecerá la pantalla de bienvenida del programa de instalación MultiVOIP Setup.

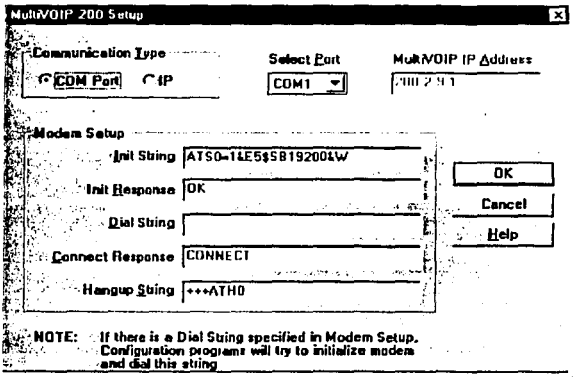



Presione Entrar o haga clic en Next (Siguiente) para continuar.

4.- Seleccione la unidad y el directorio en donde se almacenará el software para la configuración del MultiVOIP.

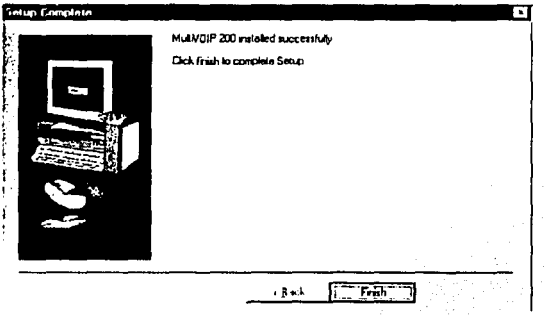



5- El cuadro de diálogo siguiente deberá seleccionarse cual es el puerto COM de la PC en donde se encuentra conectado el puerto de comandos del MultiVOIP. Para este caso, el puerto seleccionado será el puerto COM1 de la ventana Select Port

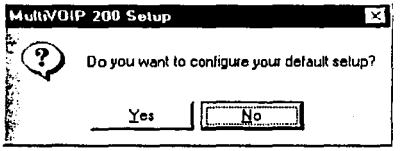



Presione OK para continuar

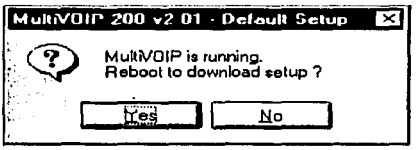
6- A continuación, aparecerá la ventana de Setup Complete. Haga clic en Finish para continuar con la instalación



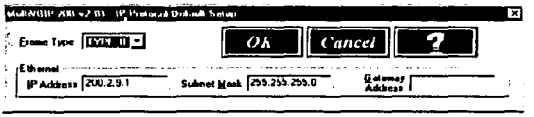

7- El siguiente mensaje, confirma el cambio de la configuración, oprima **Yes** para continuar.




8.- Una vez realizada la configuración, el MultiVOIP, tendrá que reiniciarse para tomar los nuevos valores. Oprima **Yes** para continuar.




9.- Una vez reiniciado el equipo, aparecerá el siguiente cuadro de diálogo IP Protocol Default Setup, en el cual se realizará la configuración predeterminada del protocolo IP.




Para este caso, el tipo de trama predeterminado especificado en Frame Type deberá ser TYPE_II.

10.- Los campos de la sección de Ethernet deberán contar con lo siguiente:

- El campo IP Address, contendrá la dirección IP asignada al MultiVOIP. Para este caso, la IP será: 148.243.236.227

- El campo Subnet Mask, contendrá la máscara de subred. Para este caso, el valor de la mascara será: 255.255.255.0

En el campo Gateway Address, contendrá la IP de la dirección de puerta de enlace única para la red IP LAN y esta dirección conecta al MultiVOIP a Internet.

- . Para este caso será: 148.243.236.225

Es importante señalar, que la dirección IP del MultiVOIP deberá ser única en la red LAN. Por lo que no debe encontrarse repetida y estará fuera del grupo de direcciones DHCP de la red.

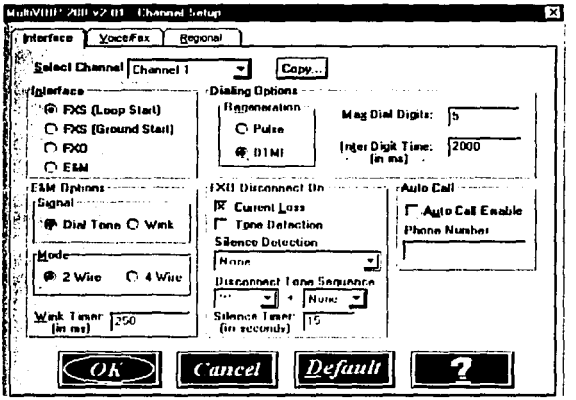
Una vez concluida la configuración, presione OK para avanzar.

11.- A continuación, aparecerá la ventana Channel Setup (Configuración de canales de voz y fax).

Esta ventana, permite establecer la interfaz de los canales de voz y fax, el codificador de voz, así como determinar cuales serán los parámetros telefónicos regionales (pares de tonos) para cada canal del MultiVOIP.

NOTA: La configuración de esta ventana deberá realizarse por cada canal de manera independiente. Es decir, primero se configurarán todas las opciones del Channel 1 (Canal 1) y al concluir, se oprimirá OK para pasar el Channel 2 (Canal2)

Al ingresar a la opción de Interface de la ventana, el primer canal a configurar, será el Channel 1 (Canal 1), el cual siempre será su valor por defecto.






12.- Dentro del Canal 1, el campo Interface (interfaz) corresponde al tipo de interfaz que se conectará al canal 1 de voz y fax en el panel posterior de MultiVOIP. Este campo tendrá como valor por defecto FXS (Loop Start). Sin embargo, para entender que representa cada opción, se describe cual es la función de cada una:

FXS (Loop Start).-
Permite conectar un dispositivo como un teléfono analógico, un fax o un sistema telefónico KTS.

FXS (Gound Start).-
Será utilizada cuando el dispositivo del equipo utiliza un inicio con toma de tierra. Para asegurarse, consulte la documentación del usuario del dispositivo a conectar

FXO
Esta opción, permite conectar una extensión analógica desde un sistema PBX digital.

E&M

Esta opción, se empleará si se desea conectar una línea troncal analógica al sistema PBX. Es decir, serán utilizados los puertos de la central telefónica en vez de una extensión.

Si es seleccionada la opción E&M, es activada un grupo de opciones E&M Options. Donde se tendrá que determinar si la señal es Dial Tone o Wink y si la conexión es de 2 ó 4 cables. Si se utiliza la señal Wink, se habilita el contador Wink Timer con un valor predeterminado de 250 milésimas de segundo. El rango del Wink Timer está entre 100 y 350 milésimas de segundo.

Debido a que la opción seleccionada para este caso será FXO, será activada la tabla de Dialing Options Regeneration (Regeneración de opciones de marcado).

En donde, se debe determinar si las señales si las señales de marcado del PBX local son de pulsos (Pulse) o tonos (DTMF). Para este caso, la opción seleccionada será PULSE.

Para las comunicaciones configuradas de FXO a FXO, es posible activar un tipo específico de desconexión FXO que son:

- Current loss (pérdida de corriente)
- Tone detection (detección de tono)
- Silence detection (detección de silencio)

Para el caso de Current loss (pérdida de corriente) el equipo que desconectado automáticamente por falta de energía eléctrica.

En el caso de la Tone detection (detección de tono), puede ser seleccionada en las listas mostradas, la cantidad de tonos que provocarán la desconexión de la

línea. Es decir, la persona que cuelga la llamada tiene que pulsar una o varias veces cualquier tecla que produzca los tonos.

Para Silence detection (detección de silencio), se deberá seleccionar las opciones de One Way (Unidireccional) o Two Way (Bidireccional). Una vez elegida cualquiera de ambas, se determinará en el contador de tiempo el número de segundos de silencio que provocarán la desconexión. Es posible que el valor predeterminado de fábrica sea de 15 segundos, por lo que, se podrá cambiar el valor disminuyendo o incrementándolo dentro de esta opción.

Finalmente de la opción de Interface, existe el campo Auto Call Enable.

Este campo permite dedicar un canal de voz y fax a un canal remoto de voz y fax (para no tener que llamar al canal remoto), para activar esta función, seleccione la opción Auto Call Enable (Activar autollamada) en el grupo Auto Call. Introduzca el número de teléfono correspondiente en el campo Phone Number.

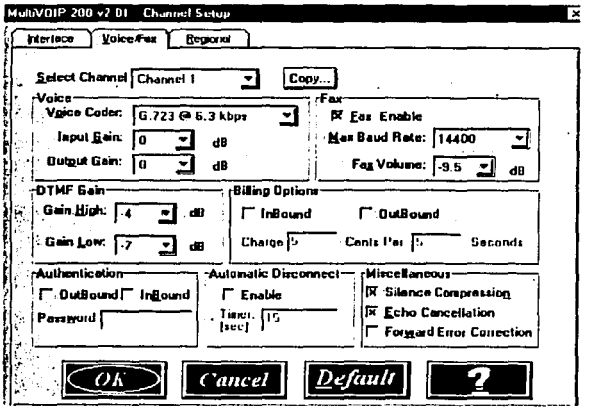
Oprima **OK** para que los campos sean registrados

13.- Una vez concluida la configuración de Channel 1 (Canal 1), es posible copiar la configuración de este canal hacia el Channel 2 (Canal 2). Para realizar esto, oprima el botón Copy (copiar) y automáticamente todo lo que aparece en la ficha Interface se copiará directamente al Channel 2 (Canal 2).

14.- Los parámetros que muestra la opción de Voice/Fax (Voz/Fax) son:

- Parámetros para la codificación de la voz
- Envío de faxes
- Ganancia de DTMF
- La facturación de gastos para llamadas entrantes o salientes
- Autenticación de contraseñas para llamadas entrantes o salientes

- Desconexión automática para limitar el tiempo de duración de las llamadas.






15.- Antes de realizar cualquier cambio para la codificación de voz, se seleccionará primero el canal en donde se realicen los cambios. Para ello, del campo Select Channel, determine cual es el número de canal en que se desean realizar los cambios. Para este caso la opción será Channel 1 (Canal 1).

Ya seleccionado el canal, se deberá seleccionar del campo Voice Coder la codificación de voz que desee emplear.

Cualquier cambio en la selección de la codificador de voz, obligará a emplear la misma codificación en el canal de voz y fax al que se va a llamar. Si no se realiza este cambio, ocasionará que en cada solicitud de marcado, sea recibida la señal de ocupado en los equipos.

16.- Como la opción seleccionada para esta implementación consistió en la interfaz FXO y el marcado se realiza mediante tonos, se debe configurar la ganancia de DTMF o nivel de potencia en decibelios (dB) para los grupos de

frecuencias más altas y más bajas del par de tonos DTMF. Esta ganancia se debe seleccionar de las listas que se presentan en el grupo DTMF Gain (Ganancia DTMF).

La ganancia de DTMF para este caso se encuentra determinada en los siguientes rangos:

Gain High : -3 dB
Gain Low : -5 dB

17.- La opción Fax, hace posible el envío y recepción de faxes en el canal de voz y fax seleccionado. Esta opción, permite, configurar la velocidad en baudios para faxes en la lista que se activa en el grupo Fax.

En el caso de no considerar el envío o recepción de fax dentro de un canal de voz y fax determinado, se tendrá que desactivar los faxes en el grupo Fax.

18.- La opción de facturación de llamadas entrantes y salientes, deberá ser seleccionada dentro del grupo Billing Options (Opciones de facturación). Donde se tendrá que configurar, insertando los costos reales por llamada hacia los destinos que sean elegidos.

Es decir, el costo por llamada (usando la red telefónica publica) proveniente de los Headquarters hacia las oficinas o sucursales donde se emplea el MultiVOIP. Debido a que el proveedor del servicio de telefonía nos es el mismo en cada región en que será (TELMEX, Telefónica Arg) implementado el servicio; el costo que será elegido como medida, será el cargo más alto que se genere por llamada entre cada localidad.

Por ejemplo:

Costo por minuto en hora pico de México a Bs As: $ 0.83 dlls
Costo por minuto en hora pico de Bs As a México: $ 1.01 dlls

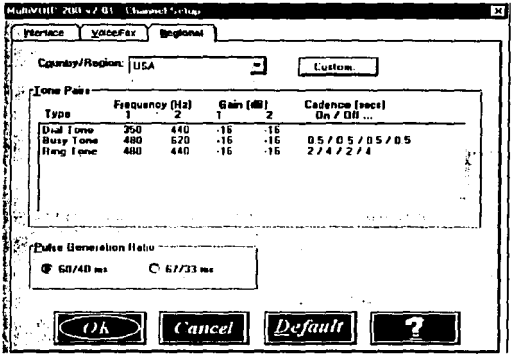
Por lo que el costo elegido será de $1.01 dlls por minuto

19.- Para activar la protección mediante contraseña en llamadas entrantes o salientes realizadas por un canal de voz y fax seleccionado, es necesario, activar el campo Authentication (Autenticación). Posteriormente, se debe introducir en el campo Password (Contraseña) una clave que contenga un mínimo de 5 y un máximo de 14 caracteres numéricos sin que estos sean caracteres especiales como &,/,$,ñ, etc.

20.- La opción Automatic Disconnect (Desconexión automática) tiene la función de limitar la duración de las llamadas, de acuerdo al tiempo determinado en segundos, que son determinados dentro del campo de contador de tiempo Timer: (sec). El valor predeterminado del equipo es de 15 segundos, sin embargo, podrá determinarse cualquier otro valor hasta un máximo de 65.535 segundos que son aproximadamente 18,2 horas.

Al concluir la configuración del Channel 1 (Canal 1), puede realizarse la configuración del Channel 2 (Canal 2), copiando la configuración del Channel 1 (Canal 1) hacia en el Channel 2 (Canal 2). Para realizar esto, oprima el botón Copy (Copiar) y la configuración realizada en la opción Voice/Fax para el Channel 1 (Canal 1) se copiará íntegramente al Channel 2 (Canal 2).

21.- La opción Regional, permite elegir el país o localidad en donde se encuentra instalado el MultiVOIP, Para realizar los cambios de los pares de tonos dentro de esta opción, se deberá elegir el campo Country/Región (País/Región) y seleccionar el país o región donde se encuentra el MultiVOIP. Para este caso, la opción elegida en el campo Country/Region será México

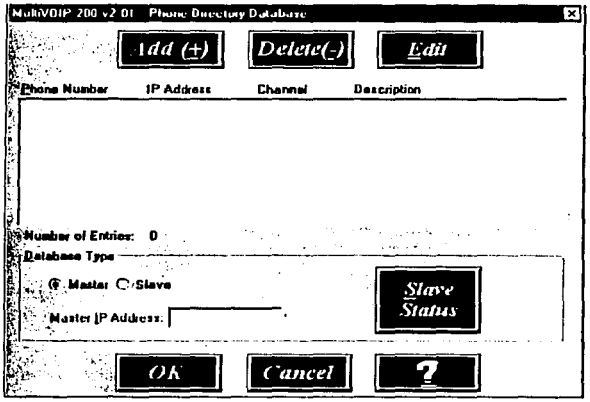



Al realizar la selección, de manera automática, los parámetros de pares de tonos cambiaran a los determinados para la región elegida.

Oprima OK para registrar los cambios y continuar la configuración

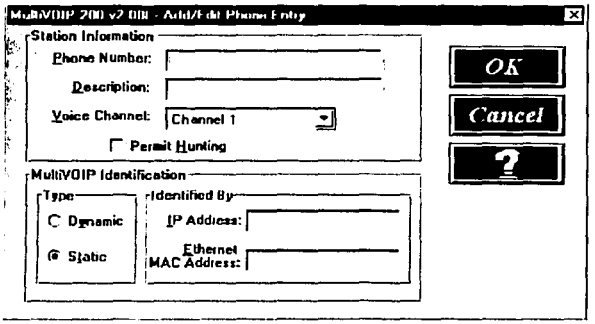
22.- Al terminar la configuración anterior, se iniciará la creación de la base de teléfonos, la cual se realizará en la ventana de Phone Directory Database (Base de datos de teléfonos). Esto permitirá crear un directorio telefónico personalizado de MultiVOIP hacia otras localidades.

Es importante señalar, que el MultiVOIP configurado como Maestro contendrá la base de datos maestra, la cual contiene los números de teléfono de todos los MultiVOIP que se encuentran disponibles para comunicarse entre las redes IP predeterminadas. Esta base de datos se descarga y actualiza en cada uno de los MultiVOIP esclavos cuando están en línea entre sí.




Para iniciar con el registro de directorio, seleccione el botón de Add (+) (Agregar) para crear la base de datos de teléfonos.

23.- Una vez seleccionada, aparecerá el cuadro de diálogo Add/Edit Pone Entry (Agregar / Editar teléfonos)






De la sección Station Information se deberá realizar lo siguiente:

Seleccione el campo Phone Number e introduzca el número de teléfono único y que corresponde al dispositivo local conectado al Channel 1(Canal 1). Para este caso el número será 101 (este código identifica al país donde se encuentra el equipo instalado)

Dentro del campo (Optional) Description (Descripción Opcional), será introducida la descripción que identifica al teléfono local. Esta descripción, tiene la función de identificar el número introducido en el paso anterior. Para este caso, la descripción será: Headquarters México

En campo de Permit Hunting tiene la función de permitir que el equipo que responde a la llamada pueda cambiar a un segundo canal si el primero se encuentra ocupado. Para este caso, se activará el campo de Permit Hunting para permitir que las llamadas pasen a un segundo canal de voz y fax.

24.- En el grupo MultiVOIP Identification (Identificación de MultiVOIP), se deberá realizar los siguientes pasos.

La sección TYPE permite que el MultiVOIP maestro pueda comunicarse con los MultiVOIP remotos o esclavos y descargar una copia de la base de datos de teléfonos maestra. Por lo que la opción Static debe encontrarse activa para realizar esta actualización.

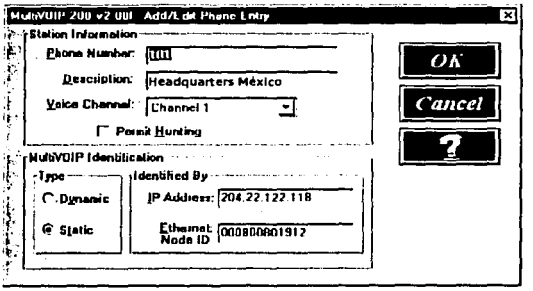
En la sección Identified By, el campo de IP Address deberá contener la dirección IP del MultiVOIP maestro. Para este caso, la dirección IP que ha sido asignada es, 148.243.236.227

El campo de Ethernet Mac Address, contendrá los 12 dígitos correspondientes al ID del nodo (0008005xxxxxx) o Mac Address de la tarjeta. Para llenar este campo, puede revisarse la placa de ID situada en el panel posterior del MultiVOIP y escribir el número que aparece como Ethernet Node ID.

Opcionalmente, puede obtenerse este número realizando el siguiente procedimiento.

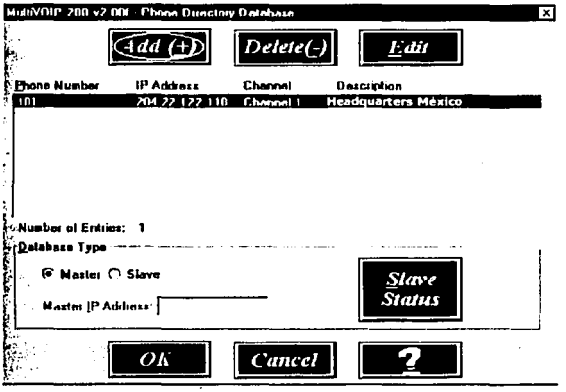
Del menú Telnet Server del MultiVOIP, introduzca el número 1 para avanzar hacia el menú principal. Una vez dentro, introduzca 3 para observar la información del sistema. Dentro de esta sección, el elemento mostrado como 1 será la dirección de puerto Ethernet que se requiere introducir en el campo Ethernet Node ID.

Finalmente, los cambios realizados en esta ventana se apreciarán con en la siguiente imagen.



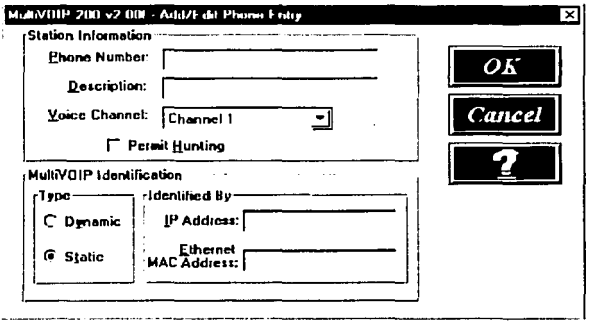

Oprima la opción de OK para regresar a la ventana de Phone Directory Database.

25.- La ventana de Pone Directory Database, contendrá la configuración realizada en el paso anterior.




Para borrar la configuración seleccione la opción Delete (-) y para revisar la configuración o para realizar cambios, seleccione la opción de Edit .

26.- Para iniciar con la configuración del MultiVOIP remoto, seleccione la opción Add (+) y volverá a mostrarse la ventana de diálogo Add/Edit Pone Entry (Agregar / Editar teléfonos)






27.- De la sección Station Information se deberá realizar lo siguiente:

Seleccione el campo Phone Number e introduzca el número de teléfono único y que corresponde al dispositivo local conectado al Channel 1(Canal 1). Para este caso el número será 201.

Dentro del campo (Optional) Description (Descripción Opcional), será introducida la descripción que identifica al teléfono local. Esta descripción, tiene la función de identificar el número introducido en el paso anterior. Para esta implementación, la descripción será: Office Country Zaniartur

En campo de Permit Hunting tiene la función de permitir que el equipo que responde a la llamada pueda cambiar a un segundo canal si el primero se encuentra ocupado. Para este caso, se activará el campo de Permit Hunting para permitir que las llamadas pasen a un segundo canal de voz y fax.

28.- En el grupo MultiVOIP Identification (Identificación de MultiVOIP), se deberá realizar los siguientes pasos.

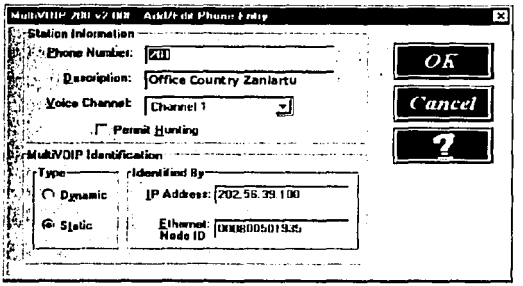
La sección TYPE permite que el MultiVOIP maestro pueda comunicarse con los MultiVOIP remotos o esclavos y descargar una copia de la base de datos de teléfonos maestra. Por lo que la opción Static debe encontrarse activa para realizar esta actualización.

Sin embargo, si el MultiVOIP remoto se encuentra implementado detrás de un Servidor Proxy que utiliza una dirección IP de asignación dinámica (DHCP), deberá seleccionar la opción, Dynamic (para desactivar la dirección IP estática) y deje en blanco el campo correspondiente a la dirección IP. El MultiVOIP maestro conocerá la dirección IP cuando el MultiVOIP remoto se comunique con él.

En la sección Identified By, el campo de IP Address deberá contener la dirección IP del MultiVOIP maestro. Para este caso, la dirección IP que ha sido asignada es, 200.23.87.19

El campo de Ethernet Mac Address, contendrá los 12 dígitos correspondientes al ID del nodo (0008005xxxxxx) o Mac Address de la tarjeta. Para llenar este campo, puede revisarse la placa de ID situada en el panel posterior del MultiVOIP y escribir el número que aparece como Ethernet Node ID.

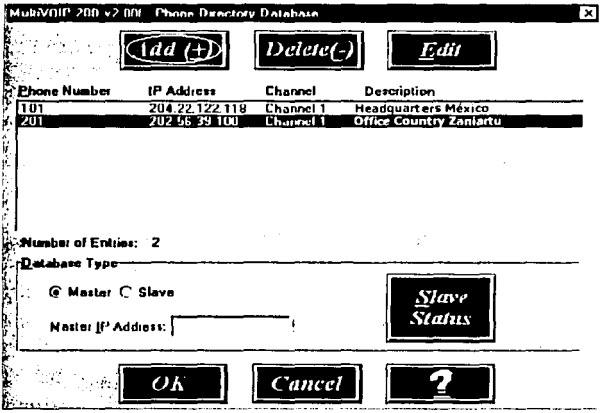
La configuración realizada se observara como en la siguiente figura.




29.- Oprima OK para regresar a la ventana de Phone Directory Database, la que muestra la segunda configuración realizada, así como la información relativa a esta dentro de la lista de números de teléfono Pone Number.

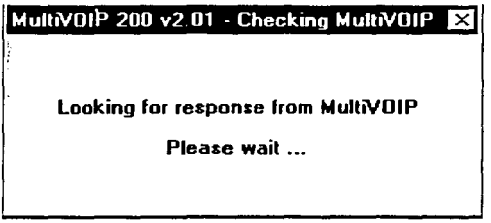
Cabe señalar, que si sólo se encuentra activo el Channel 1 (Canal 1) se tendrá que introducir dos números de teléfono. El primero corresponderá al teléfono del MultiVOIP local para el Channel 1 (Canal 1), y el segundo representará el teléfono del MultiVOIP remoto para el Channel 1 (Canal 1).

Si se encuentran activados ambos canales (1 y 2), se deben de introducir cuatro números.

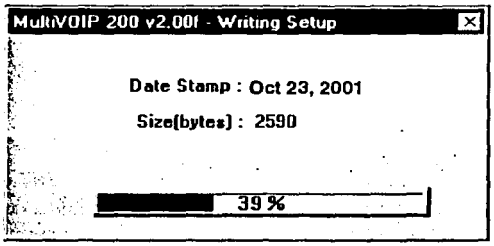



30.- Al finalizar la configuración, oprima OK para descargar la configuración en el MultiVOIP en los equipos remotos.

31.- Para realizar esta descarga, el MultiVOIP, realizará una comprobación de los equipos conectados.




32.- Al finalizar la comprobación, aparecerá la ventana de Writing Setup (Escribiendo Configuración) mientras la configuración se escribe en el MultiVOIP.




33.- Una vez escrita la configuración en el MultiVOIP, se reinicia automáticamente.

34.- Es necesario asegurarse de que el indicador BOOT del MultiVOIP se encuentre apagado una vez al completar la descarga de la configuración. Es normal, que pasen algunos unos minutos hasta que el MultiVOIP se reinicia en estos cambios.

35.- Al terminar la configuración, el usuario que se encuentre trabajando sobre Windows 95, 98, 2000 y ME; regresará a la carpeta del MultiVOIP. Esta se encontrará abierta sobre el escritorio del programa.

A partir de este momento, el MultiVOIP maestro ya se encuentra configurado para trabajar correctamente.

### 5.3- MultiVOIP esclavo

Debido a la arquitectura concerniente a la seguridad que debe contar una red LAN, es necesario realizar la apertura de puertos pertenecientes al servidor de seguridad (firewall) de la red. Los puertos UDP que deben agregarse para la instalción del MultiVOIP son los siguientes:

Status [5000]
Q.931 Signaling, Ch1[900] Q.931 Signaling, Ch2 [902]
Ch1 RTP [5004] Ch1 RTCP [5005]
Ch2 RTP [5006] Ch2 RTCP [5007]

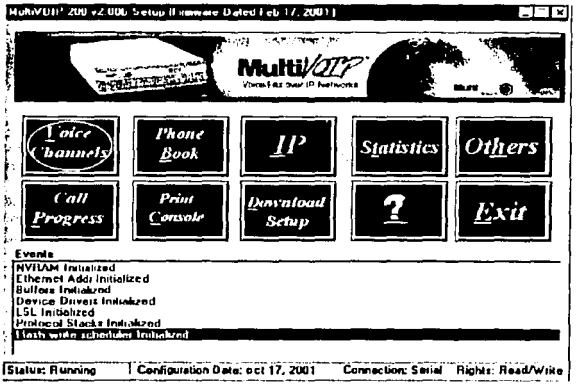
En caso de servidores PROXY, la IP asociada, debe ser excluida del grupo de IP que requiere este servidor, ya que la seguridad de datos se encuentra protegida en la tabla primaria del ruteador.

#### 5.3.1- Configuración del MultiVOIP esclavo

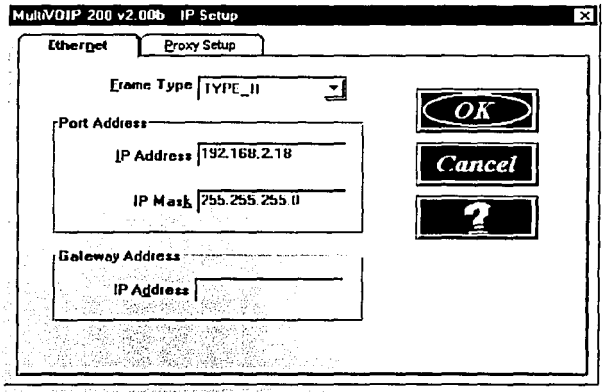
La configuración del MultiVOIP esclavo requiere la carga y configuración de software. Desconecte el PC del puerto de comandos del MultiVOIP maestro y conéctelo al puerto de comandos del MultiVOIP esclavo.

1.- Introduzca el disco 1 del MultiVOIP en la unidad de disco de la PC que ha sido conectada al MultiVOIP. Como se ha mencionado anteriormente, el sistema operativo deberá que deberá ser Windows 95, 98 ME o 2000

2.-De la barra principal de Windows seleccione el icono de Inicio, posteriormente Programas, MultiVOIP y finalmente MultiVOIP Configuration. La ventana de inicio de programa permitirá continuar con la configuración.




3.- Oprima la opción de IP para avanzar hacia la ventana de IP Setup (Configuración de IP).






Para esta implementación, el tipo de trama predeterminado especificado en Frame Type deberá ser TYPE_II.

4.- Los campos de la sección de Ethernet deberán contar con lo siguiente:

- El campo IP Address, contendrá la dirección IP asignada al MultiVOIP. Para este caso, la IP será: 200.23.87.19
- El campo Subnet Mask, contendrá la máscara de subred. Para este caso, el valor de la mascara será: 255.255.255.0

En el campo Gateway Address, contendrá la IP de la dirección de puerta de enlace única para la red IP LAN y esta dirección conecta al MultiVOIP a Internet.

- . Para este caso será: 200.23.87.1

Es importante señalar, que la dirección IP del MultiVOIP deberá ser única en la red LAN. Por lo que no debe encontrarse repetida y estará fuera del grupo de direcciones DHCP de la red.

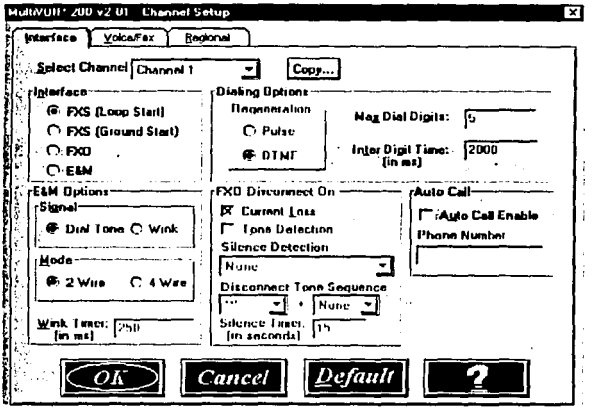
Una vez concluida la configuración, presione OK para regresar al menú principal.

5.- A continuación, aparecerá la ventana Channel Setup (Configuración de canales de voz y fax).

Esta ventana, permite establecer la interfaz de los canales de voz y fax, el codificador de voz, así como determinar cuales serán los parámetros telefónicos regionales (pares de tonos) para cada canal del MultiVOIP.

NOTA: La configuración de esta ventana deberá realizarse por cada canal de manera independiente. Es decir, primero se configurarán todas las opciones del Channel 1 (Canal 1) y al concluir, se oprimirá OK para pasar el Channel 2 (Canal2)

Al ingresar a la opción de Interface de la ventana, el primer canal a configurar, será el Channel 1 (Canal 1), el cual siempre será su valor por






6.- Dentro del Canal 1, el campo Interface (interfaz) corresponde al tipo de interfaz que se conectará al canal 1 de voz y fax en el panel posterior de MultiVOIP. Este campo tendrá como valor por defecto FXS (Loop Start). Sin embargo, para entender que representa cada opción, se describe cual es la función de cada una:

FXS (Loop Start).-
Permite conectar un dispositivo como un teléfono analógico, un fax o un sistema telefónico KTS.

FXS (Gound Start).-
Será utilizada cuando el dispositivo del equipo utiliza un inicio con toma de tierra. Para asegurarse, consulte la documentación del usuario del dispositivo a conectar

FXO
Esta opción, permite conectar una extensión analógica desde un sistema PBX digital.

E&M

Esta opción, se empleará si se desea conectar una línea troncal analógica al sistema PBX. Es decir, serán utilizados los puertos de la central telefónica en vez de una extensión.

Si es seleccionada la opción E&M, es activada un grupo de opciones E&M Options. Donde se tendrá que determinar si la señal es Dial Tone o Wink y si la conexión es de 2 ó 4 cables. Si se utiliza la señal Wink, se habilita el contador Wink Timer con un valor predeterminado de 250 milésimas de segundo. El rango del Wink Timer está entre 100 y 350 milésimas de segundo.

Debido a que la opción seleccionada para este caso será FXO, será activada la tabla de Dialing Options Regeneration (Regeneración de opciones de marcado).

En donde, se debe determinar si las señales si las señales de marcado del PBX local son de pulsos (Pulse) o tonos (DTMF). Para este caso, la opción seleccionada será PULSE.

Para las comunicaciones configuradas de FXO a FXO, es posible activar un tipo específico de desconexión FXO que son:

- Current loss (pérdida de corriente)
- Tone detection (detección de tono)
- Silence detection (detección de silencio)

Para el caso de Current loss (pérdida de corriente) el equipo que desconectado automáticamente por falta de energía eléctrica.

En el caso de la Tone detection (detección de tono), puede ser seleccionada en las listas mostradas, la cantidad de tonos que provocarán la desconexión de la línea. Es decir, la persona que cuelga la llamada tiene que pulsar una o varias veces cualquier tecla que produzca los tonos.

Para Silence detection (detección de silencio), se deberá seleccionar las opciones de One Way (Unidireccional) o Two Way (Bidireccional). Una vez elegida cualquiera de ambas, se determinará en el contador de tiempo el número de segundos de silencio que provocarán la desconexión. Es posible que el valor predeterminado de fábrica sea de 15 segundos, por lo que, se podrá cambiar el valor disminuyendo o incrementándolo dentro de esta opción.

Finalmente de la opción de Interface, existe el campo Auto Call Enable.

Este campo permite dedicar un canal de voz y fax a un canal remoto de voz y fax (para no tener que llamar al canal remoto), para activar esta función, seleccione la opción Auto Call Enable (Activar autollamada) en el grupo Auto Call. Introduzca el número de teléfono correspondiente en el campo Phone Number.

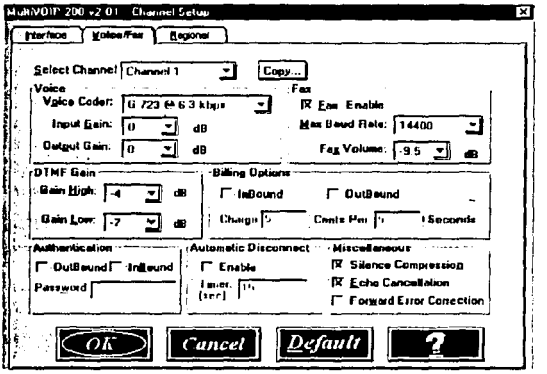
Oprima OK para que los campos sean registrados

7.- Una vez concluida la configuración de Channel 1 (Canal 1), es posible copiar la configuración de este canal hacia el Channel 2 (Canal 2). Para realizar esto, oprima el botón Copy (copiar) y automáticamente todo lo que aparece en la ficha Interface se copiará directamente al Channel 2 (Canal 2).

8.- Los parámetros que muestra la opción de Voice/Fax (Voz/Fax) son:

- Parámetros para la codificación de la voz
- Envío de faxes
- Ganancia de DTMF
- La facturación de gastos para llamadas entrantes o salientes
- Autenticación de contraseñas para llamadas entrantes o salientes

Desconexión automática para limitar el tiempo de duración de las llamadas.






9.- Antes de realizar cualquier cambio para la codificación de voz, se seleccionará primero el canal en donde se realicen los cambios. Para ello, del campo Select Channel, determine cual es el número de canal en que se desean realizar los cambios. Para este caso la opción seña Channel 1 (Canal 1).

Ya seleccionado el canal, se deberá seleccionar del campo Voice Coder la codificación de voz que desee emplear.

Cualquier cambio en la selección de la codificador de voz, obligará a emplear la misma codificación en el canal de voz y fax al que se va a llamar. Si no se realiza este cambio, ocasionará que en cada solicitud de marcado, sea recibida la señal de ocupado en los equipos.

10.- Como la opción seleccionada para esta implementación consistió en la interfaz FXO y el marcado se realiza mediante tonos, se debe configurar la ganancia de DTMF o nivel de potencia en decibelios (dB) para los grupos de frecuencias más altas y más bajas del par de tonos DTMF. Esta ganancia se debe seleccionar de las listas que se presentan en el grupo DTMF Gain (Ganancia DTMF).

La ganancia de DTMF para este caso se encuentra determinada en los siguientes rangos:

Gain High : -3 dB
Gain Low : -5 dB

11.- La opción Fax, hace posible el envío y recepción de faxes en el canal de voz y fax seleccionado. Esta opción, permite, configurar la velocidad en baudios para faxes en la lista que se activa en el grupo Fax.

En el caso de no considerar el envío o recepción de fax dentro de un canal de voz y fax determinado, se tendrá que desactivar los faxes en el grupo Fax.

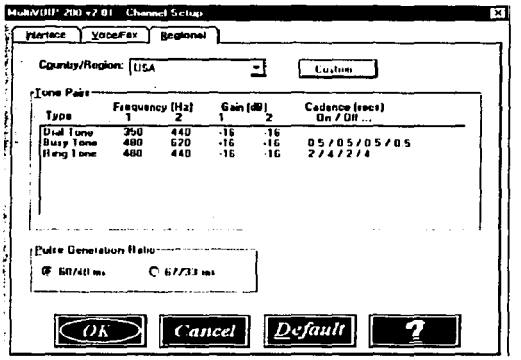
12.- La opción de facturación de llamadas entrantes y salientes, deberá ser seleccionada dentro del grupo Billing Options (Opciones de facturación). Donde se tendrá que configurar, insertando los costos reales por llamada hacia los destinos que sean elegidos.

13.- Para activar la protección mediante contraseña en llamadas entrantes o salientes realizadas por un canal de voz y fax seleccionado, es necesario, activar el campo Authentication (Autenticación). Posteriormente, se debe introducir en el campo Password (Contraseña) una clave que contenga un mínimo de 5 y un máximo de 14 caracteres numéricos sin que estos sean caracteres especiales como &,/,$,ñ, etc.

14.- La opción Automatic Disconnect (Desconexión automática) tiene la función de limitar la duración de las llamadas, de acuerdo al tiempo determinado en segundos, que son determinados dentro del campo de contador de tiempo Timer: (sec). El valor predeterminado del equipo es de 15 segundos, sin embargo, podrá determinarse cualquier otro valor hasta un máximo de 65.535 segundos que son aproximadamente 18,2 horas.

Al concluir la configuración del Channel 1 (Canal 1), puede realizarse la configuración del Channel 2 (Canal 2), copiando la configuración del Channel 1 (Canal 1) hacia en el Channel 2 (Canal 2). Para realizar esto, oprima el botón Copy (Copiar) y la configuración realizada en la opción Voice/Fax para el Channel 1 (Canal 1) se copiará íntegramente al Channel 2 (Canal 2).

15.- La opción Regional, permite elegir el país o localidad en donde se encuentra instalado el MultiVOIP, Para realizar los cambios de los pares de tonos dentro de esta opción, se deberá elegir el campo Country/Región (País/Región) y seleccionar el país o región donde se encuentra el MultiVOIP. Para este caso, la opción elegida en el campo Country/Region será México





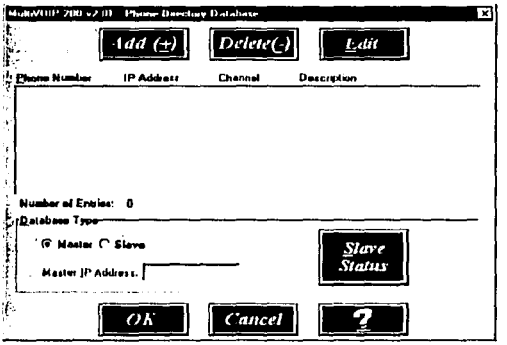

Al realizar la selección, de manera automática, los parámetros de pares de tonos cambiaran a los determinados para la región elegida.

Oprima OK para registrar los cambios y continuar la configuración

16.- Al terminar la configuración anterior, se iniciará la creación de la base de telefonos, la cual se realizará en la ventana de Phone Directory Database (Base

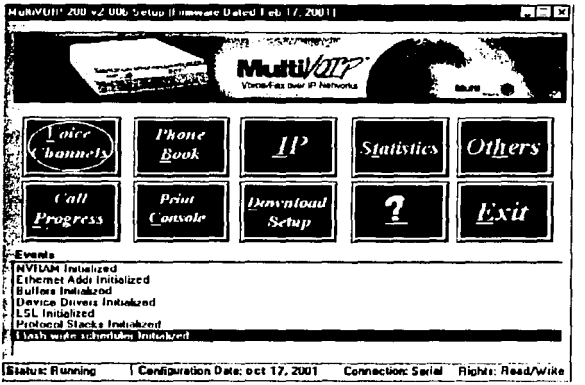
de datos de teléfonos). Esto permitirá crear un directorio telefónico personalizado de MultiVOIP hacia otras localidades.

17.- Introduzca la dirección IP del MultiVOIP maestro en el campo Master IP Address. Para esta implementación, la IP del MultiVOIP maestro es la IP: 148.243.236.227

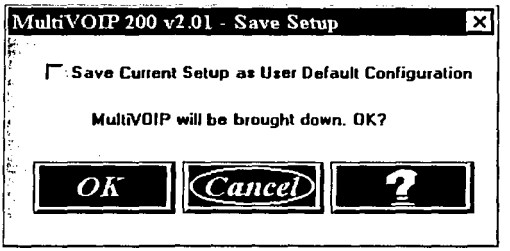



18.- Seleccione OK para aceptar los valores y regresar al menú principal.

19.- Una vez dentro del menú principal, seleccione la opción Download Setup (Descargar configuración), la cual escribirá la nueva configuración en la unidad esclava.

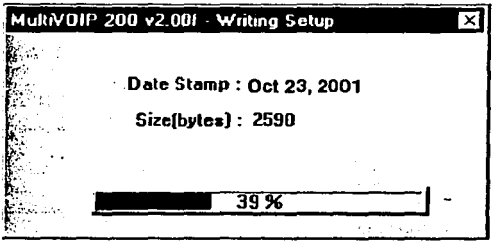



Al se seleccionada, aparecerá la venta de Save Setuo (Guardar Configuración).




20.- Dentro de esta ventana, seleccione la casilla, Save Current Setup as User Default Configuration (Guardar configuración actual como predeterminada del usuario) y oprima OK.

Se mostrará la ventana de Writing Setup (Escribiendo Configuración) mientras se escribe en el MultiVOIP.




Una vez escrita la configuración en el MultiVOIP, se reinicia automáticamente.

21.- Es necesario asegurarse de que el indicador BOOT del MultiVOIP se encuentre apagado una vez al completar la descarga de la configuración. Es normal, que pasen algunos unos minutos hasta que el MultiVOIP se reinicia en estos cambios.

Una vez reiniciado se regresará al menú principal.

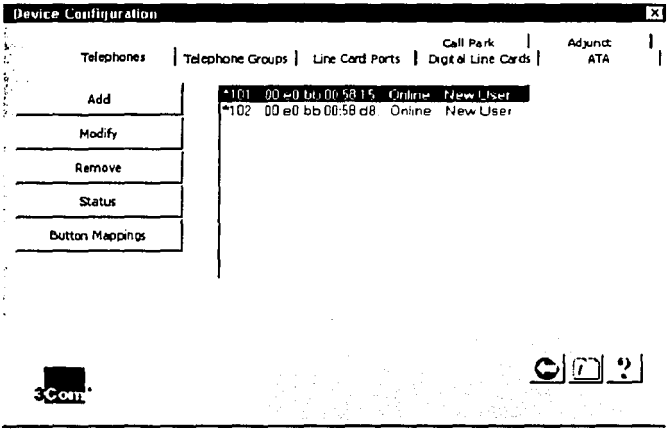
En este momento, el MultiVOIP esclavo ya puede operar correctamente.

Esta fase de configuración, se deberá realizar por cada MultiVOIP esclavo que se desee agregar.

## 5.4- Configuración de la central telefónica 3como NBX 100

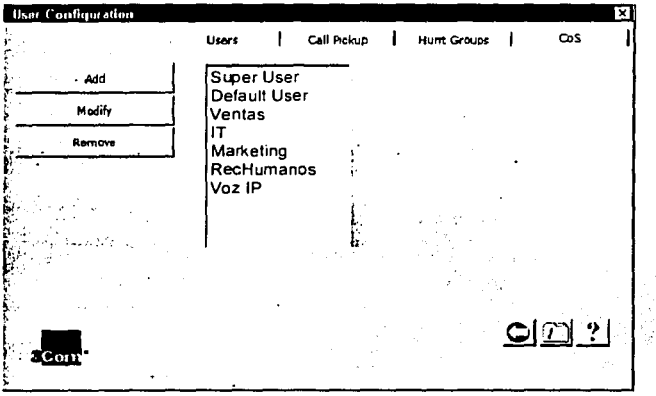
Al finalizar la instalación y configuración del MultiVOIP, es necesario realizar algunos cambios en la central telefónica. Estos cambios, tendrá la finalidad de crear un ambiente sencillo y amigable para los usuarios. Estos cambios en la central 3Com NBX 100 son los siguientes:

- Desde la consola de administración de la central, se deberá crear y asignar un nuevo numero de extensión al adaptador conectador al MultiVOIP' Para este caso el número de extensión asignadas a los equipos será la extensión 101 y 102 respectivamente

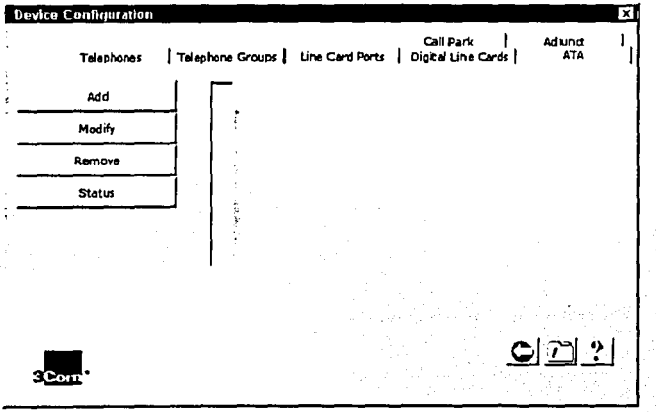





- Posteriormente, es indispensable, asignar los permisos de marcación para cada una de las extensiones creadas. Esta operación se realiza dentro de los grupos de trabajo que se encuentran dados de alta en la central.




- Restringir los permisos de marcación de la extensión habilitando códigos de acceso para la generación de llamadas de la red privada a una la red pública.

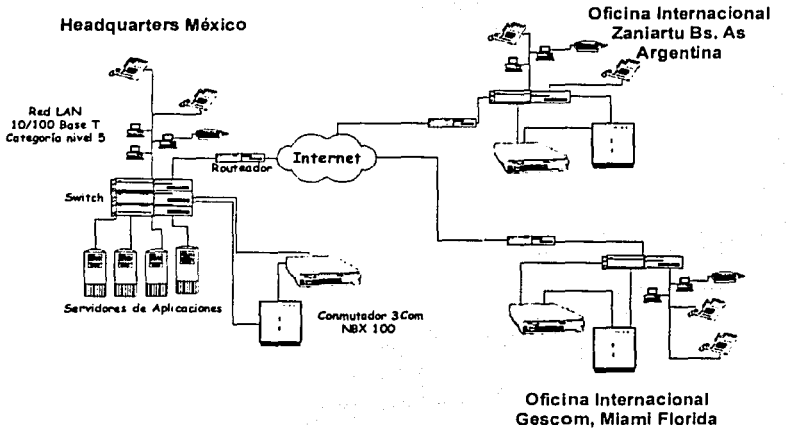


Cabe señalar, que un servicio con que cuenta la central telefónica es la identificación de las llamadas entrantes. Este puede variar debido a que el MultiVOIP representa un elemento externo a la misma. Por lo que, es necesario durante la creación de la extensión, asignar el nombre del canal del MultiVOIP por donde se recibe la llamada. Con esto, se logrará contar con una herramienta que permita determinar el uso y tráfico de llamadas que son generadas de este servicio.

Al concluir estos cambios, tanto en la central telefónica 3Com NBX 100 como con el MultiVOIP, la implementación de Voz sobre IP se debe considerar concluida.

El diagrama de conexión al finalizar la implementación es el siguiente.

**Estado final de la red con la implementación del MultiVOIP**




## 5.5- Análisis de los costos de larga distancia internacional posteriores a la implementación de voz sobre IP

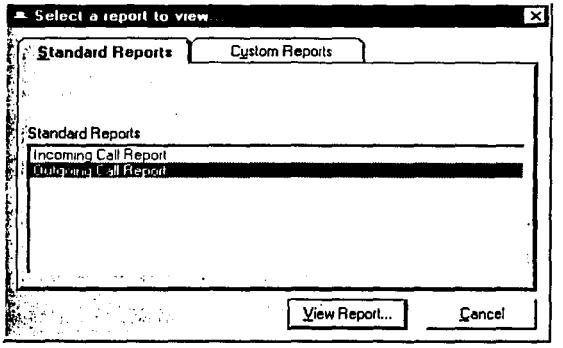
Como se ha mencionado anteriormente, este trabajo intenta obtener la reducción de los costos derivados del servicio de telefónica de larga distancia internacional entre las distintas oficinas regionales de una empresa.

Para determinar que la solución instalada sea un éxito, es necesario observar el escenario anterior y posterior a la implementación.

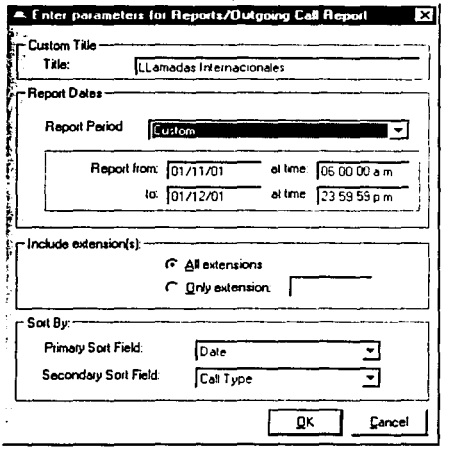
Para obtener esta información, es indispensable generar los reportes previos y posteriores mediante los reportes de llamadas realizadas con clave internacional. Esta información, se encuentra contenida en la central telefónica 3Com NBX100, y podrá obtenerse realizado los siguientes pasos.

1.- Se deberá ingresar al modulo de generación de reportes con que cuenta la central o NBX Call Reports, como se muestra en la siguiente figura:


2.- Una vez dentro de este modulo, deberá elegirse el tipo de reporte que se desea obtener. En este caso, será el reporte de llamadas realizadas (Outgoing Call Report)




3.- Una vez elegido el tipo de reporte, es necesario indicar el tiempo de un periodo previo a la implementación de la solución de voz sobre IP., tal como se indica en la siguiente ventana:




4.- La información generada por este reporte es la siguiente:

Llamadas Internacionales 01/12/01

Call Distribution for
LD Internacional

**Total: $47320.00**

Details

| Hour | # Calls | Duration (seconds) |
|---|---|---|
| 36 | 1715 | 129600 |

Donde;

Costo del servicio de telefonía de larga distancia internacional previo a la implementación de voz sobre IP fue de: $47,320.00 m.n.

5.- Para obtener el reporte posterior a implementación de voz sobre IP, deberá realizarse los pasos anteriores. Una vez determinado el periodo de tiempo, la información generada por el reporte de la central telefónica 3Com NBX 100, será la siguiente:

Llamadas Internacionales 01/12/01

Call Distribution for
LD Internacional

**Total: $4116.00**

Details

| Hour | # Calls | Duration (seconds) |
|---|---|---|
| 97 | 3741 | 349200 |



Donde;

El costo del servicio de telefonía de larga distancia internacional: $4116.00 m.n.

Comparando la información de cada reporte anterior nos permite concluir que:

- La reducción de los costos del servicio telefónico de larga distancia internacional fue del 91.7% aproximadamente

El resultado obtenido de la implementación de este servicio, cumple con el objetivo principal de este proyecto, que consiste, en la reducción de costos mediante generados por centrales telefónicas remotas implementando voz sobre IP a través del Multivoip 2000.

# Capitulo VI

# El ruteo y su función principal en las redes TCP/IP

**Capitulo VI**

## El ruteo y su función principal en las redes TCP/IP



### 6.1- ¿ Qué es el ruteo?

El ruteo, es la operación en donde se lleva a cabo la transferencia de información desde un punto de origen a un punto destino a través de las redes de computo.

Esta operación es llevada acabo por equipos conocidos con el nombre de ruteadores. Para realizar esta función, los ruteadores puede ser configurados con el fin de encaminar los paquetes de datos entre sus distintos puertos y destinos en la red.

Los ruteadores son equipos que brindan seguridad en la red; ya que al ser combinados con otros elementos, pueden crear Redes Privadas Virtuales (VPNs) y WANs amplias y escalables. Para la realización de este trabajo se emplea la serie de ruteadores Cisco 1700.

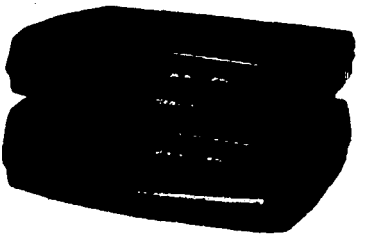


Figura 6.1- Ruteador Cisco Serie 1700

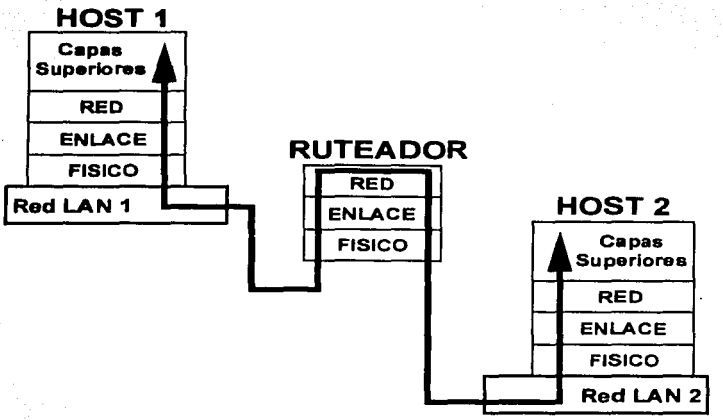
El ruteador Cisco 1700, es la solución perfecta para los crecientes anchos de bandas de las empresas que cuentan con estructuras "virtuales", empresas complementarias con las que tienen alianzas, colaboradores externos que proporcionan un servicio dedicado o incluso una red de sucursales de oficinas,

combinadas para crear una gran empresa escalable. Para este caso, la empresa cuenta con una red de oficinas internacionales que se encuentran interconectadas entre sí.

El ruteador interconecta las redes de área local LAN, que se encuentran operando en el nivel 3 del modelo OSI, por lo que su funcionalidad se encuentra condicionada por el protocolo de red. Esto ocasiona que su rendimiento sea vea afectado en cuestión de tiempo, ya que este realiza un proceso de análisis de los paquetes del nivel de red que le llegan, sin embargo, permite una organización muy flexible dentro de la interconexión de las redes.

Para seleccionar el ruteador adecuado a la red, debe considerar el tipo de protocolo de red en que se va a encaminar los paquetes. Ya que, un routeador que encamine los paquetes usando el protocolo TCP/IP no funcionará para encaminar los paquetes de algún otro protocolo. Sin embargo, los ruteadores que se distribuyen comercialmente cuentan con la capacidad de encaminar los paquetes usando los protocolos más comunes, y todos estos se encuentran operando en el nivel3 de la capa OSI, IP, IPX, Apple Talk, DECnet, XNS, etc.

A diferencia del puenteo que se presenta en la Capa 2 (la capa de enlace de datos) del modelo OSI, por lo que, las funciones de ruteo y puenteo contendrán información diferente que se utilizará durante el proceso de transferencia de información desde el origen hasta su destino. Aunque ambas funciones cumplen el mismo objetivo, cada una se realiza de forma diferente.




Sin embargo, la función que desempeña el ruteo en las redes es nueva a comparación del puenteo, ya que desde su aplicación a mediados de los años 80, dejo a atrás a las redes de entornos simples y homogéneos. La interconectividad en las redes que permite el ruteo, lo ha colocado como una aplicación generalizada y básica en el desarrollo de toda red.

**6.2- Función principal de los ruteadores.**

Las funciones principales que realiza un ruteador dentro de su operación en una red son:

1. Un ruteador interpreta las direcciones lógicas que se encuentran contenidas en la capa 3, en lugar de las direcciones MAC o de capa de enlace, como lo realizan los puentes o los conmutadores.

2. Los ruteadores son capaces de cambiar el formato de la trama, ya que estos operan en un nivel superior a la misma. Como ventaja, los ruteadores

cuentan con un elevado nivel de inteligencia, que les permite operar y administrar distintos protocolos previamente establecidos.

3. Proporcionan un nivel de seguridad a la red contra ataques externos, puesto que pueden configurarse de manera tal que restringe los accesos a ésta.

4. Reduce las congestiones de la red, al aislar el tráfico las distintas subredes que se interconectan. Por ejemplo, un ruteador que opere con el protocolo TCP/IP puede filtrar los paquetes que le llegan utilizando las máscaras IP.

La función del ruteo se encuentra formada por dos actividades básicas que son:

1. La de nación de las trayectorias óptimas de ruteo

2. El transporte de grupos de nación (llamados comúnmente paquetes) a través de una red.

El conjunto de los procesos de ruteo se le conoce como conmutación. En donde, la conmutación es relativamente directa, mientras que la determinación de la trayectoria puede ser demasiado compleja.

**6.3- Determinación de la trayectoria**

Para determinar una trayectoria de ruteo, es necesario realizar una medición o métrica de la longitud en la trayectoria en donde los algoritmos de ruteo inicializan, actualizan y conservan sus tablas de ruteo. Estas tablas contienen la información acerca de todas las rutas y por consecuencia la trayectoria de las mismas, aunque esta información podrá variar dependiendo del algoritmo de ruteo que se utilice.

Estas tablas de ruteo se alimentan gracias al empleo de cualquiera de los algoritmos de ruteo, los cuales proveen una gran variedad de información que van registrándose dentro de las tablas.

Mediante el empleo de las asociaciones de salto destino/próximo, se informa al ruteador la trayectoria optima para enviar los paquetes a un destino establecido. Esto se realiza, enviando el paquete a un ruteador que represente el "próximo salto" en el camino hacia su destino final.

Es decir, cuando un ruteador recibe un paquete entrante, verifica la dirección de destino del mismo e intenta asociar esta dirección hacia el siguiente salto de la dirección del destino, para que posteriormente, intente asociar esta dirección con el siguiente salto.

Otra información con las que cuentan las tablas de ruteo, son los datos acerca de la conveniencia para el uso de una trayectoria. Ya que los ruteadores comparan las trayectorias con el objeto de determinar cuales son las rutas óptimas a emplear, estas trayectorias difieren en función del diseño al algoritmo de ruteo que se este empleando.

Los ruteadores se encuentran en constante comunicación entre ellos, esta característica les permite actualizar constantemente sus tablas de ruteo. Esta actualización, se realiza mediante el envío de una gran variedad de mensajes entre los ruteadores. De estos mensajes, el principal El mensaje principal que es generado por los ruteadores, consiste en enviarse la actualización del ruteo dentro de la red.

Este mensaje de actualización, se encuentra constituido por una tabla completa de ruteo o una porción de la misma. Al analizar las actualizaciones del encaminamiento de todos los demás ruteadores; este podrá generar una estructura detallada sobre la topología que presenta la red.

Asimismo, otro mensaje que es generado por los ruteadores, es el del estado de enlace. Este mensaje informa a los demás ruteadores acerca del estado en que se encuentran los enlaces del emisor. Los ruteadores pueden utilizar esta información sobre los enlaces para hacerse establecer una visión completa de la topología de la red.

### 6.4- La conmutación

Los algoritmos de conmutación son relativamente simples y básicamente son empleados en los protocolos de ruteo. En la mayoría de los casos, un host determina el envió de un paquete hacia otro host. Cuando un host ha conseguido la dirección de un ruteador, el host origen envía un paquete que se encuentra direccionado específicamente hacia una dirección física MAC (capa de Control de Acceso a Medios) de un ruteador del host destino.

Al examinar la dirección del protocolo de destino dentro del paquete, el ruteador determina si conoce o no cómo encaminar el paquete hacia el siguiente salto. En caso de que el ruteador desconozca cómo direccionar eliminara el paquete. En cambio, si conoce cómo direccionar el paquete, este cambiará la dirección física de destino a la correspondiente del salto siguiente y transmitirá el paquete.

Es importante señalar, que el salto siguiente al que es enviado el paquete puede ser el último y puede ser su host destino. Si no es así, el salto siguiente será otro ruteador que ejecutará nuevamente el mismo proceso de decisión en cuanto a la conmutación. A medida que el paquete viaja a través de la ruta, su dirección física cambia, pero su dirección de protocolo se mantiene constante.

El análisis anterior describe la función de conmutación entre un origen y un sistema terminal de destino.

Para ayudar a mantener un control de estas funciones, la Organización Internacional de Estándares (ISO) ha desarrollado una terminología jerárquica de gran utilidad para la descripción de este proceso.

De acuerdo con esta terminología, a los dispositivos de red que no tengan la capacidad de encaminar los paquetes entre las subredes se les conoce como Sistemas Terminales (ESs). Mientras que a los dispositivos de red que tienen la capacidad de encaminar los paquetes entre las subredes se les asignará el nombre de Sistemas Intermedios (ISs).

Los Sistemas Intermedios (ISs) se dividen en:

- ISs de intradominio, que son aquellos que se pueden comunicar dentro de dominios de ruteo

- ISs de interdominio, que son los que pueden comunicarse con y entre diferentes dominios de ruteo

En general, se considera que un dominio de ruteo es parte de una red que está bajo una autoridad administrativa común, la que se encuentra regulada por un conjunto particular de estatutos administrativos. A los dominios de ruteo también son conocidos como sistemas autónomos.

Con el uso de determinados protocolos, los dominos de ruteo se pueden dividir en áreas de ruteo, pero los protocolos de ruteo de intradominio aún se utilizan para la conmutación dentro de esas áreas.

### 6.5- Algoritmos de ruteo

Los ruteadores generan una tabla de encaminamiento o algoritmo de ruteo en el que se registran los nodos y redes que son alcanzables por cada uno de sus

puertos de salida; es decir, cada tabla registra y describe la topología en que se encuentra conformada la red.

Existen diferentes tipos de algoritmos de ruteo y cada uno de ellos tienen un impacto diferente en los recursos de la red y del ruteador. Los algoritmos de ruteo utilizan una gran variedad de medidas que afectan el cálculo de las rutas óptimas.

Los algoritmos de ruteo se pueden diferenciar tomando en cuenta determinadas características fundamentales en que se encuentran comprendidos. Por lo que, los objetivos particulares del diseño del algoritmo afectan directamente la operación del protocolo de ruteo resultante.

Estos algoritmos de ruteo se pueden clasificar como:

a) Algoritmos de ruteo estáticos
b) Algoritmos de ruteo dinámicos
c) Algoritmo de ruteo de una sola trayectoria
d) Algoritmo de ruteo multitrayectoria
e) Algoritmo plano de ruteo
f) Algoritmos jerárquicos de ruteo
g) Ruteador inteligente
h) Host inteligente
i) Intradomino
j) Interdominio
k) Basados en estado de enlaces
l) Basados en el vector de distancia

Donde;

**a) Algoritmos de ruteo estáticos**

Los algoritmos de ruteo estático son mapeos de tablas determinadas previamente por el administrador de la red antes de empezar el ruteo. Estos mapeos se mantendrán estáticos, a menos que el administrador de la red modifique las tablas, por lo que no pueden ser considerados verdaderos algoritmos de ruteo.

Estos algoritmos de ruteo son basados dentro de un diseño simple de red, y funcionan correctamente en entornos donde el tráfico en la red es predecible.

Esta limitación no les permite reaccionar ante los cambios de la red, por lo que, no son considerados para ser empleados dentro de grandes redes.

**b) Algoritmos de ruteo dinámicos**

Los algoritmos de ruteo dinámico son capaces de aprender y adaptarse por sí mismos la topología de la red, analizando los mensajes entrantes de actualización del ruteo. Estos ruteo que se han implantado en los últimos años contando con una gran aceptación., son algoritmos dinámicos,

Este algoritmo envía un mensaje si detecta que se ha presentado algún cambio en la red; el software de ruteo recalculará las rutas y enviará el mensaje de actualización del nuevo encaminamiento. Estos mensajes penetran la red y, al hacerlo, estimulan a los ruteadores a ejecutar de nuevo sus algoritmos y actualizar sus tablas de ruteo de acuerdo a las circunstancias que los mensajes han reestablecido. Los algoritmos de ruteo dinámico se pueden ir complementando con las rutas establecidas una vez que estas sean convenientes.

**c) Algoritmo de ruteo de una sola trayectoria**

Este algoritmo calcula y registra en la tabla de ruteo un valor para cada conexión entre el router y cualquier nodo que pueda ser alcanzado por él. Este valor se obtiene ya sea en el número de saltos dentro de la red para que un paquete

alcance su destino, el valor que identifique el ancho de banda de la línea utilizada, el costo económico en la transmisión de cada paquete, la distancia geográfica, etc. Es decir, el ruteador dirigirá los paquetes de acuerdo a la ruta más optima considerando los factores anteriores.

**d) Algoritmo de ruteo multitrayectoria**

El uso de estos algoritmos permite que algunos ruteadores sean capaces de gestionar múltiples trayectorias hacia el mismo destino empleando la misma conexión. Estos algoritmos realizan el multiplexaje del tráfico a través de múltiples líneas. Las ventajas que presentan los algoritmos de multitrayectoria, son una mayor confiabilidad y rendimiento eficiente total sustancialmente mejores.

**e) Algoritmo plano de ruteo**

Un sistema que emplee algoritmo de ruteo plano, se presenta cuando todos los ruteadores son equivalentes entre sí y no pertenecen a ninguna estructura jerárquica. Al no encontrarse dentro de una estructura jerárquica centralizada. Los ruteadores cuentan con una flexibilidad total en cuanto a la topología y al tráfico generado en la red.

**f) Algoritmos jerárquicos de ruteo**

Dentro de este algoritmo de ruteo, cada nodo de la red informa periódicamente a un ruteador central los datos y características sobre la topología y parámetros de la red, como el tráfico congestión, etc.

En un sistema que de ruteo jerárquico, algunos ruteadores forman lo que constituye una troncal de ruteo. En donde, los paquetes que son enviados desde los ruteadores que no pertenecen a la troncal, viajan hacia los ruteadores de la troncal, y estos les permiten alcanzar su destino. Es decir, los paquetes viajan

desde el último ruteador de la troncal a través de uno o más ruteadores que no pertenecen a la troncal hacia su destino final.

Los sistemas de ruteo suelen designar grupos lógicos de nodos, llamados dominios, sistemas autónomos y áreas. En los sistemas jerárquicos, algunos ruteadores pertenecientes a un dominio se pueden comunicar con ruteadores de otros dominios, en tanto que otros sólo se pueden establecer comunicación con ruteadores pertenecientes a su dominio. En redes muy grandes pueden existir niveles jerárquicos adicionales, en donde los ruteadores de nivel jerárquico más alto forman la troncal de ruteo.

La ventaja principal del ruteo jerárquico es que imita a la organización con la que cuenta la mayor parte de las compañías y, por lo tanto, soporta muy bien sus patrones de tráfico.

**g) Ruteador Inteligente**

Se define como ruteo inteligente, cuando las trayectorias a través de la red han sido determinadas por los ruteadores, tomando como base sus propios cálculos realizados. Ya que los algoritmos consideran que los hosts de la red desconocen las rutas de los mismos.

En los sistemas que utilizan el ruteo de origen, los ruteadores solamente actúan como dispositivos de almacenar y enviar: envían el paquete al punto siguiente sin pensar. Esto se debe a que, algunos algoritmos de ruteo suponen que el nodo terminal de origen determinará la ruta completa. A estos se le conoce en general como *ruteo de origen.*

**h) Host Inteligente**

Los sistemas en que la inteligencia se encuentra en el host, seleccionarán las con más de frecuencia las mejores rutas, ya que normalmente descubren todas las rutas posibles hacia el destino antes de que se envíe el paquete. Posteriormente, elegirá la mejor trayectoria que considere "óptima" dentro de topología de la red.

Sin embargo, la operación para descubrir todas las rutas disponibles tendrá requerir de un tráfico muy intenso y a su vez del consumo de una gran cantidad de tiempo. La ventaja en el uso de este método consiste en optimizar la trayectoria que se vaya a emplear.

**i) Intradominio**

Los ruteadores de intradominio necesitan conocer solamente a otros ruteadores que se encuentran dentro de su dominio, sus algoritmos de ruteo pueden simplificarse y, dependiendo del algoritmo de ruteo que se esté utilizando el tráfico de actualización del ruteo puede disminuir en la misma medida. Esto es común, ya que la mayor parte de la comunicación de red se da en grupos pequeños dentro de la compañía (dominios).

**j) Interdominio**

Algunos algoritmos de ruteo operan solamente dentro de los dominios; que operan desde dentro del dominio y entre otros dominios. La naturaleza de estos tipos de algoritmos es diferente. Por lo tanto, es razonable que un algoritmo óptimo de ruteo de intradominio no necesariamente será un algoritmo óptimo de ruteo interdominio.

**j) Basados en estado de enlaces**

Los algoritmos basados en estado de enlaces (conocidos como algoritmos abiertos de primero la ruta más corta) distribuyen la información de ruteo a través

de los nodos en la red. Sin embargo, cada ruteador envía solamente la porción de la tabla de ruteo que describe el estado de sus propios enlaces. Es decir, os algoritmos basados en estado de enlaces envían pequeñas actualizaciones hacia todos lados.

**k) Basados en el vector de distancia**

Los algoritmos basados en vector de distancia (conocidos como algoritmos Bellman-ford) hacen que cada ruteador envíe toda o sola una parte de su tabla de ruteo a sus vecinos. Los algoritmos basados en vector de distancia envían actualizaciones más grandes pero sólo a los ruteadores vecinos.

### 6.6- Métricas de ruteo

Las tablas de ruteo contienen información que es utilizada por el software de conmutación para seleccionar la mejor ruta o trayectoria en la red. Los algoritmos de ruteo emplean diferentes métricas con el fin de obtener cuál será la mejor ruta a usar. Los algoritmos sofisticados de ruteo se basan en la selección de varias rutas que se obtienen en la combinación de una sola métrica o híbrido.

La métricas que se emplean son:

- Longitud de la trayectoria
- Confiabilidad
- Retardo
- Ancho de banda
- Carga
- Costos de Comunicación

En todos los casos anteriores, cuando falla una red, algunos enlaces en la red pueden repararse más fácil y rápidamente que otros.

La *longitud de la trayectoria* es la métrica de ruteo más común. Algunos protocolos de ruteo permiten que los administradores de red asignen costos de manera arbitraria a cada uno de los enlaces de la red. En este caso, la longitud de la trayectoria es la suma de los costos asociados de cada uno de los enlaces por los que se pasa la información. Mientras que, otros protocolos de ruteo definen el conteo de saltos, como una métrica que especifica el número de veces que un paquete pasa a través de los productos que conforman la red; por ejemplo, esto se presenta en los ruteadores, que determinan su trayecto desde el origen hasta su destino.

La *confiabilidad*, dentro de los algoritmos de ruteo, se refiere a la dependencia (generalmente descrita en términos de la tasa de errores) de cada enlace en la red. Algunos enlaces de red pueden caerse con mayor frecuencia que otros.

Cualquier factor de confiabilidad se puede tomar en cuenta para la determinación del valor de la misma, ya que son valores numéricos arbitrariamente asignados generalmente a los enlaces de red por los administradores del sistema.

El *retardo* de ruteo, se considera como el periodo de tiempo que se requiere para transferir a través de la red, un paquete desde el origen hasta su destino. Los retardos dependen de varios factores, entre los cuales se encuentran:

- El ancho de banda de los enlaces intermedios de la red
- Las colas en los puertos de cada ruteador a lo largo del camino
- La saturación de la red en todos sus enlaces intermedios y la distancia física a recorrer.

Como el retardo es un conglomerado de alguna variables importantes, es una métrica muy común y útil a la vez.

El *ancho de banda* se refiere a la capacidad de tráfico disponible de un enlace. Si todos los demás parámetros son iguales, sería preferible un enlace Ethernet a 10 Mbps, en vez de una línea privada a 64 Kbps.

Aunque el ancho de banda es una medida del rendimiento eficiente total máximo que se puede alcanzar en un enlace, las rutas que pasan a través de enlaces con una ancho de banda mayor no necesariamente son mejores rutas que las que viajan a través de enlaces más lentos. Si, por ejemplo, un enlace más rápido está muy ocupado, puede requerir de más tiempo para enviar un paquete a su destino.

La *carga* se refiere a qué tan ocupado está un recurso de la red, como un ruteador por ejemplo. La carga se puede calcular de muchas maneras, entre otras la utilización del CPU y el número de paquetes procesados por segundo. La supervisión continua de estos parámetros puede consumir por sí misma muchos recursos.

Los costos de comunicación son otra métrica importante, sobre todo porque a algunas compañías no le importa tanto el desempeño de una red como los costos de operación de la misma. A pesar de que el retardo de la línea puede ser más grande, enviarán paquetes a través de sus propias líneas en vez de hacerlos por líneas públicas, las cuales tiene un costos asociado en función de tiempo de uso.

# Conclusiones

## CONCLUSIONES

Con la implementación de voz sobre IP para conectar centrales telefónicas remotas, se ha logrado reducir considerablemente costos generados del servicio de telefonía de larga distancia. Dichas reducciones, son reflejadas en el consumo del servicio, el cual es facturado y pagado mensualmente a las empresas telefónicas regionales de cada oficina.

Esta modalidad de comunicación, surge, de la necesidad de reducir costos de operación, mediante un esquema de baja inversión de instalación y administración.

Esta condición, ha sido cumplida, gracias a la evolución que han experimentado las redes de área local LAN durante los últimos años. Ya que, al integrar el servicio de voz dentro de una red de transmisión de datos, se ha obtenido una nueva y gran herramienta, esencial en la logística de operación de las empresas. Adicionalmente a esto, un ahorro significativo de los gastos de la misma; al utilizar para ello, la infraestructura de su red de datos existente, sin que ello, represente una disminución en la calidad en la prestación del servicio.

Cabe señalar, que la implementación de voz sobre IP, agrego a la lista de ventajas competitivas, una arquitectura de seguridad total, la cual es casi invulnerable a las interferencias presentadas en los medios convencionales.

Con esta reducción de costos en servicio de telefonía, existe la posibilidad de invertir en nuevas áreas de desarrollo o tecnología dentro de la empresa, que permitan, cada vez más, reducir los tiempos en los procesos operativos, sin que ello represente la separación de capital humano en la misma.

Cabe señalar, actualmente las reducciones de gastos se dan en su totalidad dentro de este rubro, consecuencia de la poca dedicación hacia las soluciones enfocadas al uso de la ingeniería que esta a nuestro servicio.

Finalmente, como se ha descrito, las áreas de ingeniería y tecnología han agregado al contenido de sus funciones principales, un nuevo carácter de tipo financiero y decisivo. Esta cualidad, las ha ido ubicando, cada vez más, como áreas estratégicas y de planeación dentro de las empresas.

Esta nueva función, incrementa el espacio y oportunidades, antes limitadas, del ingeniero, hacia nuevos procesos administrativos y de dirección dentro de la nueva globalización, la cual se rige bajo sus propios modelos de negocios.

# BIBLIOGRAFIA

**Tecnologías de interconectividad de redes**
Cisco Solutions
Edición 1999

**Redes privadas virtuales**
Bay Networks
Edición 2000

**H.323 Multimedia sobre redes IP**
Jose Manuel Huidobro
Editorial BIT
Edición 2001

## Glosario de Términos

**Address resolution (Resolución de direcciones)**
Conversión de una dirección Internet a la dirección física correspondiente.

**Agent Name Delivery (Envío de acuerdo al Agente utilizado)**
Proceso de enviar a los robots de los motores de búsqueda a una página adaptada, dirigiendo sus visitas hacia lo que Usted desea que vean. Esto es realizado (pensamos) mediante la utilización de capacidades instaladas en el servidor (Server Side Includes) u otras técnicas de contenido dinámico. Los SSI, por ejemplo, pueden ser utilizados para mostrar al visitante diferente contenido dependiendo del valor del HTTP_USER_AGENT.

**Ancho de banda (Bandwidth)**
Capacidad de un medio para transmitir una señal, que en el caso de una red hace referencia a la cantidad de ficheros y mensajes que se pueden enviar sin degradar sus prestaciones.
Capacidad máxima de transmisión de enlace. Usualmente se mide en bits por segundo (bps). Es uno de los recursos más caros de toda la red y es una de las principales limitantes para el desarrollo de aplicaciones que requieren transferir grandes cantidades de información.

**ANSI (American National Standards Institute)**
Instituto de estandarización de EE.UU., que ha creado diversos entándares, entre los que podemos citar ASCII.

**ASCII**
American Standard Code Information Interchange.Estándar que define como representar dígitos, letras, signos y signos de puntuación en computadoras.

**ARPA (Advanced Research Project Agency)**
Agencia de Gobierno de EE.UU. quien fue la agencia precursora de Internet.

**Applet**

Pequeño programa, habitualmente escrito en Java, que suele correr en el navegador, como parte de una página web. Es posible que el uso de estos programas eviten la indexación de una página por parte de los virus y robots.

**Backbone**

Es la infraestructura de conexión principal de una red y está constituida por los enlaces de mayor velocidad dentro de dicha red.

**Baudio:**

Medida de transmisión de datos que se puede considerar, a efectos prácticos, como un bit por segundo. Basada del nombre de J.M.E. Baudot.

**Bit**

La unidad mínima de información, equivalente a una elección binaria: S o no, 1 o 0. En inglés binary digit, "dígito binario".

**Bps**

Bits por segundo. Unidad de medida que indica los bits por segundo transmitidos por un equipo.

**Buscador**

Programa de computo que tiene la función de localizar contenidos en la Web, como Yahoo! (http://www.yahoo.com/)

**Cliente**

Programa que interactúa dentro de una estructura de red, realizando peticiones a un programa ubicado en el servidor a través del uso de un mismo protocolo.

**Channel listings (Canales)**

Listados de enlaces hacia sitios web seleccionados, usualmente populares. Mantenidos por los motores de búsqueda y directorios. Los enlaces son ordenados en categorías o canales. Los sitios son elegidos por un editor del

canal, habitualmente porque dicho sitio ya tiene un alto ranking en los buscadores.

**Dial-up**

Cuenta de Internet que permite la conexión vía módem a la red. Normalmente requiere de la contratación con un ISP (Internet Service Provider, Proveedor de servicios de Internet) quien cuenta con una conexión dedicada a la red y revende el acceso a través de bancos de módems.

**Dirección IP**

Internet Protocol; Protocolo de Internet. Dirección única de un dispositivo en una red TCP/IP. Consiste en cuatro números entre 0 y 255 separados por puntos. Por ejemplo: 255.255.240.70)

**DNS**

Domain Name System; Sistemas de nombres de dominios. Sistema para facilitar la administración y localización de direcciones IP que funciona asignando uno o más alias a cada dirección IP. También suele llamarse así a las computadoras encargadas de administrar la base de datos del sistema de nombres de dominio. Una aplicación del DNS es la creación de nombres de dominio para correo.

**Dominio**

Un componente en la jerarquía de nombres. Un dominio consiste en una secuencia de nombres o otras palabras separadas por puntos. Asimismo realiza la localización del servidor de la Internet que contiene la página a la que remite un enlace.

**Datagrama**

Es la unidad de información básica usada en Internet. Contiene direcciones de fuente y destino, conjuntamente con el dato. Aquellos mensajes que son muy grandes se dividen en una secuencia de datagramas IP.

**Dead Link (Enlace muerto)**
Un enlace que no lleva a ninguna página o sitio, quizá debido a que el servidor esta caído o la página fue removida o no existe más. La mayoría de los motores de búsqueda tienen técnicas para remover estas páginas de sus listados automáticamente, pero como Internet continúa creciendo, se vuelve más y más difícil para un buscador controlar regularmente todas las páginas de sus índices.

**Directory (Directorio)**
Es un servidor o conjunto de servidores dedicados a indexar páginas web en Internet y devolver listas de éstas que se ajusten a una consulta determinada.

**Encriptación**
Procedimiento de ocultación de contenidos mediante una clave. Actualmente, los algoritmos de encriptación puede utilizar hasta 2200 bits para garantizar la confidencialidad de la información.

**Ethernet**
Esquema de red de 10 Mbits/seg. Qué fue desarrollado originalmente por Xerox Corporation. Su empleo se extiende a las redes de área local, ya que está disponible para muchos tipos de ordenadores, no precisa de licencias y existen componentes para soportarla de diversos fabricantes.

**FAQ**
Frecuently Asked Questions; Preguntas más frecuentes. Es un archivo con la respuesta a las preguntas más comunes sobre algún tema.

**Firewall**
Programa o equipo encargado de proteger la red o computadoras conectada a Internet de accesos externos de la misma no autorizados.

**FTP**

File Transfer Protocol; Protocolo de Transferencia de Archivos. Como su nombre lo indica, define los mecanismos y reglas para transferir archivos entre las diversas computadoras de la red.

**FDDI (Fiber Distributed Data Inerface)**

Estándar para tecnología de red basado en fibra óptica establecido por la ANSI que está siendo utilizado cada vez más.

**FYI**

Abreviatura de la frase "For Your Information." También se designan con este término documentos que resuelven dudas típicas de los usuarios nuevos y otras cosas útiles.

**Gateway**

Ordenador dedicado que conecta dos o más redes y encamina los paquetes de una red a otra. Los gateways encaminan los paquetes hacia otros gateways hasta pueden ser entregados al destino final directamente a través de una red física.

**Headquarters**

Descripción actual de las oficinas corporativas de una empresa u organización

**Hipertexto / Hipertext**

Un texto especial que contiene la dirección de otro texto, con lo que se convierte en algo más que un texto, un hipertexto.

**HTML**

Hiper Text Markup Language; Lenguaje de Marcación de Hipertexto. Lenguaje utilizado para la creación de documentos de hipertexto e hipermedia. Es el estándar usado en el WWW.

**Http (HiperText Transfer Protocol)**

Protocolo de transmisión mediante el uso del hipertexto.

**Hipertexto**

Conjunto de texto y contenidos multimedia que no está creado para ser leído linealmente (es decir, empezando por el principio y acabando por el final), sino que utiliza enlaces para hacer remisiones, poner en contacto distintas partes, o para conectarse con otros textos.

**Hostname**

Identifica el nombre del servidor principal de la red.

**Intranet**

Red de uso privado que emplea los mismos estándares y herramientas de Internet. Es uno de los segmentos del mercado de computación que más desarrollo ha experimentado.

**Interfaz:**

Sistema de comunicación de un programa con su usuario; la interfaz comprende las pantallas y los elementos que informan al usuario sobre lo que puede hacer, o sobre lo que está ocurriendo.

**Internet**

Conjunto de ordenadores, o servidores, conectados en una red de redes mundial, que comparten un mismo protocolo de comunicación, y que prestan servicio a los ordenadores que se conectan a esa red.

**ISP**

Internet Service Provider; Proveedor de Servicios de Internet. Compañía dedicada a revender el acceso a Internet. Puede proveer desde enlaces dial-up hasta enlaces dedicados de muy alta velocidad. También puede ofrecer servicios adicionales como desarrollo y mantenimiento de web sites, de servidores de correo electrónico, etc.

**ISO (International Organization for Standarization).**

Organización internacional que establece normalizaciones en muchos campos de la técnica. Entre otras cosas, coordina los principales estándares de redes que se usan actualmente.

**Java**

Lenguaje de programación independiente de la plataforma, creado por Sun Microsystems. Está pensado para una arquitectura cliente/servidor en la que sólo es necesario intercambiar pequeñas porciones de código (llamadas Applets) que son ejecutadas por el cliente.

**LAN (Local Area Network)**

Término que significa "Red de Área Local," y que describe cualquier tecnología de red física que trabaja a gran velocidad en distancias cortas (de hasta unos cientos de metros).

**Login o Username (Nombre de Usuario)**

Entrada, Acceso, Conectado. Clave de acceso. Proceso de entrar a un sistema dando una clave y una contraseña.

**Medio**

Material utilizado para la transmisión de los datos. Puede ser cable de cobre, coaxial, fibra óptica o ondas electromagnéticas.

**Multiplexor**

División de un único medio de transmisión en múltiples canales lógicos que soportan muchas sesiones simultáneas.

**Módem**

Dispositivo que se usa para transmitir información entre un ordenador y la línea telefónica.

**Multimedia**

Combinación de texto, imagen, sonido e imagen en movimiento.

**Navegador (Browser)**

Programa cliente que permite navegar o recorrer el WWW manejando cualquiera de los siguientes protocolos y servicios: HTTP, FTP, Gopher, e-mail y News.

**Nombre de dominio (Domain Name)**

Nombre base de un lugar en Internet, por ejemplo www.tvspots.com.mx.

**Navegación**

La exploración de una obra en hipertexto, como una página Web, saltando de un punto a otro de la página, o de una página a otra según los deseos del usuario.

**NFS (Network File System).**

Método desarrollado por Sun Microsystems que permite compartir ficheros en una red de la misma manera en que fuesen locales a cada uno de los sistemas.

**NIC**

Network Information Center. Organismo de regular el control de nombres de dominios dentro de Internet

**POP (Post Oficce Protocol)**

Protocolo empleado por el software cliente para extraer mensajes de los servidores de correo.

**PPP (Point to Point Protocol)**

Protocolo punto a punto que maneja TCP/IP por líneas telefónicas y que permite correr un programa cliente (navegador, correo electrónico u otro) en el equipo del usuario.

**Protocolo**

Estándar que permiten la comunicación entre dos o más computadoras dentro de cualquier topología de red.

**Query (Consulta)**
Una palabra, frase o grupo de palabras, posiblemente combinadas con otra sintaxis, utilizada para instruir a los motores de búsqueda o directorios que localicen páginas web.

**Red**
Grupo de equipos de computo conectadas entre sí, permitiendo la trasmisión de información entre ellos. Existen varios tipos de redes, ya sean locales (LAN), amplias (WAN), etc.

**Resolver**
Traducción de un nombre Internet en su dirección IP equivalente u otra información para DNS.

**Router**
Equipo conectado a un enlace encargado de transmitir paquetes de información dentro y hacia de cualquier red LAN o WAN.

**Paquete**
Unidad de datos enviados dentro de una red conmutada. También es posible referirse a aquellos datos enviados físicamente por la red o a los datagramas que son utilizados por el protocolo IP.

**SLIP (Serial Line Internet Protocol)**
Protocolo antecesor al PPP que también permite el establecimiento de conexiones TCP/IP a través de una línea seriada.

**SMTP (Simple Mail Transfer Protocol)**
Protocolo sencillo de transferencia de correo. Protocolo original de intercambio de correo en Internet.

**Servidor**
Equipo de computo que suministra información, a través de una red, a otros ordenadores llamados "clientes".

**Relación Señal-Ruido (SNR)**

Describe la relación entre la cantidad de información en una discusión comparada con su calidad.

**Servidor de terminales.**

Ordenador especializado que conecta un conjunto de terminales a una red de área local.

**T1**

Enlace para la transmisión de datos con una conexión dedicada de alta velocidad a (1.54 Mbps)

**T3**

Enlace para transmisión de datos con una conexión dedicada de alta velocidad a (44 Mbps)

**TCP/IP**

Transmit Control Protocol / Internet Protocol. Protocolo de control de transmisión por medio de paquetes de mensajes y protocolo de interconexión de redes.

**Telnet**

Programa que permite establecer una conexión en modo terminal a otra computadora que se encuentre en Internet y que brinde este servicio. En lugar de hacer una llamada telefónica, se usa la red de Internet para acceder a otro equipo.

**TCP/IP (Transmission Control Protocol/Internet Protocol)**

Conjunto de protocolos usados en Internet para soportar servicios tales como acceso remoto telnet, transferencia de ficheros FTP y correo electrónico SMTP.

**Tráfico**

También refiere al número de usuarios, accesos, solicitudes que viajan por la red durante un periodo de tiempo determinado.

**URL (Uniform Resource Locator)**

Dirección del recurso de Internet, ya sea una página WWW, un servicio FTP o un grupo de noticias UseNet u otros recursos.

**WWW**

Forma abreviada para describir World Wide Web.

**World Wide Web**

Interfaz de comunicación en la Internet, que hace uso de enlaces de hipertexto en el interior de una misma página, o entre distintas